kaspersky

Kaspersky Embedded Systems Security

Contenu

A propos de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security protège les ordinateurs et les autres systèmes imbriqués sous Microsoft® Windows® (ci-après les périphériques protégés) contre les virus et les autres menaces informatiques. Les utilisateurs de Kaspersky Embedded Systems Security sont les administrateurs de réseau de l'organisation et les personnes chargées de la protection antivirus de ce réseau.

Vous pouvez installer Kaspersky Embedded Systems Security sur plusieurs systèmes imbriqués sous Windows, y compris les types d'appareils suivants :

- GAB (guichets automatiques bancaires)
- TPV (terminal de point de vente)

Kaspersky Embedded Systems Security peut être géré de la manière suivante :

- via la console de l'application installée sur le même périphérique protégé que Kaspersky Embedded Systems Security ou sur un autre périphérique
- via la ligne de commande
- Via la console d'administration de Kaspersky Security Center

Vous pouvez utiliser également l'application Kaspersky Security Center pour l'administration centralisée de plusieurs périphériques protégés dotés de Kaspersky Embedded Systems Security.

Il est possible de consulter les compteurs de performance de Kaspersky Embedded Systems Security pour l'application « Moniteur système » ainsi que les compteurs et les interruptions SNMP.

Composants et fonctions de Kaspersky Embedded Systems Security

L'application intègre les modules suivants :

- **Protection des fichiers en temps réel**. Kaspersky Embedded Systems Security analyse les objets à l'accès. Kaspersky Embedded Systems Security analyse les objets suivants :
  - Les fichiers ;
  - Flux alternatifs des systèmes de fichiers (flux NTFS) ;
  - Enregistrements de démarrage principal et les secteurs d'amorçage des disques durs locaux ou amovibles.
- **Analyse à la demande**. Kaspersky Embedded Systems Security recherche une fois des virus et autres menaces informatique dans la zone indiquée. L'application analyse les fichiers, la mémoire vive et les objets de démarrage sur un périphérique protégé.
- **Contrôle du lancement des applications**. Ce composant surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus sur un périphérique protégé.
- **Contrôle des périphériques**. Le composant contrôle l'enregistrement et l'utilisation des périphériques externes afin de protéger le périphérique contre les menaces sur la sécurité de l'information qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou des périphériques externes d'un autre type connectés par USB.

- **Gestion du pare-feu**. Ce composant permet d'administrer le pare-feu Windows : il permet de configurer les paramètres et les règles du pare-feu du système d'exploitation et interdit toute possibilité de configuration externe du pare-feu.

- **Moniteur d'intégrité des fichiers**. Kaspersky Embedded Systems Security détecte les modifications introduites dans les fichiers qui appartiennent aux zones de surveillance définies dans les paramètres de la tâche. Ces modifications peuvent signaler une violation de la sécurité sur l'appareil protégé.

- **Inspection des journaux**. Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.

L'application peut remplir les fonctions suivantes :

- **Mise à jour des bases de l'application** et **Mise à jour des modules de l'application**. Kaspersky Embedded Systems Security télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky, depuis le Serveur d'administration de Kaspersky Security Center ou depuis d'autres sources de mises à jour.

- **Quarantaine**. Kaspersky Embedded Systems Security place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers le dossier *Quarantaine*. Pour des raisons de sécurité, les objets dans le dossier de quarantaine sont conservés sous forme chiffrée.

- **Sauvegarde**. Kaspersky Embedded Systems Security enregistre une copie chiffrée des objets dont le statut est *Infecté* dans la *Sauvegarde* avant de les désinfecter ou de les supprimer.

- **Notifications de l'administrateur et des utilisateurs**. Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au périphérique protégé sur les événements liés au fonctionnement de Kaspersky Embedded Systems Security et à l'état de la protection antivirus du périphérique.

- **Importation et exportation des paramètres**. Vous pouvez exporter les paramètres de Kaspersky Embedded Systems Security dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Embedded Systems Security depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.

- **Application des modèles**. Vous pouvez configurer manuellement les paramètres de sécurité du nœud dans l'arborescence ou dans la liste des ressources fichier de l'appareil protégé et enregistrer les valeurs définies dans un modèle. Vous pourrez ensuite appliquer ce modèle à la configuration des paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Embedded Systems Security.

- **Gestion des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security** Vous pouvez configurer les autorisations d'administration de Kaspersky Embedded Systems Security et des services Windows que l'application enregistre pour des utilisateurs ou des groupes d'utilisateurs.

- **Enregistrement des événements Windows**. Kaspersky Embedded Systems Security enregistre les informations relatives aux paramètres de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution des tâches, aux événements associés avec Kaspersky Embedded Systems Security et aux informations requises pour diagnostiquer les erreurs dans Kaspersky Embedded Systems Security.

- **Zone de confiance**. Vous pouvez composer la liste des exclusions de la zone de protection ou d'analyse que Kaspersky Embedded Systems Security appliquera aux tâches d'analyse à la demande et de protection en temps réel de l'ordinateur.

- **Protection contre les exploits**. Vous pouvez protéger la mémoire du processus contre l'exploitation des vulnérabilités à l'aide de l'Agent de protection intégré dans ce processus.

Nouveautés

La nouvelle version de Kaspersky Embedded Systems Security présente les nouvelles fonctionnalités et améliorations suivantes :

- Les systèmes d'exploitation suivants sont désormais compatibles :
  - Windows 10 22H2
  - Windows 11 22H2
- La tâche Contrôle des périphériques accepte l'utilisation de masques pour la zone d'application des règles, permet d'autoriser l'accès aux appareils uniquement aux utilisateurs ou aux groupes d'utilisateurs de confiance et créer les règles sur la base des données de la liste réseau Kaspersky Security Center des appareils ajoutés.
- L'ensemble des critères de déclenchement de la tâche Contrôle du lancement des applications est étendu : vous pouvez lancer les applications via la ligne de commande définie et vous pouvez sélectionner plusieurs critères.
- Un nouveau composant d'analyse des scripts exécutables à l'aide de la technologie AMSI pour Windows a été introduit.
- Tâche Gestion du pare-feu : des règles pour les connexions sortantes sont ajoutées, ainsi que la gestion des connexions ICMPv4 et ICMPv6.
- La section Diagnostic des échecs est introduite dans les stratégies de Kaspersky Security Center : vous pouvez gérer les paramètres des fichiers de traçage et des fichiers dump. Vous pouvez également gérer ces options à l'aide de l'utilitaire de ligne de commande kavshell.exe et à l'aide de la ligne de commande du programme d'installation setup.exe lors de l'installation. Les options de gestion du traçage et de gestion des vidages pour l'appareil protégé par Kaspersky Embedded Systems Security sont disponibles dans l'utilitaire de diagnostic à distance de Kaspersky Security Center.
- Lors de l'installation, vous pouvez sélectionner l'étendue des données enregistrées pour la migration vers une nouvelle version de Kaspersky Embedded Systems Security à l'aide de la ligne de commande du programme d'installation.
- La condition prérequise suivante pour l'installation du produit a été ajoutée : le système d'exploitation doit être compatible avec les certificats affichant des signatures SHA-256.
- La publication d'événements dans le journal d'événement Windows est ajoutée pour la tâche d'inspection des journaux.
- Les tâches de mise à jour des bases de données sont créées automatiquement lors de l'installation pour tous les types de paquets d'installation (avec et sans bases antivirus).

La version de l'application est cumulative et inclut les problèmes résolus des versions précédentes.

Sources d'informations sur Kaspersky Embedded Systems Security

Cette section décrit les différentes sources d'informations sur l'application.

Vous pouvez choisir celle qui vous convient le mieux en fonction du niveau d'importance et de l'urgence de la question.

Sources de données pour des consultations indépendantes

Vous pouvez utiliser les sources suivantes pour rechercher vous-même des informations sur Kaspersky Embedded Systems Security :

- Page de Kaspersky Embedded Systems Security sur le site Internet de Kaspersky.
- Page de Kaspersky Embedded Systems Security sur le site du Support Technique (Base de connaissances).
- Manuels.

Si vous ne trouvez pas la solution à votre problème, veuillez contacter le Support Technique de Kaspersky.

L'utilisation des sources d'informations sur le site Internet de Kaspersky requiert une connexion à Internet.

Page de Kaspersky Embedded Systems Security sur le site Internet de Kaspersky

La page de Kaspersky Embedded Systems Security fournit des informations générales sur l'application, sur ses fonctionnalités et ses particularités.

La page de Kaspersky Embedded Systems Security affiche un lien vers le magasin en ligne. Dans la boutique, vous pourrez acheter l'application ou prolonger vos droits d'utilisation.

Page de Kaspersky Embedded Systems Security dans la base des connaissances

La base de connaissances est une section du site du Support technique.

La page de Kaspersky Embedded Systems Security dans la Base des connaissances permet de trouver les articles qui proposent 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 qui concernent non seulement Kaspersky Embedded Systems Security mais également d'autres applications de Kaspersky. Ces articles peuvent également contenir des actualités du Support technique.

Documentation de Kaspersky Embedded Systems Security

Le Manuel de l'administrateur de Kaspersky Embedded Systems Security reprend les informations relatives à l'installation, à la désinstallation, à la configuration des paramètres et à l'utilisation de l'application.

Discussions sur les applications Kaspersky dans le forum

Vous pouvez discuter des questions relatives aux applications Kaspersky avec d'autres utilisateurs et des experts de Kaspersky dans notre Forum.

Dans le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires et créer des sujets de discussion.

Kaspersky Embedded Systems Security

Cette section décrit les fonctions, les modules et le kit de distribution de Kaspersky Embedded Systems Security. Elle reprend la configuration matérielle et logicielle requise pour l'application.

Kit de distribution

Le kit de distribution contient une page de bienvenue au départ de laquelle vous pouvez réaliser les opérations suivantes :

- lancer l'assistant Installation de Kaspersky Embedded Systems Security.
- lancer l'assistant Installation de la console de Kaspersky Embedded Systems Security.
- lancer l'assistant d'installation du plug-in Kaspersky Embedded Systems Security pour gérer l'application via Kaspersky Security Center.
- Ouvrez la page de Kaspersky Embedded Systems Security sur le site Internet de Kaspersky.
- Visiter le site Internet du Support technique.
- lire les informations relatives à la version actuelle de Kaspersky Embedded Systems Security.

Le dossier \console contient les fichiers d'installation de la console de l'application (ensemble des composants "Outils d'administration de Kaspersky Embedded Systems Security").

Le dossier \product contient :

- les fichiers d'installation des composants de Kaspersky Embedded Systems Security sur un périphérique protégé tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows ;
- le fichier d'installation du plug-in Kaspersky Embedded Systems Security via Kaspersky Security Center ;
- l'archive contenant les bases antivirus d'actualité au moment de l'édition de l'application ;
- un fichier contenant le texte du Contrat de licence utilisateur final et de la Politique de confidentialité.

Le dossier \product_no_avbases contient les fichiers d'installation des composants et du plug-in d'administration de Kaspersky Embedded Systems Security sans les bases antivirus.

Le dossier \setup contient les fichiers indispensables au lancement de l'application de bienvenue.

Les fichiers du kit de distribution s'installent dans les différents dossiers en fonction de leur rôle (cf. tableau ci-après).

Fichiers u kit de distribution de Kaspersky Embedded Systems Security

Fichier	Fonction
autorun.inf	Fichier de démarrage automatique de l'assistant d'installation de Kaspersky Embedded Systems Security pour l'installation de l'application depuis un disque amovible.
release_notes.txt	Ce fichier contient les informations relatives à la version.

migration.txt	Le fichier décrit la migration depuis les versions antérieures de l'application.
setup.exe	Fichier d'accueil de lancement de l'application (lance setup.hta).
\console\esstools_x86.msi	Package Windows Installer ; installe la Console de l'application sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 32 bits.
\console\esstools_x64.msi	Package Windows Installer ; installe la Console de l'application sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 64 bits.
\console\setup.exe	Fichier de lancement de l'Assistant d'installation de l'ensemble des composants "Outils d'administration" (contient la console de l'application) ; lance le fichier du paquet d'installation esstools.msi selon les paramètres d'installation définis dans l'Assistant d'installation.
\product\bases.cab	Archive contenant les bases antivirus d'actualité au moment de l'édition de l'application.
\product\setup.exe	Fichier d'installation de Kaspersky Embedded Systems Security sur le périphérique protégé à l'aide de l'assistant ; il démarre le fichier du paquet d'installation ess.msi avec les paramètres d'installation spécifiés dans l'assistant.
\product\ess_x86.msi	paquet Windows Installer ; installe la configuration **Protéger l'ordinateur avec des bases antivirus** de Kaspersky Embedded Systems Security sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 32 bits. Si la configuration Protéger l'ordinateur avec des bases antivirus est sélectionnée, tous les composants de Kaspersky Embedded Systems Security sont inclus par défaut à l'exception des composants Gestion du pare-feu et Compteurs de performance. Lorsque vous installez la configuration Protéger l'ordinateur avec les bases antivirus de Kaspersky Embedded Systems Security sur une version de l'application qui n'utilise pas l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement enrichi via l'ajout des composants suivants : • Protection des fichiers en temps réel • Analyse à la demande • Protection contre les menaces réseau
\product\ess_x64.msi	paquet Windows Installer ; installe la configuration **Protéger l'ordinateur avec des bases antivirus** de Kaspersky Embedded Systems Security sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 64 bits.

	Si la configuration Protéger l'ordinateur avec des bases antivirus est sélectionnée, tous les composants de Kaspersky Embedded Systems Security sont inclus par défaut à l'exception des composants Gestion du pare-feu et Compteurs de performance. Lorsque vous installez la configuration Protéger l'ordinateur avec les bases antivirus de Kaspersky Embedded Systems Security sur une version de l'application qui n'utilise pas l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement enrichi via l'ajout des composants suivants : • Protection des fichiers en temps réel • Analyse à la demande • Protection contre les menaces réseau
\product\ess.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de Kaspersky Embedded Systems Security via Kaspersky Security Center.
\product\klcfginst.exe	Programme d'installation du plug-in Kaspersky Embedded Systems Security via Kaspersky Security Center. Installez le plug-in d'administration sur chacun des périphériques protégés dotés de la Console d'administration Kaspersky Security Center si vous avez l'intention de l'utiliser pour administrer Kaspersky Embedded Systems Security.
\product\license.txt	Texte du Contrat de licence utilisateur final et de la Politique de confidentialité.
\product_long_term\setup.exe	Fichier d'installation de Kaspersky Embedded Systems Security sur le périphérique protégé à l'aide de l'assistant ; il démarre le fichier du paquet d'installation ess.msi avec les paramètres d'installation spécifiés dans l'assistant.
\product_long_term\ess_x86.msi	paquet Windows Installer ; installe la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut** de Kaspersky Embedded Systems Security sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 32 bits.

	Les composants qui permettent les mises à jour ne sont pas inclus dans la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut. Si la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut est sélectionnée, les composants suivants sont inclus par défaut : • Core • Protection contre les exploits • Contrôle du lancement des applications • Icône de la barre d'état système Lorsque vous installez la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut de Kaspersky Embedded Systems Security sur une version de l'application qui utilise l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement réduit via l'élimination des composants suivants : • Protection des fichiers en temps réel • Analyse à la demande • Les composants qui permettent les mises à jour Cette configuration est recommandée pour protéger les systèmes aux ressources limitées. Dans ce cas, vous pouvez activer l'application à long terme et le composant Contrôle du lancement des applications assure la protection de l'ordinateur.
\product_long_term\ess_x64.msi	paquet Windows Installer ; installe la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut** de Kaspersky Embedded Systems Security sur le périphérique protégé exécutant un système d'exploitation Microsoft Windows 64 bits.

	Les composants qui permettent les mises à jour ne sont pas inclus dans la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut. Si la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut est sélectionnée, les composants suivants sont inclus par défaut : • Core • Protection contre les exploits • Contrôle du lancement des applications • Icône de la barre d'état système Lorsque vous installez la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut de Kaspersky Embedded Systems Security sur une version de l'application qui utilise l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement réduit via l'élimination des composants suivants : • Protection des fichiers en temps réel • Analyse à la demande • Les composants qui permettent les mises à jour Cette configuration est recommandée pour protéger les systèmes aux ressources limitées. Dans ce cas, vous pouvez activer l'application à long terme et le composant Contrôle du lancement des applications assure la protection de l'ordinateur.
\product_long_term\ess_light.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de Kaspersky Embedded Systems Security via Kaspersky Security Center.
\product_long_term\klcfginst.exe	Programme d'installation du plug-in Kaspersky Embedded Systems Security via Kaspersky Security Center. Installez le plug-in d'administration sur chacun des périphériques protégés dotés de la Console d'administration Kaspersky Security Center si vous avez l'intention de l'utiliser pour administrer Kaspersky Embedded Systems Security.
\product_long_term\license.txt	Texte du Contrat de licence utilisateur final et de la Politique de confidentialité.
\setup\setup.hta	Fichier pour le lancement de l'application d'accueil.

Configurations logicielle et matérielle requises

Avant d'installer Kaspersky Embedded Systems Security, il convient de supprimer du périphérique tout autre logiciel antivirus qui serait installé.

Configuration logicielle requise pour le périphérique protégé

Vous pouvez installer Kaspersky Embedded Systems Security sur un périphérique tournant sous une version 32 ou 64 bits d'un système d'exploitation Microsoft Windows.

Windows Installer 3.1 est obligatoire pour une installation correcte de l'application et fonctionne sur un périphérique protégé sous Microsoft Windows XP.

Pour installer et utiliser Kaspersky Embedded Systems Security sur des périphériques protégés avec des systèmes d'exploitation embarqués, le composant Gestionnaire de filtre est obligatoire.

Pour que Kaspersky Embedded Systems Security fonctionne correctement, la prise en charge de SHA-2 sous Windows est requise. Pour obtenir des informations détaillées, consultez la page suivante : https://support.kaspersky.com/15728.

Vous pouvez installer Kaspersky Embedded Systems Security sur un périphérique tournant sous un des systèmes d'exploitation Microsoft Windows 32 bits ou 64 bits suivants :

- Postes de travail :
  - Windows XP Pro SP2 32 bits/64 bits
  - Windows XP Pro SP3 (32 bits)
  - Windows 7 Professional/Enterprise/Ultimate SP1 32 bits/64 bits
  - Windows 8 Pro/Enterprise 32 bits/64 bits
  - Windows 8.1 Pro/Enterprise 32 bits/64 bits
  - Windows 10 version 1507 Home / Pro / Education / Enterprise 32 bits/64 bits
  - Windows 10 LTSC 2015 version 1507 32 bits/64 bits
  - Windows 10 RS1 version 1607 Home / Pro / Education / Enterprise 32 bits/64 bits
  - Windows 10 LTSC 2016 version 1607 32 bits/64 bits
  - Windows 10 RS2 version 1703 Home / Pro / Education / Enterprise 32 bits/64 bits
  - Windows 10 RS3 version 1709 Home / Pro / Education / Enterprise 32 bits/64 bits
  - Windows 10 RS4 version 1803 Home / Pro / Education / Enterprise 32 bits/64 bits
  - Windows 10 RS5 version 1809 Home / Pro / Education / Enterprise 32 bits/64 bits

- Windows 10 LTSC 2019 version 1809 32 bits/64 bits
- Windows 10 19H2 version 1909 Home / Pro / Education / Enterprise 32 bits/64 bits
- Windows 10 21H2 version 21H2 Home / Pro / Education / Enterprise 32 bits/64 bits
- Windows 10 LTSC 2021 version 21H2 32 bits/64 bits
- Windows 10 22H2 version 22H2 Home / Pro / Education / Enterprise 32 bits/64 bits
- Windows 11 21H2 version 21H2 Home / Pro / Education / Enterprise 64 bits
- Windows 11 22H2 version 2H2 Home / Pro / Education / Enterprise 64 bits

- Systèmes embarqués :
  - Windows XP Embedded SP2 (WEPOS) 32 bits / 64 bits
  - Windows XP Embedded SP3 (POS Ready 2009) 32 bits
  - Windows 7 SP1 Embedded 32-bit / 64 bits
  - Windows Embedded 8.1 Industry Pro 32 bits/64 bits
  - Windows Embedded 8.0 Industry Pro 32 bits/64 bits
  - Windows 10 IoT 32 bits/64 bits

Configuration matérielle requise pour le périphérique protégé

La configuration matérielle requise pour le périphérique protégé varie en fonction du système d'exploitation Windows :

- Configuration matérielle requise pour un périphérique tournant sous Windows XP (32 / 64 bits), Windows Embedded POS Ready 32 bits ou Windows Embedded POS Ready 7 :
  - Configuration minimale :
    - Espace disque requis :
      - Pour installer le composant Contrôle du lancement des applications : 50 Mo.
      - Pour installer tous les composants Kaspersky Embedded Systems Security : 2 Go.
    - Mémoire vive :
      - 256 Mo pour installer uniquement le composant Contrôle du lancement des applications sur les périphériques tournant sous Microsoft Windows.
      - 512 Mo pour effectuer une installation complète de tous les composants.
    - Exigences du processeur :
      - pour les systèmes d'exploitation Microsoft Windows 32 bits :

Processeur monocœur 1,4 GHz

Intel® Pentium® III

- pour les systèmes d'exploitation Microsoft Windows 64 bits :

Processeur monocœur 1,4 GHz

Intel Pentium IV

- Configuration recommandée :
  - Espace disque requis :
    - Pour installer le composant Contrôle du lancement des applications : 2 Go.
    - Pour installer tous les composants Kaspersky Embedded Systems Security : 4 Go.
  - Mémoire vive : 1 Go.
  - Configuration du processeur : quadricœur 2,4 GHz
- Configuration matérielle requise pour un appareil fonctionnant sous le système d'exploitation Windows Embedded 7, Windows Embedded 8 ou Windows Embedded 10 :
  - Configuration minimale :
    - Espace disque requis :
      - Pour installer le composant Contrôle du lancement des applications : 50 Mo.
      - Pour installer tous les composants Kaspersky Embedded Systems Security : 2 Go.
    - Mémoire vive : 1 Go.
    - Configuration requise pour le processeur : processeur monocœur Intel Pentium IV de 1,4 GHz.
  - Configuration recommandée :
    - Espace disque requis :
      - Pour installer le composant Contrôle du lancement des applications : 2 Go.
      - Pour installer tous les composants Kaspersky Embedded Systems Security : 4 Go.
    - Mémoire vive : 1 Go.
    - Configuration du processeur : quadricœur 2,4 GHz
- Configuration matérielle requise pour un périphérique tournant sous Windows 7 (64 bits), Windows 8 (64 bits), Windows 10 (64 bits) ou Windows 11 (64 bits) :
  - Configuration minimale :
    - Espace disque requis :
      - Pour installer le composant Contrôle du lancement des applications : 50 Mo.

- Pour installer tous les composants Kaspersky Embedded Systems Security : 2 Go.

- Mémoire vive :
  - 1 Go pour installer uniquement le composant Contrôle du lancement des applications sur les périphériques tournant sous Microsoft Windows.
  - 2 Go pour effectuer une installation complète de tous les composants.
- Configuration requise pour le processeur : processeur monocœur Intel Pentium IV de 1,4 GHz.

- Configuration recommandée :
  - Espace disque requis :
    - Pour installer le composant Contrôle du lancement des applications : 2 Go.
    - Pour installer tous les composants Kaspersky Embedded Systems Security : 4 Go.
  - Mémoire vive :
    - 1 Go pour installer uniquement le composant Contrôle du lancement des applications sur les périphériques tournant sous Microsoft Windows.
    - 2 Go pour effectuer une installation complète de tous les composants.
  - Configuration du processeur : quadricœur 2,4 GHz

- Configuration matérielle requise pour un périphérique tournant sous Windows 7 (32 bits), Windows 8 (32 bits) ou Windows 10 (32 bits) :
  - Configuration minimale :
    - Espace disque requis :
      - Pour installer le composant Contrôle du lancement des applications : 50 Mo.
      - Pour installer tous les composants Kaspersky Embedded Systems Security : 2 Go.
    - Mémoire vive :
      - 256 Mo pour installer uniquement le composant Contrôle du lancement des applications sur les périphériques tournant sous Microsoft Windows.
      - 2 Go pour effectuer une installation complète de tous les composants.
    - Exigences du processeur :
      - pour les systèmes d'exploitation Microsoft Windows 32 bits :

        Processeur monocœur 1,4 GHz
        Intel Pentium III
      - pour les systèmes d'exploitation Microsoft Windows 64 bits :

        Processeur monocœur 1,4 GHz

Intel Pentium IV

- Configuration recommandée :
  - Espace disque requis :
    - Pour installer le composant Contrôle du lancement des applications : 2 Go.
    - Pour installer tous les composants Kaspersky Embedded Systems Security : 4 Go.
  - Mémoire vive : 1 Go.
  - Configuration du processeur : quadricœur 2,4 GHz

Exigences fonctionnelles et restrictions

Cette section décrit des exigences fonctionnelles supplémentaires et les restrictions existantes pour les modules de Kaspersky Embedded Systems Security.

Installation et désinstallation

Voici la liste des restrictions au niveau de l'installation et de la désinstallation :

- Pour que Kaspersky Embedded Systems Security fonctionne correctement, la prise en charge de SHA-2 sous Windows est requise.
- Lors de l'installation de l'application, un avertissement peut s'afficher à l'écran si le chemin d'accès au dossier d'installation saisi de Kaspersky Embedded Systems Security contient plus de 150 caractères. L'avertissement n'affecte pas le processus d'installation : vous pouvez installer et exécuter Kaspersky Embedded Systems Security.
- Si vous souhaitez installer le module prise en charge du protocole SNMP, assurez-vous de redémarrer le service SNMP si celui-ci est en cours d'exécution.
- Si vous souhaitez installer et exécuter Kaspersky Embedded Systems Security sur un appareil fonctionnant sous un système d'exploitation embarqué, assurez-vous d'installer le composant Gestionnaire de filtre.
- Vous ne pouvez pas installer les Outils d'administration de Kaspersky Embedded Systems Security via les stratégies de groupe Microsoft Active Directory®.
- Si vous excluez le nœud Protection antivirus de la liste des modules d'application installés, ce nœud disparaît de la liste des composants disponibles une fois l'installation terminée. Pour installer les composants du nœud Endpoint Protection, lancez l'Assistant d'installation depuis le paquet d'installation, car celui-ci contient une liste complète des composants.
- Si la Console d'administration de Kaspersky Embedded Systems Security est installée, l'Assistant d'installation peut vous inviter à redémarrer l'ordinateur. Dans ce cas, le redémarrage n'est pas obligatoire. Il suffit de fermer la session de l'utilisateur qui a installé la Console d'Administration et de se connecter à nouveau au système.
- Si vous installez l'application sur des appareils protégés tournant sous des systèmes d'exploitation plus anciens qui ne peuvent pas recevoir les mises à jour régulières, assurez-vous que les certificats racines suivants sont

installés :

- Autorité de certification racine DigiCert ID garanti
- DigiCert_High_Assurance_EV_Root_CA
- DigiCertAssuredIDRootCA

Si les certificats racine indiqués ne sont pas installés, l'application peut ne pas fonctionner correctement. Nous vous recommandons d'installer les certificats dès que possible.

Moniteur d'intégrité des fichiers

Par défaut, le Contrôle de l'intégrité des fichiers ne contrôle pas les modifications réalisées dans les dossiers système ou dans les fichiers d'entretien du système de fichiers afin de ne pas encombrer les rapports relatifs aux tâches avec des informations relatives aux modifications de routine réalisées en permanence par le système d'exploitation. Vous ne pouvez pas inclure ces dossiers dans la zone de surveillance.

Les dossiers et fichiers suivants sont exclus de la zone de surveillance :

- Fichiers d'entretien NTFS porteurs de l'identifiant de 0 à 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\

- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

L'application exclut les dossiers du niveau supérieur.

Le composant ne surveille pas les modifications de fichiers qui contournent le système de fichiers ReFS/NTFS (les modifications de fichier sont réalisées via BIOS, LiveCD, etc.)

Gestion du pare-feu

Voici la liste des restrictions pour la Gestion du pare-feu :

- Vous devez indiquer plusieurs adresses. Sinon, l'utilisation avec IPv6 n'est pas disponible.
- Les règles prédéfinies de stratégie du Pare-feu prennent en charge des scénarios d'interaction de base entre les appareils protégés et le Serveur d'administration. Pour exploiter totalement les fonctions de Kaspersky Security Center, il faut configurer les règles de port. Vous trouverez les informations relatives aux numéros de port, aux protocoles et à leurs fonctions dans la Base de connaissances de Kaspersky Security Center.
- Une fois que vous avez installé l'application et configuré les règles de la tâche, l'application contrôle la modification des règles et des groupes de règles du Pare-feu Windows au lancement de la tâche Gestion du pare-feu. Pour mettre à jour l'état et ajouter les règles requises, assurez-vous de redémarrer la tâche Gestion du pare-feu.
- Lorsque la tâche Gestion du pare-feu est lancée, les règles de refus et les règles de surveillance du trafic sortant sont automatiquement supprimées des paramètres du pare-feu du système d'exploitation.

Autres restrictions

Limitations des tâches **Analyse à la demande** et **Protection des fichiers en temps réel** :

- L'analyse des appareils MTP connectés n'est pas disponible.
- L'analyse des archives n'est pas disponible sans l'analyse des archives SFX : si l'analyse des archives est activée dans les paramètres de protection de Kaspersky Embedded Systems Security, l'application analyse automatiquement les objets dans les archives et les archives SFX. L'analyse des archives SFX est disponible sans l'analyse des archives.
- Si la case **Analyse plus profonde du lancement de processus (le lancement de processus est bloqué jusqu'à la fin de l'analyse)** est cochée et que le service **Utilisation du KSN**est activé simultanément, tout processus lancé qui reçoit l'adresse Internet comme argument sera bloqué, même si le mode Statistiques seulement a été choisi. Pour éviter de bloquer le processus, veuillez choisir l'une des options suivantes :
  - Désactivez le service **Utilisation du KSN**
  - Décochez la case **Analyse plus profonde du lancement de processus (le lancement de processus est bloqué jusqu'à la fin de l'analyse)**

  Option recommandée : décochez la case Analyse approfondie des processus de lancement

Licence :

- Vous ne pouvez pas activer l'application avec une clé via l'assistant d'installation si la clé a été créée à l'aide de la commande SUBST ou si le chemin d'accès au fichier clé est un chemin de réseau.

- Si vous prévoyez d'utiliser le serveur proxy de Kaspersky Security Center pour activer le produit sur un appareil client, désactivez l'optimisation VDI sur cet appareil lors de l'installation de l'Agent d'administration de Kaspersky Security Center.

Mises à jour :

- Par défaut, l'icône de l'application est masquée après l'installation des mises à jour critiques des modules Kaspersky Embedded Systems Security.

- KLRAMDISK n'est pas pris en charge sur les périphériques protégés tournant sous Windows XP ou Windows Server® 2003.

Interface :

- Dans la console de l'application, le filtrage dans la Quarantaine, la Sauvegarde, le journal d'audit système ou le journal d'exécution de la tâche est sensible à la case.

- Lors de configuration d'une zone de protection ou d'analyse dans la console de l'application, vous ne pouvez utiliser qu'un seul masque et uniquement à la fin du chemin. Voici quelques exemples de masque correct : "C:\Temp\Temp*", or "C:\Temp\Temp???.doc" et "C:\Temp\Temp*.doc". Cette restriction n'a aucun impact sur la configuration de la Zone de confiance.

Sécurité :

- Si la fonction de contrôle des comptes utilisateur est activée dans les paramètres du système d'exploitation, un compte utilisateur doit appartenir au groupe KAVWSEE Administrators pour pouvoir ouvrir la Console de l'application d'un double clic sur l'application de l'icône dans la zone de notification de la barre d'état. Dans le cas contraire, il sera nécessaire de vous connecter en tant qu'utilisateur autorisé à ouvrir l'interface de diagnostic compacte ou le composant logiciel enfichable Microsoft Management Console.

- Si le Contrôle de compte d'utilisateur est activé, vous ne pouvez pas désinstaller l'application via la fenêtre Programmes et fonctionnalités de Microsoft Windows.

Intégration à Kaspersky Security Center :

- Lors de la réception des paquets de mise à jour, le Serveur d'administration vérifie les mises à jour des bases de données avant de les envoyer aux appareils protégés du réseau. Le Serveur d'administration ne vérifie pas les mise à jour des modules de l'application.

- Assurez-vous que les cases requises sont cochées dans les paramètres Interaction avec le Serveur d'administration quand vous utilisez des composants qui transmettent les données dynamiques à Kaspersky Security Center à l'aide des listes réseau (Quarantaine, Sauvegarde).

Protection contre les exploits :

- La Protection contre les exploits n'est pas disponible si les bibliothèques apphelp.dll ne sont pas chargées dans la configuration d'environnement actuelle.

- Le composant Protection contre les exploits est incompatible avec l'utilitaire EMET de Microsoft sur les appareils protégés tournant sous le système d'exploitation Microsoft Windows 10 : Kaspersky Embedded Systems Security bloque EMET si le composant Protection contre les exploits est installé sur un appareil protégé doté d'EMET.

- Le composant Protection contre les exploits est incompatible avec le moteur de base de données SQL Server® 2012. Si vous installez Kaspersky Embedded Systems Security sur l'ordinateur doté de MS SQL Server 2012, vous devez ajouter la bibliothèque sqlos.dll du serveur de base de données à la liste des exclusions dans la tâche Protection contre les exploits.

Installation et suppression de l'application

Cette section explique pas à pas la procédure d'installation et de désinstallation de Kaspersky Embedded Systems Security.

Codes des composants logiciel de Kaspersky Embedded Systems Security pour le service Windows Installer

Les fichiers \product_long_term\ess_x86.msi et \product_long_term\ess_x64.msi sont conçus pour installer la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut** de Kaspersky Embedded Systems Security, tandis que les fichiers \product\ess_x86.msi et \product\ess_x64.msi sont prévus pour installer la configuration **Protéger l'ordinateur avec les base antivirus** Kaspersky Embedded Systems Security.

Si la configuration Protéger l'ordinateur avec des bases antivirus est sélectionnée, tous les composants de Kaspersky Embedded Systems Security sont inclus par défaut à l'exception des composants Gestion du pare-feu et Compteurs de performance.

Lorsque vous installez la configuration Protéger l'ordinateur avec les bases antivirus de Kaspersky Embedded Systems Security sur une version de l'application qui n'utilise pas l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement enrichi via l'ajout des composants suivants :

- Protection des fichiers en temps réel
- Analyse à la demande
- Protection contre les menaces réseau

Les composants qui permettent les mises à jour ne sont pas inclus dans la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut.

Si la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut est sélectionnée, les composants suivants sont inclus par défaut :

- Core
- Protection contre les exploits
- Contrôle du lancement des applications
- Icône de la barre d'état système

Lorsque vous installez la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut de Kaspersky Embedded Systems Security sur une version de l'application qui utilise l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement réduit via l'élimination des composants suivants :

- Protection des fichiers en temps réel
- Analyse à la demande
- Les composants qui permettent les mises à jour

Cette configuration est recommandée pour protéger les systèmes aux ressources limitées. Dans ce cas, vous pouvez activer l'application à long terme et le composant Contrôle du lancement des applications assure la protection de l'ordinateur.

Les fichiers \console\esstools_x86.msi et \console\esstools_x64.msi installent tous les composants logiciels de la sélection "Outils d'administration".

Les rubriques suivantes indiquent les codes des composants de Kaspersky Embedded Systems Security pour le service Windows Installer. Vous pouvez utiliser les codes du composant dans le but de définir la liste des composants à installer lors de l'installation de Kaspersky Embedded Systems Security via la ligne de commande.

Composants logiciels de Kaspersky Embedded Systems Security

Le tableau suivant contient les codes et les descriptions des composants logiciels de Kaspersky Embedded Systems Security.

Description des composants logiciels de Kaspersky Embedded Systems Security

Composant	Identifiant	Fonction exécutée
Fonction principale	Core	Ce composant contient une sélection de fonctions de base de l'application et garantit leur fonctionnement. Si d'autres modules Kaspersky Embedded Systems Security sont spécifiés lors de l'installation de Kaspersky Embedded Systems Security à partir de la ligne de commande, mais que le composant Core n'est pas spécifié, le composant Core est installé automatiquement.
Contrôle du lancement des	AppCtrl	Ce composant surveille les tentatives des utilisateurs de lancer des applications et autorise ou interdit le lancement des applications

applications		conformément aux règles spécifiées du Contrôle du lancement des applications. Le composant intervient dans la tâche Contrôle du lancement des applications.
Contrôle des périphériques	DevCtrl	Ce composant suit les tentatives de connexion d'appareils externes à un appareil protégé et autorise ou interdit l'utilisation de ces appareils conformément aux règles de contrôle des périphériques spécifiées. Le composant intervient dans la tâche Contrôle des périphériques.
Protection antivirus	AVProtection	Ce composant garantit la protection antivirus et reprend les composants suivants : • Analyse à la demande • Protection des fichiers en temps réel • Protection contre les menaces réseau
Protection contre les menaces réseau	IDS	Ce composant analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau ciblant votre ordinateur, Kaspersky Embedded Systems Security bloque l'activité réseau de l'ordinateur attaquant.
Analyse à la demande	Ods	Ce composant installe les fichiers système de Kaspersky Embedded Systems Security et propose des tâches d'analyse à la demande (analyse à la demande des objets sur l'appareil protégé).
Protection des fichiers en temps réel	Oas	Ce composant réalise les recherches de virus sur les fichiers sur l'appareil protégé lorsque ces fichiers sont sollicités. Le composant exécute la tâche Protection des fichiers en temps réel.
Utilisation de Kaspersky Security Network	Ksn	Ce composant offre une protection sur la base des technologies cloud de Kaspersky. Le composant exécute la tâche Utilisation du KSN (envoi de requêtes au Service Kaspersky Security Network et réception des conclusions de ce même Service Kaspersky Security Network).
Moniteur d'intégrité des fichiers	Fim	Ce composant permet de consigner les opérations réalisées sur les fichiers dans la zone de surveillance sélectionnée. Le composant intervient dans la tâche Moniteur d'intégrité des fichiers.
Moniteur d'accès au registre	RegMonitor	Ce composant permet de surveiller les actions exécutées avec les branches de registre et les clés indiquées dans les zones de surveillance définies dans les paramètres de la tâche. Le composant met en oeuvre le Moniteur d'accès au registre.
Protection contre les exploits	AntiExploit	Ce composant garantit l'administration des paramètres de la protection des processus dans la mémoire de l'appareil protégé.
Gestion du pare-feu	Pare-feu	Ce composant permet de gérer le Pare-feu Windows via l'interface utilisateur graphique de Kaspersky Embedded Systems Security. Le composant intervient dans la tâche Gestion du pare-feu.

Module d'intégration de l'Agent d'administration de Kaspersky Security Center	AKIntegration	Ce composant assure la connexion entre Kaspersky Embedded Systems Security et l'Agent d'administration de Kaspersky Security Center. Vous pouvez installer ce composant sur l'appareil protégé si vous avez l'intention d'administrer l'application via Kaspersky Security Center.
Inspection des journaux	LogInspector	Le composant contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.
Sélection de compteurs de performance de l'application "System Monitor"	PerfMonCounters	Le composant installe la sélection de compteurs de performance de l'application "System Monitor". Les compteurs de performance permettent de mesurer les performances de Kaspersky Embedded Systems Security et de localiser les goulots d'étranglement potentiels sur l'appareil protégé lorsque Kaspersky Embedded Systems Security est utilisé avec d'autres applications.
Prise en charge du protocole SNMP	SnmpSupport	Ce composant publie les compteurs et les interruptions de Kaspersky Embedded Systems Security via le protocole SNMP (Simple Network Management Protocol) sous Microsoft Windows. Ce composant peut être installé sur l'appareil protégé uniquement si le service Microsoft SNMP est installé sur le même appareil protégé.
Icône de Kaspersky Embedded Systems Security dans la zone de notification	TrayApp	Ce composant affiche l'icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches de l'appareil protégé. L'icône Kaspersky Embedded Systems Security affiche l'état de la protection de l'appareil et permet d'ouvrir la Console de Kaspersky Embedded Systems Security dans Microsoft Management Console (si elle est installée) et la fenêtre **A propos de l'application**.

Composant logiciel "Outils d'administration"

Le tableau suivant contient le code et la description du composant logiciel "Outils d'administration".

Description du composant logiciel "Outils d'administration"

Composant	Code	Fonctions du composant
Composant logiciel enfichable de Kaspersky Embedded Systems Security	MmcSnapin	Le composant installe le composant logiciel enfichable Microsoft Management Console pour administrer l'application via la Console de Kaspersky Embedded Systems Security. Si lors de l'installation de la sélection "Outils d'administration" via la ligne de commande vous désignez d'autres composants de la sélection sans le composant MmcSnapin, celui-ci sera installé automatiquement.

Modifications introduites dans le système après l'installation de Kaspersky Embedded Systems Security

Lors de l'installation de Kaspersky Embedded Systems Security et de la sélection d'« Outils d'administration » (y compris la Console de l'application), le service Windows Installer procède aux modifications suivantes sur le périphérique protégé :

- création des dossiers de Kaspersky Embedded Systems Security sur le périphérique protégé et sur le périphérique protégé sur lequel la Console de l'application est installée .
- enregistrement des services Kaspersky Embedded Systems Security ;
- création d'un groupe d'utilisateurs de Kaspersky Embedded Systems Security.
- Les clés de Kaspersky Embedded Systems Security sont enregistrées dans la base de registres.

Ces modifications sont décrites ci-dessous.

Dossiers de Kaspersky Embedded Systems Security sur un périphérique protégé

Suite à l'installation de Kaspersky Embedded Systems Security, les dossiers suivants sont créés sur un périphérique protégé :

- Le dossier d'installation par défaut de Kaspersky Embedded Systems Security contenant les fichiers exécutables de Kaspersky Embedded Systems Security dépend de la version (bits) du système d'exploitation. Par conséquent, les dossiers d'installation par défaut sont les suivants :
  - Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Les fichiers Management Information Base (MIB) contenant une description des compteurs et les pièges publiés par Kaspersky Embedded Systems Security selon le protocole SNMP :
  - %Kaspersky Embedded Systems Security%\mibs
- Version 64 bits des fichiers exécutables de Kaspersky Embedded Systems Security (le dossier est créé uniquement lors de l'installation de Kaspersky Embedded Systems Security sur une version 64 bits de Microsoft Windows) :
  - %Kaspersky Embedded Systems Security%\x64
- Fichiers de service de Kaspersky Embedded Systems Security :
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Dskm

  Pour Windows XP, le chemin d'accès au dossier de Kaspersky Lab est %ALLUSERSPROFILE%\Application Data
- Fichiers contenant les paramètres pour les sources de mise à jour :

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update

- Mises à jour des bases de données et des modules logiciels récupérés à l'aide de la tâche Copie des mises à jour (le dossier est créé à la première réception des mises à jour à l'aide de la tâche Copie des mises à jour).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Update\Distribution

- Journaux d'exécution de la tâche et journal d'audit système.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Reports

- Ensemble de bases de données utilisées actuellement.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Current

- Copies de sauvegarde des bases ; elles sont écrasées à chaque mise à jour des bases de données.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Backup

- Fichiers temporaires créés lors de l'exécution des tâches de mise à jour.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Bases\Temp\

- Objets en quarantaine (dossier par défaut).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Quarantine

- Objets dans la sauvegarde (dossier par défaut).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Backup

- Objets restaurés de la sauvegarde ou de la quarantaine (dossier par défaut pour les objets restaurés).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Restored

Dossier créé lors de l'installation de la Console de l'application

Les dossiers d'installation par défaut de la Console de l'application contenant les fichiers "Outils d'administration dépendent de la version (bits) du système d'exploitation. Par conséquent, les dossiers d'installation par défaut sont les suivants :

- Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Services de Kaspersky Embedded Systems Security

Les services de Kaspersky Embedded Systems Security suivants sont lancés sous le compte utilisateur Système local (SYSTEM) :

- Service Kaspersky Security (KAVFS) : service essentiel de Kaspersky Embedded Systems Security qui gère les tâches et les flux de travail de Kaspersky Embedded Systems Security.

- Service Kaspersky Security Management (KAVFSGT) : ce service est destiné à l'administration de l'application Kaspersky Embedded Systems Security via la Console de l'application.

- Service Kaspersky Security Exploit Prevention : service qui agit en tant qu'intermédiaire de communication des paramètres de sécurité aux agents de sécurité externes et de réception des données relatives aux événements de sécurité.

Groupe Kaspersky Embedded Systems Security

Administrateurs ESS désigne un groupe sur le périphérique protégé dont les utilisateurs ont un accès total au service Kaspersky Security Management et à toutes les fonctions de Kaspersky Embedded Systems Security.

Clés de la base de registres système

L'installation de Kaspersky Embedded Systems Security s'accompagne de la création des clés de la base de registres système suivantes :

- Propriétés de Kaspersky Embedded Systems Security : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Paramètres du journal des événements de Kaspersky Embedded Systems Security (journal des événements de Kaspersky) : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Propriétés du service d'administration de Kaspersky Embedded Systems Security : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Paramètres des compteurs de performance :
  - Sur la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - Sur la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Paramètres du composant « prise en charge du protocole SNMP » :
  - Sur la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\SnmpAgent]
  - Sur la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\SnmpAgent]
- Paramètres du fichier dump :
  - Sur la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\CrashDump]
  - Sur la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\CrashDump]
- Paramètres du fichier de trace :
  - Sur la version 32 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\Trace]
  - Sur la version 64 bits de Microsoft Windows : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\Trace]
- Configuration des tâches et des fonctions de l'application : [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\Environment]

Processus de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security lance les processus décrits dans le tableau ci-dessous.

Processus de Kaspersky Embedded Systems Security

Nom du fichier	Fonction
kavfswp.exe	Flux de travail de Kaspersky Embedded Systems Security
kavtray.exe	Processus de l'icône dans la barre d'état système
kavfsmui.exe	Processus du composant Interface de diagnostic compacte
kavshell.exe	Processus de l'utilitaire de la ligne de commande
kavfsrcn.exe	Processus d'administration à distance Kaspersky Embedded Systems Security
kavfs.exe	Processus du Service Kaspersky Security
kavfsgt.exe	Processus du Service Kaspersky Security Management
kavfswh.exe	Processus du service Kaspersky Security Exploit Prevention Management

Paramètres d'installation et de désinstallation et options de ligne de commande correspondantes pour le service Windows Installer

Cette section décrit les paramètres d'installation et de désinstallation de Kaspersky Embedded Systems Security ainsi que leur valeur par défaut. Elle renseigne également les arguments pour modifier les valeurs des paramètres d'installation et leurs valeurs possibles. Vous pouvez utiliser ces arguments avec les arguments standard de l'instruction `msiexec` du service Windows Installer lors de l'installation de Kaspersky Embedded Systems Security via la ligne de commande.

Paramètres de d'installation et options de ligne de commande dans Windows Installer

- Acceptation des termes du Contrat de licence utilisateur final : il faut accepter les dispositions pour installer Kaspersky Embedded Systems Security.

  Les valeurs qui peuvent être attribuées au paramètre `EULA=<value>` dans la ligne de commande sont les suivantes :

  - `0` : vous n'acceptez pas les termes du Contrat de licence utilisateur final.
  - `1` : vous acceptez les termes du Contrat de licence utilisateur final.

- Acceptation des termes de la Politique de confidentialité : il faut accepter les dispositions pour installer Kaspersky Embedded Systems Security.

  Les valeurs qui peuvent être attribuées au paramètre `PRIVACYPOLICY=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` : vous n'acceptez pas les termes de la Politique de confidentialité (valeur par défaut).
  - `1` : vous acceptez les termes de la Politique de confidentialité.

- Autorisez l'installation de Kaspersky Embedded Systems Security si la mise à jour KB4528760 n'est pas installée. Pour en savoir plus sur la mise à jour KB4528760, veuillez visiter le site Web de Microsoft.

  Les valeurs qui peuvent être attribuées au paramètre `SKIPCVEWINDOWS10=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` : annule l'installation de Kaspersky Embedded Systems Security si la mise à jour KB4528760 n'est pas installée (valeur par défaut).
  - `1` : autorise l'installation de Kaspersky Embedded Systems Security si la mise à jour KB4528760 n'est pas installée.

  La mise à jour KB4528760 corrige la vulnérabilité de sécurité CVE-2020-0601. Pour en savoir plus sur la vulnérabilité de sécurité CVE-2020-0601, veuillez visiter le site Web de Microsoft.

- Installation de Kaspersky Embedded Systems Security avec les paramètres définis restaurés de la version précédente lors de la mise à jour.

  Les valeurs qui peuvent être attribuées au paramètre RESTOREDEFSETTINGS=<valeur> dans la ligne de commande sont les suivantes :

  - `0` : toutes les données de la version précédente sont transférées vers une nouvelle version lors de la mise à jour (valeur par défaut).
  - `1` : seul le fichier contenant les données d'activation et les clés privées est transféré vers une nouvelle version lors de la mise à jour ([lecteur]:\ProgramData\Kaspersky Lab\<product>\<version>\Data\product.dat). Toutes les autres données de la version précédente, telles que les paramètres, les bases antivirus, les rapports, les objets de quarantaine et de sauvegarde, sont supprimées.

- Installation de Kaspersky Embedded Systems Security avec les rapports conservés des versions précédentes lors de la mise à jour.

  Les valeurs qui peuvent être attribuées au paramètre KEEP_REPORTS=<valeur> dans la ligne de commande sont les suivantes :

  - `0` : toutes les données de la version précédente sont transférées dans la nouvelle version lors de la mise à jour, à l'exception des rapports ([lecteur]:\ProgramData\Kaspersky Lab\<product>\<version>\Reports). Les rapports sont supprimés.
  - `1` : toutes les données de la version précédente, telles que les paramètres, les bases antivirus, les rapports, les objets de quarantaine et de sauvegarde, sont transférées dans une nouvelle version lors de la mise à jour (valeur par défaut).

- Installation de Kaspersky Embedded Systems Security avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux.

  Les valeurs qui peuvent être attribuées au paramètre `PRESCAN=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` : ne pas effectuer d'analyse préliminaire des processus actifs et des secteurs d'amorçage des disques locaux pendant l'installation (valeur par défaut).
  - `1` : effectuer une analyse préliminaire des processus actifs et des secteurs d'amorçage des disques locaux pendant l'installation.

- Dossier d'installation dans lequel les fichiers de Kaspersky Embedded Systems Security vont être enregistrés lors de son installation. Vous pouvez indiquer un autre dossier.

Les valeurs par défaut attribuées au paramètres `INSTALLDIR=<chemin d'accès complet au dossier>` via la ligne de commande sont les suivantes :

- Kaspersky Embedded Systems Security : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Outils d'administration : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- Dans la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%

- La tâche Protection des fichiers en temps réel démarre immédiatement après le démarrage de Kaspersky Embedded Systems Security. Activez ce paramètre pour démarrer la Protection des fichiers en temps réel lorsque Kaspersky Embedded Systems Security démarre (recommandé).

  Les valeurs qui peuvent être attribuées au paramètre `RUNRTP=<valeur>` dans la ligne de commande sont les suivantes :

  - `1` – lancement (valeur par défaut).
  - `0` : ne pas démarrer.

- Objets exclus de la zone de protection conformément aux recommandations de Microsoft Corporation. Dans la tâche Protection des fichiers en temps réel sont exclus de la zone de protection les objets de l'appareil dont l'exclusion est recommandée par Microsoft Corporation. Certaines applications sur l'appareil protégé peuvent devenir instables lorsqu'une application antivirus intercepte ou modifie les fichiers auxquels ces fichiers qu'elles utilisent. Ainsi, Microsoft Corporation inclus certains logiciels chargés du contrôle des domaines dans cette catégorie.

  Les valeurs qui peuvent être attribuées au paramètre `ADDMSEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

  - `1` – exclusion (valeur par défaut).
  - `0` : ne pas exclure.

- Objets exclus de la zone de protection conformément aux recommandations de Kaspersky. Dans la tâche Protection des fichiers en temps réel, les objets du périphérique dont l'exclusion est recommandée par Kaspersky sont exclus de la zone de protection.

  Les valeurs qui peuvent être attribuées au paramètre `ADDKLEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

  - `1` – exclusion (valeur par défaut).
  - `0` : ne pas exclure.

- Autoriser les connexions à distance à la console de l'application. Par défaut, la connexion à distance à la console de l'application installée sur l'appareil protégé n'est pas autorisée. Vous pouvez autoriser cette connexion pendant l'installation. Kaspersky Embedded Systems Security crée les règles d'autorisation pour le processus kavfsgt.exe sur le protocole TCP pour tous les ports.

  Les valeurs qui peuvent être attribuées au paramètre `ALLOWREMOTECON=<valeur>` dans la ligne de commande sont les suivantes :

  - `1` : autoriser.
  - `0` – interdire (valeur par défaut).

- Chemin d'accès au fichier clé (`LICENSEKEYPATH`
)

  . Par défaut, Windows Installer tente de trouver le fichier avec l'extension .key dans le dossier \product du kit de distribution. Si le dossier \product contient plusieurs fichiers clés, Windows Installer choisit le fichier clé qui possède la date de fin de validité la plus lointaine. Vous pouvez enregistrer au préalable le fichier clé dans le répertoire \product ou indiquer un autre chemin d'accès au fichier clé à l'aide du paramètre **Ajouter une clé**. Vous pouvez ajouter une clé après l'installation de Kaspersky Embedded Systems Security à l'aide de l'outil d'administration que vous aurez choisi, par exemple via la console de l'application. Si vous n'ajoutez pas la clé de l'application lors de son installation, Kaspersky Embedded Systems Security ne fonctionnera pas.

- Chemin d'accès au fichier de configuration. Kaspersky Embedded Systems Security importe les paramètres depuis le fichier de configuration indiqué et créé dans l'application. Kaspersky Embedded Systems Security n'importe pas les mots de passe contenus dans le fichier de configuration tels que les mots de passe des comptes utilisateur de lancement de tâches ou les mots de passe de connexion au serveur proxy. Après l'importation des paramètres, vous devrez saisir tous les mots de passe manuellement. Si vous ne désignez pas le fichier de configuration, Kaspersky Security for Windows Server fonctionnera après l'installation selon les paramètres par défaut.

  La valeur pour le paramètre `CONFIGPATH=<nom du fichier de configuration>` n'est pas définie.

- Mode de la tâche **Analyse au démarrage du système d'exploitation** (SCANSTARTUP_BLOCKING). Si vous installez Kaspersky Embedded Systems Security en mode d'installation sans la clé SCANSTARTUP_BLOCKING, les valeurs suivantes sont attribuées au paramètre **Zone d'analyse** de la tâche **Analyse au démarrage du système d'exploitation** :

  - **Actions à exécuter sur les objets infectés et autres : informer uniquement**
  - **Actions à exécuter sur les objets probablement infectés : informer uniquement**

  Si vous installez Kaspersky Embedded Systems Security en mode d'installation à l'aide de la clé SCANSTARTUP_BLOCKING, les valeurs suivantes sont attribuées au paramètre **Zone d'analyse** de la tâche **Analyse au démarrage du système d'exploitation** :

  - **Actions à exécuter sur les objets infectés et autres : exécuter l'action recommandée**
  - **Actions à exécuter sur les objets probablement infectés : exécuter l'action recommandée**

  La tâche **Analyse au démarrage du système d'exploitation** est créée automatiquement. Par défaut, le mode **Informer uniquement** est appliqué. Dans ce cas, après avoir déployé Kaspersky Embedded Systems Security sur les appareils, vous pouvez activer la tâche **Analyse au démarrage du système d'exploitation** si aucun problème avec les services système n'a été détecté lors de l'analyse. Si l'application détecte des services système critiques infectés ou des objets probablement infectés, le mode **Informer uniquement** vous donne le temps d'en trouver la raison et de résoudre le problème. Si l'application applique le mode **Exécuter l'action recommandée**, qui évoque l'action **Désinfecter. Supprimer si la désinfection est impossible**, la désinfection ou la suppression des fichiers système peut entraîner des problèmes critiques au démarrage du système d'exploitation.

- L'Autorisation des connexions de réseau pour la Console de l'application permet d'installer la Console de Kaspersky Embedded Systems Security sur un autre périphérique. Grâce à la console de Kaspersky Embedded Systems Security installée sur un autre périphérique, vous pourrez administrer la protection d'un ordinateur à distance. Le port TCP 135 est ouvert dans le pare-feu de Microsoft Windows, les connexions réseau sont autorisées pour le fichier exécutable du processus d'administration à distance de Kaspersky Embedded Systems Security kavfsrcn.exe et l'accès aux applications DCOM est ouvert. Une fois l'installation terminée, ajoutez les utilisateurs au groupe ESS Administrators pour leur permettre d'administrer l'application à distance et autorisez les connexions au Service Kaspersky Security Management (kavfsgt.exe) sur le périphérique protégé. Vous pouvez lire des informations complémentaires sur la configuration quand la Console de Kaspersky Embedded Systems Security est installée sur un autre périphérique.

Les valeurs qui peuvent être attribuées au paramètre `ADDWFEXCLUSION=<valeur>` dans la ligne de commande sont les suivantes :

- `1` : autoriser.
- `0` – interdire (valeur par défaut).

- Désactivation de la recherche d'une application non compatible. Ce paramètre permet d'activer ou de désactiver la recherche d'applications incompatibles lors de l'installation en arrière-plan de l'application sur l'appareil protégé. Quelle que soit la valeur de ce paramètre, lors de l'installation de Kaspersky Embedded Systems Security, l'application signale toujours l'installation d'autres versions de l'application sur l'appareil protégé.

  Les valeurs qui peuvent être attribuées au paramètre `SKIPINCOMPATIBLESW=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` : la recherche d'applications incompatibles a lieu (valeur par défaut).
  - `1` : la recherche d'applications non compatibles n'a pas lieu.

Paramètres de désinstallation et options de ligne de commande dans Windows Installer

- Restauration du contenu de la quarantaine.

  Les valeurs qui peuvent être attribuées au paramètre `RESTOREQTN=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` – suppression du contenu en quarantaine (valeur par défaut).
  - `1` : restaurer le contenu de la quarantaine dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \Quarantine.

- Restauration du contenu de la Sauvegarde.

  Les valeurs qui peuvent être attribuées au paramètre `RESTOREBCK=<valeur>` dans la ligne de commande sont les suivantes :

  - `0` – suppression du contenu de la sauvegarde (valeur par défaut).
  - `1` : restaurer le contenu de la Sauvegarde dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \Backup.

- Saisie du mot de passe actif pour la confirmation de l'opération de désinstallation (lorsque la protection par mot de passe est activée).

  La valeur par défaut pour le paramètre `UNLOCK_PASSWORD=<mot de passe défini>` n'est pas définie.

- Dossier pour la restauration des objets. Les objets restaurés seront enregistrés dans le dossier spécifié.

  La valeur par défaut pour l'option `RESTOREPATH=<chemin d'accès complet au dossier>` de la ligne de commande est %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Restored

Journaux d'installation et de désinstallation de Kaspersky Embedded Systems Security

Si vous installez ou désinstallez Kaspersky Embedded Systems Security à l'aide de l'Assistant d'installation (Désinstallation), le service Windows Installer crée le journal d'installation (de désinstallation). Un fichier journal est enregistré sous le nom ess_v3.2_install_<uid>.log (où <uid> désigne un identifiant unique de 8 caractères) dans le dossier %temp% pour l'utilisateur sous le compte duquel le fichier setup.exe a été lancé.

Si vous exécutez l'option **Modify or Remove** de la Console de l'application ou Kaspersky Embedded Systems Security à partir du menu **Démarrer**, le fichier journal ess_3.2_maintenance.log est automatiquement créé dans le dossier %temp%.

Si vous installez ou désinstallez Kaspersky Embedded Systems Security via la ligne de commande, le fichier journal d'installation n'est pas créé par défaut.

Pour installer Kaspersky Embedded Systems Security et créer le fichier journal sur le disque C:\, exécutez l'instruction suivante :

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Planification de l'installation

Cette section décrit la sélection d'outils d'administration de Kaspersky Embedded Systems Security, les particularités de l'installation et de la suppression de Kaspersky Embedded Systems Security à l'aide d'un assistant, via la ligne de commande, via Kaspersky Security Center et via une stratégie de groupe Active Directory.

Avant de lancer l'installation de Kaspersky Embedded Systems Security, il convient de préparer les principales étapes de la procédure.

1. Définissez les outils d'administration que vous utiliserez pour administrer et configurer Kaspersky Embedded Systems Security.
2. Déterminez les composants d'application requis à installer.
3. Sélectionnez le mode d'installation.

Sélection des outils d'administration

Définissez les outils d'administration que vous utiliserez pour la configuration des paramètres de Kaspersky Embedded Systems Security et son administration. En guise d'outils d'administration de Kaspersky Embedded Systems Security, vous pouvez choisir la console de l'application, l'utilitaire de ligne de commande ou la console d'administration de Kaspersky Security Center.

Console de Kaspersky Embedded Systems Security

La console de Kaspersky Embedded Systems Security est un composant logiciel enfichable autonome qui est ajouté à la console Microsoft Management Console. Il est possible d'administrer Kaspersky Embedded Systems Security via la Console de l'application installée sur le périphérique protégé ou sur tout autre périphérique du réseau de l'organisation.

Dans une des consoles Microsoft Management Console, ouverte en mode auteur, vous pouvez ajouter plusieurs composants logiciels enfichables Kaspersky Embedded Systems Security afin de pouvoir administrer ainsi la protection de plusieurs périphériques sur lesquels Kaspersky Embedded Systems Security est installé.

La Console de l'application fait partie des composants d'application "Outils d'administration".

Utilitaire de la ligne de commande

Vous pouvez administrer Kaspersky Embedded Systems Security via la ligne de commande du périphérique protégé.

L'utilitaire de ligne de commande fait partie des composants logiciels de Kaspersky Embedded Systems Security.

Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center afin de centraliser l'administration de la protection antivirus des périphériques de votre entreprise, vous pourrez administrer Kaspersky Embedded Systems Security via la Console d'administration Kaspersky Security Center.

Il faudra installer les composants suivants :

- **Module d'intégration de l'Agent d'administration de Kaspersky Security Center**. Ce composant fait partie des composants logiciels de Kaspersky Embedded Systems Security. Il garantit la communication entre Kaspersky Embedded Systems Security et l'Agent d'administration. Installez le module d'intégration à l'Agent d'administration Kaspersky Security Center sur l'appareil protégé.

- **Agent d'administration de Kaspersky Security Center**. Installez-le sur chaque appareil protégé. Ce composant garantit l'interaction entre la copie de Kaspersky Embedded Systems Security sur le périphérique protégé et la Console d'administration de Kaspersky Security Center. Le fichier d'installation de l'Agent d'administration fait partie du kit de distribution de Kaspersky Security Center.

- **Plug-in d'administration de Kaspersky Embedded Systems Security 3.2**. De plus, sur le périphérique protégé où est installé le Serveur d'administration de Kaspersky Security Center, installez le plug-in Kaspersky Embedded Systems Security pour pouvoir administrer l'application via la Console d'administration. Il s'agit de l'interface d'administration de l'application via Kaspersky Security Center. Le fichier d'installation du plug-in d'administration, \product\klcfginst.exe, fait partie du kit de distribution de Kaspersky Embedded Systems Security.

Sélection du type d'installation

Après avoir sélectionné les composants logiciels pour l'installation de Kaspersky Embedded Systems Security, sélectionnez la méthode d'installation de l'application.

Sélectionnez le mode d'installation en fonction de l'architecture du réseau et des conditions suivantes :

- Que vous ayez besoin de paramètres d'installation spéciaux pour Kaspersky Embedded Systems Security ou des paramètres recommandés.

- Paramètres d'installation identiques pour tous les appareils protégés ou propres à chaque appareil protégé ?

Vous pouvez installer Kaspersky Embedded Systems Security à l'aide d'un assistant Installation ou en mode silencieux en exécutant le package d'installation selon les paramètres d'installation via la ligne de commande. Vous pouvez réaliser une installation centralisée à distance de Kaspersky Embedded Systems Security via les stratégies de groupe Active Directory ou à l'aide d'une tâche d'installation à distance de Kaspersky Security Center.

Kaspersky Embedded Systems Security peut être installé et configuré sur un périphérique protégé unique avec ses paramètres enregistrés sur un fichier de configuration ; le fichier permet alors d'installer Kaspersky Embedded Systems Security sur d'autres périphériques protégés. Remarque : cette capacité n'existe pas lorsque l'application est installée via les stratégies de groupe Active Directory.

Lancement de l'Assistant d'installation

Grâce à l'Assistant d'installation, vous pouvez installer :

- Les composants de Kaspersky Embedded Systems Security sur un périphérique protégé depuis le fichier \product\setup.exe inclus dans le kit de distribution.
- La Console de Kaspersky Embedded Systems Security depuis le fichier \client\setup.exe du kit de distribution sur le périphérique protégé ou sur un autre hôte LAN.

Lancement du package d'installation via la ligne de commande selon les paramètres d'installation requis

Si vous lancez le fichier du package d'installation sans les options de la ligne de commande, Kaspersky Embedded Systems Security sera installé selon les paramètres par défaut. Grâce aux arguments de Kaspersky Embedded Systems Security, vous pouvez modifier les paramètres d'installation.

Vous pouvez installer la Console de l'application sur l'appareil protégé et/ou sur le poste de travail de l'administrateur.

Vous pouvez aussi utiliser des exemples de commande pour l'installation de Kaspersky Embedded Systems Security et de la Console de l'application.

Installation centralisée via Kaspersky Security Center

Si vous utilisez Kaspersky Security Center dans votre réseau pour administrer la protection antivirus des périphériques en réseau, vous pouvez installer Kaspersky Embedded Systems Security sur plusieurs périphériques à l'aide de la tâche d'installation à distance.

Les périphériques protégés sur lesquels vous souhaitez installer Kaspersky Embedded Systems Security via Kaspersky Security Center peuvent soit se trouver dans le même domaine que Kaspersky Security Center, soit dans un autre domaine. Ils peuvent également n'appartenir à aucun domaine.

Installation centralisée via les stratégies de groupe Active Directory

Les stratégies de groupe Active Directory permettent d'installer Kaspersky Embedded Systems Security sur le périphérique protégé. Vous pouvez installer la console de l'application sur l'appareil protégé ou sur le poste de travail de l'administrateur.

Vous pouvez installer Kaspersky Embedded Systems Security uniquement avec les paramètres par défaut.

Les périphérique protégés sur lesquels Kaspersky Embedded Systems Security sont installé à l'aide des stratégies de groupe Active Directory doivent se trouver dans le même domaine et dans la même unité organisationnelle. L'installation a lieu lors du démarrage de l'appareil protégé avant la connexion à Microsoft Windows.

Installation et suppression de l'application à l'aide de l'assistant

La section décrit l'installation et la désinstallation de Kaspersky Embedded Systems Security et de la Console de l'application via l'assistant Installation. Elle contient des informations sur la configuration avancée de Kaspersky Embedded Systems Security et définit les actions à réaliser lors de l'installation.

Installation à l'aide de l'Assistant d'installation

Les sections suivantes contiennent des informations sur l'installation de Kaspersky Embedded Systems Security et de la console de l'application.

Pour installer et utiliser Kaspersky Embedded Systems Security :

1. Installez Kaspersky Embedded Systems Security sur un périphérique protégé.
2. Installez la Console de l'application sur les périphériques sur lesquels vous avez l'intention d'administrer Kaspersky Embedded Systems Security.
3. Si vous avez installé la Console de l'application sur n'importe quel ordinateur du réseau autre que le périphérique protégé, procédez à une configuration complémentaire afin que les utilisateurs de la Console de l'application puissent administrer Kaspersky Embedded Systems Security à distance.
4. Réalisez les actions après l'installation de Kaspersky Embedded Systems Security.

Installation de Kaspersky Embedded Systems Security

Avant d'installer Kaspersky Embedded Systems Security, suivez les étapes suivantes :

1. Assurez-vous qu'aucun autre logiciel antivirus n'est installé sur l'appareil protégé.
2. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au groupe d'administrateurs de l'appareil protégé.

Lorsque les actions décrites ci-dessus ont été effectuées, passez à la procédure d'installation. Définissez les paramètres d'installation de Kaspersky Embedded Systems Security en suivant les instructions de l'Assistant. Vous pouvez interrompre l'installation de Kaspersky Embedded Systems Security à n'importe quelle étape de l'assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'assistant d'installation.

Vous pouvez en apprendre plus sur les paramètres d'installation (de désinstallation).

Pour installer Kaspersky Embedded Systems Security à l'aide de l'Assistant d'installation :

1. Lancez le fichier setup.exe sur l'appareil protégé.
2. Dans la fenêtre qui s'ouvre, dans la section **Installation**, cliquez sur le lien **Protéger l'ordinateur avec la technologie d'interdiction par défaut** ou **Protéger l'ordinateur avec des bases antivirus**.

Si la configuration Protéger l'ordinateur avec des bases antivirus est sélectionnée, tous les composants de Kaspersky Embedded Systems Security sont inclus par défaut à l'exception des composants Gestion du pare-feu et Compteurs de performance.

Lorsque vous installez la configuration Protéger l'ordinateur avec les bases antivirus de Kaspersky Embedded Systems Security sur une version de l'application qui n'utilise pas l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement enrichi via l'ajout des composants suivants :

- Protection des fichiers en temps réel
- Analyse à la demande
- Protection contre les menaces réseau

Les composants qui permettent les mises à jour ne sont pas inclus dans la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut.

Si la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut est sélectionnée, les composants suivants sont inclus par défaut :

- Core
- Protection contre les exploits
- Contrôle du lancement des applications
- Icône de la barre d'état système

Lorsque vous installez la configuration Protéger l'ordinateur avec la technologie d'interdiction par défaut de Kaspersky Embedded Systems Security sur une version de l'application qui utilise l'analyse sur la base des signatures et les bases antivirus pour protéger votre ordinateur, l'ensemble des composants de l'application est automatiquement réduit via l'élimination des composants suivants :

- Protection des fichiers en temps réel
- Analyse à la demande
- Les composants qui permettent les mises à jour

Cette configuration est recommandée pour protéger les systèmes aux ressources limitées. Dans ce cas, vous pouvez activer l'application à long terme et le composant Contrôle du lancement des applications assure la protection de l'ordinateur.

3. Dans la fenêtre d'accueil de l'Assistant d'installation de Kaspersky Embedded Systems Security, appuyez sur le bouton **Suivant**.

   La fenêtre **Contrat de licence utilisateur final et politique de confidentialité** s'ouvre.

4. Révisez le Contrat de licence et la Politique de confidentialité.

5. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **Je confirme que j'ai lu, compris et que j'accepte l'intégralité des termes de ce Contrat de licence utilisateur final** et **Je sais que mes données vont être traitées et transmises (y compris vers des pays tiers) conformément aux dispositions de la Politique de confidentialité et je l'accepte. J'ai lu la Politique de confidentialité dans sa totalité et je l'ai comprise** afin de procéder à l'installation.

Si vous n'acceptez pas le Contrat de licence utilisateur final et/ou la Politique de confidentialité, l'installation sera interrompue.

6. Cliquez sur **Suivant**.

   La fenêtre **Installation personnalisée** s'ouvre.

7. Sélectionnez les composants que vous souhaitez installer.

   Le composant Prise en charge du protocole SNMP de Kaspersky Embedded Systems Security apparaît dans la liste des composants à installer uniquement si le service SNMP Microsoft Windows est installé sur le périphérique protégé.

8. Pour annuler toutes les modifications, cliquez sur , cliquez sur le bouton **Réinitialiser** dans la fenêtre **Installation personnalisée**. Cliquez sur **Suivant**.

9. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :

   - Le cas échéant, désignez un dossier pour la copie des fichiers de Kaspersky Embedded Systems Security.
   - Le cas échéant, consultez les informations concernant l'espace disponible sur les disques durs locaux en cliquant sur **Disque**.

   Cliquez sur **Suivant**.

10. Dans la fenêtre **Paramètres avancés d'installation** qui s'ouvre, définissez les paramètres d'installation suivants :

    - **Activer la protection en temps réel après l'installation de l'application**.
    - **Ajouter les exclusions recommandées par Microsoft**.
    - **Ajouter les fichiers recommandés par Kaspersky aux exclusions**.

      Cliquez sur **Suivant**.

11. Dans la fenêtre **Importation des paramètres du fichier de configuration**, procédez comme suit :

    a. Désignez le fichier de configuration pour importer les paramètres de Kaspersky Embedded Systems Security depuis un fichier de configuration existant créé dans n'importe quelle version précédente compatible de l'application.

    b. Cliquez sur **Suivant**.

12. Dans la fenêtre **Activation de l'application**, exécutez l'une des actions suivantes :

    - Si vous souhaitez activer l'application, sélectionnez un fichier clé de Kaspersky Embedded Systems Security.
    - Si vous souhaitez activer l'application plus tard, cliquez sur **Suivant**.
    - Si vous aviez déjà enregistré un fichier clé dans le dossier \product du kit de distribution, le nom de ce fichier apparaît dans le champ **Clé**.

Si vous souhaitez ajouter une licence à l'aide d'un fichier clé qui se trouve dans un autre dossier, spécifiez le fichier clé.

Après l'ajout du fichier clé, la fenêtre affiche les informations concernant la licence. Kaspersky Embedded Systems Security la date d'expiration de la licence calculée. La date de validité de la licence est calculée à partir de l'ajout de la clé et elle ne dépasse jamais la date d'expiration de la validité du fichier clé.

Cliquez sur **Suivant** pour appliquer le fichier clé dans l'application.

13. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**. L'assistant lance l'installation des composants de Kaspersky Embedded Systems Security.

14. La fenêtre **Installation terminée** s'ouvre à la fin de l'installation.

15. Cochez la case **Lire les notes de publication** afin de consulter les informations relatives à la version après la fin de l'Assistant d'installation.

16. Cliquez sur **Terminer**.

L'assistant d'installation se ferme. Une fois l'installation terminée, Kaspersky Embedded Systems Security est prêt à l'emploi si vous avez ajouté une clé d'activation.

Installation de la console de Kaspersky Embedded Systems Security

Configurez la console de l'application en suivant les instructions de l'Assistant d'installation. Vous pouvez interrompre l'installation à n'importe quelle étape de l'Assistant. Pour ce faire, cliquez sur **Annuler** dans la fenêtre de l'Assistant d'installation.

Pour installer la Console de l'application :

1. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au groupe des administrateurs sur l'appareil.

2. Exécutez le fichier setup.exe sur l'appareil protégé.

   La fenêtre de bienvenue de l'application s'ouvre.

3. Cliquez sur le lien **Installer la console de Kaspersky Embedded Systems Security**.

   La fenêtre d'accueil de l'Assistant d'installation s'ouvre.

4. Cliquez sur **Suivant**.

5. Dans la fenêtre qui s'ouvre, lisez les dispositions du Contrat de licence utilisateur final et de la Politique de confidentialité, puis cochez les cases sous **Je confirme que j'ai lu, compris et que j'accepte l'intégralité des termes de ce Contrat de licence utilisateur final** afin de poursuivre l'installation.

6. Cliquez sur **Suivant**.

   La fenêtre **Paramètres avancés d'installation** s'ouvre.

7. Dans la fenêtre **Paramètres avancés d'installation**, procédez comme suit :

   - Si vous avez l'intention d'administrer Kaspersky Embedded Systems Security sur un périphérique distant à l'aide de la Console de l'application, cochez la case **Autoriser l'accès à distance**.

- Pour ouvrir la fenêtre **Installation personnalisée** et sélectionner des composants, procédez comme suit :

  a. Cliquez sur le bouton **Avancé**.

  La fenêtre **Installation personnalisée** s'ouvre.

  b. Sélectionnez le composant "Outils d'administration" dans la liste.

  Par défaut, tous les composants sont installés.

  c. Cliquez sur **Suivant**.

Vous pouvez obtenir de plus amples informations sur les composants de Kaspersky Embedded Systems Security.

8. Exécutez les actions suivantes dans la fenêtre **Sélection d'un dossier de destination** qui s'ouvre :

   a. Le cas échéant, désignez un autre dossier pour la conservation des fichiers installés.

   b. Cliquez sur **Suivant**.

9. Dans la fenêtre **Prêt pour l'installation**, cliquez sur le bouton **Installer**.

   L'Assistant lance l'installation des composants sélectionnés.

10. Cliquez sur **Terminer**.

L'assistant d'installation se ferme. La Console de l'application sera installée sur l'appareil protégé.

Si vous avez installé la sélection Outils d'administration sur tout périphérique du réseau autre que le périphérique protégé, configurez les paramètres avancés.

Configuration avancée après l'installation de la console de l'application sur un autre appareil

Si vous avez installé la Console de l'application sur un périphérique quelconque du réseau autre qu'un périphérique protégé, réalisez les actions suivantes afin que les utilisateurs puissent administrer Kaspersky Embedded Systems Security à distance :

- Ajoutez les utilisateurs de Kaspersky Embedded Systems Security au groupe ESS Administrators.
- Autorisez les connexions réseau pour le Service Kaspersky Security Management (kavfsgt.exe) si le pare-feu Windows ou un pare-feu tiers est utilisé sur le périphérique protégé.
- Si lors de l'installation de la Console de l'application sur un appareil tournant sous Microsoft Windows vous n'avez pas coché la case **Autoriser l'accès à distance**, autorisez manuellement les connexions réseau pour la Console de l'application via le pare-feu de cet appareil.

La Console de l'application sur le périphérique distant utilise le protocole DCOM pour obtenir des informations sur les événements de Kaspersky Embedded Systems Security (objets analysés, tâches terminées, etc.) fournies par le Service Kaspersky Security Management sur le périphérique protégé. Vous devez autoriser les connexions réseau pour la Console de l'application dans le pare-feu Windows pour la Console de l'application afin d'établir une connexion entre la Console de l'application et le Service Kaspersky Security Management.

Sur l'appareil distant où la Console de l'application est installée, procédez comme suit :

- Assurez-vous que l'accès à distance anonyme aux applications COM est autorisé (mais pas le lancement à distance et l'activation des applications COM).
- Dans le pare-feu Windows, ouvrez le port TCP 135 et autorisez les connexions réseau pour le fichier exécutable kavfsrcn.exe du processus d'administration à distance de Kaspersky Embedded Systems Security.

  Le périphérique sur lequel la Console de l'application est installée utilise le port TCP 135 pour accéder au périphérique protégé et pour recevoir une réponse.
- Configurez une règle sortante pour que le pare-feu Windows autorise la connexion.

  Contrairement aux services TCP/IP et UDP/IP classiques où un seul protocole est associé à un port fixe, le service DCOM affecte des ports de manière dynamique aux objets COM distants. Si un pare-feu existe entre le client (ou la Console de l'application est installée) et le terminal DCOM (l'appareil protégé), un grand éventail de ports doit être ouvert.

Les mêmes étapes doivent être appliquées pour configurer tout autre pare-feu logiciel ou matériel.

Si la Console de l'application est ouverte pendant que vous configurez la connexion entre l'appareil protégé et l'appareil sur lequel elle est installée, procédez comme suit :

1. Fermez la console de l'application.
2. Attendez la fin du processus de gestion à distance de Kaspersky Embedded Systems Security kavfsrcn.exe.
3. Redémarrez la console de l'application.

   Les nouvelles valeurs des paramètres de connexion seront appliquées.

Autorisation de l'accès à distance anonyme aux applications COM

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

Pour autoriser l'accès à distance anonyme aux applications COM :

1. Sur le périphérique distant sur lequel la console de Kaspersky Embedded Systems Security est installée, ouvrez la console du Service des composants.
2. Choisissez **Démarrer** → **Exécuter**.
3. Saisissez la commande `dcomcnfg`.
4. Cliquez sur le bouton **OK**.
5. Dans la console du **Service des composants** de votre périphérique protégé, développez le nœud **Ordinateurs**.
6. Ouvrez le menu contextuel du nœud **Poste de travail**.
7. Choisissez l'option **Propriétés**.
8. Sous l'onglet **Sécurité COM** de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les limites** du groupe de paramètres **Autorisations d'accès**.

9. Dans la fenêtre **Autoriser l'accès à distance**, assurez-vous que la case **Autoriser l'accès à distance** est cochée pour l'utilisateur ANONYMOUS LOGON.

10. Cliquez sur le bouton **OK**.

Autorisation des connexions réseau pour le processus d'administration à distance de Kaspersky Embedded Systems Security

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

Pour ouvrir le port TCP 135 du pare-feu Windows et autoriser les connexions de réseau pour le processus d'administration à distance de Kaspersky Embedded Systems Security :

1. Sur le périphérique distant, fermez la console de Kaspersky Embedded Systems Security.

2. Exécutez une des actions suivantes :

   - Dans Microsoft Windows XP SP2 et suivants :

     a. Sélectionnez **Démarrer** > **Pare-feu Windows**.

     b. Dans la fenêtre **Pare-feu Windows** (ou Paramètres du pare-feu Windows), cliquez sur le bouton **Ajouter un port** sous l'onglet **Exclusions**.

     c. Dans le champ **Nom**, indiquez le nom du port RPC (TCP/135) ou saisissez un autre nom, par exemple DCOM Kaspersky Embedded Systems Security et dans le champ **Nom de port**, indiquez le numéro du port : 135.

     d. Sélectionnez le protocole **TCP**.

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

     f. Sous l'onglet **Exclusions**, cliquez sur le bouton **Ajouter**.

   - Dans Microsoft Windows 7 et suivants :

     a. Sélectionnez **Démarrer** > **Panneau de configuration** > **Pare-feu Windows**.

     b. Dans la fenêtre **Pare-feu Windows**, sélectionnez **Autoriser le lancement de l'application ou du module via le Pare-feu Windows**.

     c. Dans la fenêtre **Autoriser un programme via le Pare-feu Windows**, cliquez sur le bouton **Autoriser un autre programme**.

3. Dans la fenêtre **Ajout de programme**, désignez le fichier kavfsrcn.exe. Il se trouve dans le dossier cible désigné lors de l'installation de la console de Kaspersky Embedded Systems Security à l'aide de Microsoft Management Console.

4. Cliquez sur le bouton **OK**.

5. Cliquez sur le bouton **OK** dans la fenêtre **Pare-feu Windows (Paramètres du pare-feu Windows)**.

Ajout d'une règle sortante pour le pare-feu Windows

Les noms des paramètres peuvent varier selon le système d'exploitation Windows installé.

Pour ajouter la règle sortante pour le pare-feu Windows :

1. Sélectionnez **Démarrer** > **Panneau de configuration** > **Pare-feu Windows**.
2. Dans la fenêtre **Pare-feu Windows**, cliquez sur le lien **Paramètres avancés**.
   La fenêtre **Pare-feu Windows avec sécurité avancée** s'ouvre.
3. Cochez le nœud enfant **Règles de trafic sortant**.
4. Dans le panneau **Actions**, cliquez sur l'option **Nouvelle règle**.
5. Dans la fenêtre de l'**assistant de création de nouvelle règle de sortie**, sélectionnez l'option **Port** et cliquez sur **Suivant**.
6. Sélectionnez le protocole **TCP**.
7. Dans le champ **Ports distants spécifiques** spécifiez la plage de ports suivante pour autoriser les connexions sortantes : 1024-65535.
8. Dans la fenêtre **Action**, sélectionnez l'option **Autoriser la connexion**.
9. Enregistrez la nouvelle règle et fermez la fenêtre **Pare-feu Windows avec fonctions avancées de sécurité**.

Le pare-feu Windows autorise désormais les connexions réseau entre la console de l'application et le Service Kaspersky Security Management :

Actions à réaliser après l'installation de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si l'option **Activer la protection en temps réel après l'installation de l'application** (option par défaut) est sélectionnée lors de l'installation de Kaspersky Embedded Systems Security, l'application analyse les objets du système de fichiers du périphérique lorsqu'ils sont sollicités. Chaque vendredi à 20h00, Kaspersky Embedded Systems Security lance la tâche Analyse rapide.

Après l'installation de Kaspersky Embedded Systems Security, il est conseillé de réaliser les actions suivantes :

- Lancez la tâche Mise à jour des bases de l'application. Une fois installé, Kaspersky Embedded Systems Security analyse les objets à l'aide des bases livrées avec le kit de distribution de l'application.

  Nous recommandons de mettre à jour immédiatement les bases de Kaspersky Embedded Systems Security car elles peuvent être obsolètes.

  Par la suite, l'application mettra à jour les bases toutes les heures conformément à la planification définie dans la tâche par défaut.

- Lancez une analyse rapide du périphérique si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur le périphérique protégé avant l'installation de Kaspersky Embedded Systems Security.
- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Embedded Systems Security.

Lancement et configuration de la tâche de mise à jour des bases de l'application de Kaspersky Embedded Systems Security

Pour mettre à jour les bases de l'application après l'installation :

1. Configurer la connexion avec une source des mises à jour, les serveurs HTTP ou FTP de mise à jour de Kaspersky, dans les propriétés de la tâche Mise à jour des bases de l'application.
2. Lancer la tâche Mise à jour des bases de l'application.

Le protocole WPAD (Web Proxy Auto-Discovery) n'est peut-être pas configuré sur votre réseau pour détecter automatiquement les paramètres du serveur proxy dans le LAN. De plus, le réseau requiert peut-être l'authentification pour accéder au serveur proxy.

Pour définir les paramètres du serveur proxy en option ainsi que les paramètres d'authentification pour accéder au serveur proxy :

1. Ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application** s'ouvre.
3. Ouvrez l'onglet **Paramètres de connexion**.
4. Dans la section **Paramètres du serveur proxy**, cochez la case **Utiliser le serveur proxy indiqué**.
5. Saisissez l'adresse du serveur proxy dans le champ **Adresse** et saisissez le numéro de port du serveur proxy dans le champ **Port**.
6. Dans la section **Paramètres d'authentification du serveur proxy**, sélectionnez la méthode d'authentification nécessaire dans la liste déroulante :

   - **Utiliser l'authentification NTLM** si le serveur proxy prend en charge l'analyse intégrée de l'authenticité dans Microsoft Windows (NTLM authentification). Kaspersky Embedded Systems Security accède alors au serveur proxy à l'aide du compte utilisateur indiqué dans les paramètres de la tâche (la tâche est exécutée par défaut sous le compte utilisateur **Système local** (**SYSTEM**)).
   - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** si le serveur prend en charge l'authentification NTLM Microsoft Windows intégrée. Kaspersky Embedded Systems Security utilisera le compte utilisateur que vous aurez défini pour accéder au serveur proxy. Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.
   - **Utiliser le nom d'utilisateur et le mot de passe** pour choisir l'authentification traditionnelle (Basic authentification). Saisissez le nom et le mot de passe de l'utilisateur ou sélectionnez un utilisateur dans la liste.

7. Cliquez sur **OK** dans la fenêtre **Paramètres de l'application**.

Pour configurer la connexion aux serveurs de mise à jour de Kaspersky dans la tâche Mise à jour des bases de l'application, procédez comme suit :

1. Lancez la Console de l'application d'une des manières suivantes :

   - Ouvrez la console de l'application sur l'appareil protégé. Pour cela, cliquez sur **Démarrer** > **Tous les programmes** > **Kaspersky Embedded Systems Security** > **Outils d'administration** > **Console de Kaspersky Embedded Systems Security 3.2**.

   - Si vous avez lancé la Console de l'application sur un appareil autre que celui qui est protégé, connectez-vous à l'appareil protégé :

     a. Ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security** dans l'arborescence de la Console de l'application.

     b. Sélectionnez l'option **Se connecter à un autre ordinateur**.

     c. Dans la fenêtre **Sélection de l'appareil protégé** qui s'ouvre, choisissez **Autre appareil** et saisissez le nom de réseau de l'appareil protégé dans le champ textuel.

     Si le compte utilisateur employé pour se connecter à Microsoft Windows ne possède pas les autorisations d'accès au Service Kaspersky Security Management, indiquez un compte utilisateur doté de ces autorisations.

   La fenêtre Console de l'application s'ouvre.

2. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.

3. Sélectionnez le nœud enfant **Mise à jour des bases de l'application**.

4. Dans le volet résultats, cliquez sur le lien **Propriétés**.

5. Dans la fenêtre **Paramètres de la tâche** qui s'ouvre, ouvrez l'onglet **Paramètres de connexion**.

6. Sélectionnez **Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky**.

7. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres de connexion à la source des mises à jour dans la tâche Mise à jour des bases de l'application sont sauvegardés.

Pour lancer la tâche Mise à jour des bases de l'application, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.

2. Dans le menu contextuel du nœud enfant **Mise à jour des bases de l'application**, sélectionnez l'option **Démarrer**.

La tâche de Mise à jour des bases de l'application démarre.

Une fois la tâche terminée, vous pouvez consulter la date de publication des dernières mises à jour des bases de l'application installées dans le panneau des résultats du nœud **Kaspersky Embedded Systems Security**.

Analyse rapide

Une fois que les bases de Kaspersky Embedded Systems Security ont été mises à jour, recherchez la présence éventuelle d'applications malveillantes sur le périphérique protégé à l'aide de la tâche Analyse rapide.

Pour lancer la tâche Analyse rapide :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Dans le menu contextuel du nœud enfant **Analyse rapide**, sélectionnez la commande **Démarrer**.

La tâche est lancée et l'état **Exécution en cours** apparaît dans le volet résultats.

Pour consulter le journal d'exécution de la tâche,

dans le volet résultats du nœud **Analyse rapide**, cliquez sur le lien **Ouvrir le journal d'exécution de la tâche**.

Modification de la sélection de composants et réparation de Kaspersky Embedded Systems Security

Vous pouvez ajouter ou supprimer des composants de Kaspersky Embedded Systems Security. Vous devez d'abord arrêter la tâche Protection des fichiers en temps réel si vous souhaitez supprimer le composant Protection des fichiers en temps réel. Dans tous les autres cas, il n'est pas nécessaire d'arrêter la Protection des fichiers en temps réel ou le Service Kaspersky Security.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Embedded Systems Security requiert la saisie du mot de passe lors de toute tentative de suppression de composants ou de modification de la liste des composants de l'application dans l'assistant d'installation.

Pour modifier la sélection de composants de Kaspersky Embedded Systems Security :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes** > **Kaspersky Embedded Systems Security** > **Modification ou suppression de Kaspersky Embedded Systems Security**.

   La fenêtre **Réparer ou supprimer l'installation** de l'Assistant d'installation s'ouvre.

2. Sélectionnez **Modification de la liste des composants**. Cliquez sur **Suivant**.

   La fenêtre **Installation personnalisée** s'ouvre.

3. Dans la liste des composants disponibles qui apparaît dans la fenêtre **Installation personnalisée**, sélectionnez les composants à ajouter ou à supprimer dans Kaspersky Embedded Systems Security. Pour ce faire, procédez comme suit :

   - Pour modifier la composition des composants, cliquez sur le bouton situé en regard du composant sélectionné. Puis, sélectionnez dans le menu contextuel :

     - L'option **Le composant sera installé sur un disque dur local** si vous souhaitez installer un composant ;

- L'option **Le composant et ses sous-composants seront installés sur le disque dur local** si vous souhaitez installer un groupe de composants.

- Pour supprimer un composant déjà installé, cliquez sur le bouton en regard du nom du composant sélectionné. Puis sélectionnez **Ce composant ne sera plus disponible** dans le menu contextuel.

Cliquez sur **Suivant**.

4. Dans la fenêtre **Prêt pour l'installation**, confirmez la modification de la liste des composants de l'application en cliquant sur le bouton **Installer**.

5. Dans la fenêtre qui s'ouvre lorsque l'installation est terminée, cliquez sur le bouton **OK**.

La liste des composants de Kaspersky Embedded Systems Security sera modifiée conformément aux paramètres définis.

Si des problèmes se présentent durant l'utilisation de Kaspersky Embedded Systems Security (Kaspersky Embedded Systems Security s'arrête, les tâches se soldent par un échec ou ne sont pas lancées), vous pouvez réparer Kaspersky Embedded Systems Security. Vous pouvez procéder à la réparation en conservant les valeurs actuelles des paramètres de Kaspersky Embedded Systems Security ou en sélectionnant le mode qui rétablira toutes les valeurs par défaut des paramètres de Kaspersky Embedded Systems Security.

Pour réparer Kaspersky Embedded Systems Security après une erreur de l'application ou d'une tâche :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.

2. Sélectionnez **Kaspersky Embedded Systems Security**.

3. Sélectionnez **Modification ou suppression de Kaspersky Embedded Systems Security**.

   La fenêtre **Réparer ou supprimer l'installation** de l'Assistant d'installation s'ouvre.

4. Sélectionnez **Réparation des composants installés**. Cliquez sur **Suivant**.

   La fenêtre **Réparation des composants installés** s'ouvre.

5. Dans la fenêtre **Réparation des composants installés**, cochez la case **Rétablir les paramètres recommandés de l'application** si vous souhaitez réinitialiser les paramètres et restaurer les paramètres par défaut de Kaspersky Embedded Systems Security. Cliquez sur **Suivant**.

6. Dans la fenêtre **Prêt pour la réparation**, confirmez la réparation de l'application en cliquant sur le bouton **Installer**.

7. Dans la fenêtre qui s'ouvre lorsque la réparation est terminée, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security sera réparés conformément aux paramètres définis.

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

Cette section contient des instructions pour supprimer Kaspersky Embedded Systems Security et la Console de l'application sur un périphérique protégé à l'aide de l'Assistant d'installation/de désinstallation.

Désinstallation de Kaspersky Embedded Systems Security

Les fichiers dump et de trace ne sont pas supprimés lors de la désinstallation de Kaspersky Embedded Systems Security. Vous pouvez supprimer manuellement les fichiers dump et de trace dans le dossier spécifié lors de la configuration de l'écriture des fichiers dump et de trace.

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Vous pouvez désinstaller Kaspersky Embedded Systems Security du périphérique protégé à l'aide de l'Assistant d'installation/de désinstallation.

Il faudra peut-être redémarrer le périphérique protégé sur lequel Kaspersky Embedded Systems Security a été désinstallé. Le redémarrage peut être reporté.

La suppression, la réparation et l'installation d'une application via le panneau d'administration Windows sont impossible si le système d'exploitation utilise la fonction Contrôle des comptes utilisateurs (User Account Control) ou si l'accès à l'application est protégé par un mot de passe.

Si l'accès à l'administration de l'application est protégé par un mot de passe, Kaspersky Embedded Systems Security requiert la saisie du mot de passe lors de toute tentative de suppression de composants ou de modification de la liste des composants de l'application dans l'assistant d'installation.

Pour désinstaller Kaspersky Embedded Systems Security :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.
2. Sélectionnez **Kaspersky Embedded Systems Security**.
3. Sélectionnez **Modification ou suppression de Kaspersky Embedded Systems Security**.

   La fenêtre **Réparer ou supprimer l'installation** de l'Assistant d'installation s'ouvre.
4. Sélectionnez **Suppression des composants de l'application**. Cliquez sur **Suivant**.

   La fenêtre **Paramètres avancés de désinstallation de l'application** s'ouvre.
5. Si nécessaire, dans la fenêtre **Paramètres avancés de désinstallation de l'application**, procédez comme suit :

   a. Cochez la case **Exporter les objets de la quarantaine** pour que Kaspersky Embedded Systems Security exporte les objets qui ont été mis en quarantaine. Cette case est décochée par défaut.

   b. Cochez la case **Exporter les objets de la sauvegarde** pour exporter les objets de la Sauvegarde de Kaspersky Embedded Systems Security. Cette case est décochée par défaut.

   c. Cliquez sur le bouton **Enregistrer dans** et indiquez le dossier vers lequel vous souhaitez exporter les objets. Par défaut, les objets sont exportés vers le dossier %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

   Cliquez sur **Suivant**.
6. Dans la fenêtre **Prêt pour la désinstallation**, confirmez l'opération de désinstallation en cliquant sur **Désinstaller**.
7. Dans la fenêtre qui s'ouvre lorsque la désinstallation est terminée, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security est désinstallé du périphérique protégé.

Désinstallation de la console de Kaspersky Embedded Systems Security

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Vous pouvez désinstaller la console de l'application sur l'appareil protégé à l'aide de l'Assistant d'installation/de désinstallation.

Il n'est pas nécessaire de redémarrer l'appareil protégé après la désinstallation de la Console de l'application.

Pour désinstaller la console de l'application, procédez comme suit :

1. Dans le menu **Démarrer**, sélectionnez **Tous les programmes**.
2. Sélectionnez **Kaspersky Embedded Systems Security**.
3. Sélectionnez **Modification ou suppression de Kaspersky Embedded Systems Security**.
   La fenêtre **Réparer ou supprimer l'installation** de l'Assistant s'ouvre.
4. Choisissez l'option **Suppression des composants de l'application**, puis cliquez sur **Suivant**.
5. La fenêtre **Prêt pour la désinstallation** s'ouvre. Cliquez sur le bouton **Désinstaller**.
   La fenêtre **Désinstallation terminée** s'ouvre.
6. Cliquez sur le bouton **OK**.

L'opération de désinstallation est terminée et la fenêtre de l'Assistant se ferme.

Installation et suppression de l'application via la ligne de commande

Cette section décrit les particularités de l'installation et de la désinstallation de Kaspersky Embedded Systems Security via la ligne de commande. Elle fournit également des exemples de commande pour l'installation et la désinstallation de Kaspersky Embedded Systems Security et des exemples de commandes pour l'ajout et la suppression de composants de Kaspersky Embedded Systems Security via la ligne de commande.

A propos de l'installation et de la désinstallation de Kaspersky Embedded Systems Security via la ligne de commande

Les fichiers dump et de trace ne sont pas supprimés lors de la désinstallation de Kaspersky Embedded Systems Security. Vous pouvez supprimer manuellement les fichiers dump et de trace dans le dossier spécifié lors de la configuration de l'écriture des fichiers dump et de trace.

Vous pouvez installer ou désinstaller Kaspersky Embedded Systems Security et ajouter ou supprimer ses composants en exécutant le fichier du paquet d'installation \product\ess_x86.msi ou \product\ess_x64.msi à partir de la ligne de commande après avoir spécifié les paramètres d'installation à l'aide de clés.

Vous pouvez installer la sélection "Outils d'administration" sur l'appareil protégé ou sur un autre appareil du réseau afin d'utiliser la console de l'application localement ou à distance. Pour ce faire, utilisez le paquet d'installation \console\esstools.msi.

Réalisez l'installation sous un compte utilisateur appartenant au groupe d'administrateurs de l'appareil protégé sur lequel l'application est installée.

Si vous exécutez l'un des fichiers \product\ess_x86.msi ou \product\ess_x64.msi sur le périphérique protégé sans clés additionnelles, Kaspersky Embedded Systems Security est installé avec les paramètres d'installation recommandés.

Vous pouvez définir la sélection des composants à installer à l'aide de l'argument de ligne de commande ADDLOCAL et en utilisant en guise de valeur le code des composants sélectionnés ou de la sélection de composants.

Exemple de commandes pour l'installation de Kaspersky Embedded Systems Security

Cette section présente des exemples de commandes pour l'installation de Kaspersky Embedded Systems Security.

Sur les appareils protégés fonctionnant sous Microsoft Windows 32 bits, exécutez les fichiers du kit de distribution dont le suffixe est x86. Sur les appareils protégés fonctionnant sous Microsoft Windows 64 bits, exécutez les fichiers du kit de distribution dont le suffixe est x64.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des instructions et des clés standard de Windows Installer.

Exemples d'installation de Kaspersky Embedded Systems Security depuis le fichier setup.exe

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande suivante :

```
\product\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

Vous pouvez installer Kaspersky Embedded Systems Security avec les paramètres suivants :

- Installer uniquement les composants Protection des fichiers en temps réel et Analyse à la demande
- Ne pas lancer la Protection des fichiers en temps réel au démarrage de Kaspersky Embedded Systems Security
- Ne pas exclure de la zone d'analyse les fichiers recommandés par Microsoft Corporation

Pour installer les composants, tels que le Contrôle des périphériques, exécutez la commande suivante :

```
\product\setup.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

Vous pouvez utiliser les clés facultatives suivantes avec cette commande lorsque vous installez Kaspersky Embedded Systems Security sur les ordinateurs dotés d'appareils réseau et d'appareils SCSI qui provoquent une panne du système après l'installation de <NOM_DU_PRODUIT_COMPLET> :

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

Active (1) ou désactive (0) l'interception des connexions des cartes réseau.

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

Active (1) ou désactive (0) l'interception des connexions des cartes SCSI.

Exemples de commandes pour l'installation : exécution d'un fichier .msi

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés sans intervention de l'utilisateur, exécutez la commande suivante :

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security selon les paramètres recommandés et afficher l'interface d'installation, saisissez la commande suivante :

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés et pour activer la rotation des fichiers de traçage une fois que le nombre maximal défini de fichiers de traçage est atteint, exécutez la commande suivante :

```
msiexec /i ess.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

Notez que le paramètre `TRACE_FOLDER` est obligatoire.

Pour le paramètre `TRACE_MAX_ROLL_COUNT`, les conditions suivantes sont introduites :

- Si le paramètre est définir, la rotation des fichiers de traçage est activée avec le nombre maximal de fichiers de traçage que vous définissez. Plage de valeurs disponible : de 1 à 999.
- Si la valeur 0 pour le nombre maximal de fichiers de traçage est attribuée au paramètre, la rotation des fichiers de traçage est désactivée.
- Si le paramètre est défini et que la valeur du nombre maximal de fichiers de traçage n'est pas valide ou dépasse la plage autorisée de 1 à 999 fichiers, la rotation des fichiers de traçage est activée avec la valeur par défaut de 5 comme nombre maximal de fichiers de traçage.
- Si le paramètre n'est pas renseigné :
  - Si la rotation des fichiers de traçage est déjà configurée sur l'appareil, les paramètres restent inchangés. L'application ignorera les paramètres que vous saisissez.
  - Si la rotation des fichiers de traçage n'est pas encore configurée sur l'appareil, l'option de rotation est activée avec un nombre maximal de fichiers de traçage égal à 5.

Pour installer et activer Kaspersky Embedded Systems Security à l'aide du fichier clé C:\0000000A.key :

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux, saisissez la commande suivante :

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security dans le dossier d'installation C:\ESS, exécutez la commande suivante :

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security et enregistrer un fichier journal d'installation sous le nom ess.log dans le dossier qui contient le fichier msi de Kaspersky Embedded Systems Security, exécutez la commande suivante :

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

Pour installer la console de Kaspersky Embedded Systems Security, exécutez la commande suivante :

```
msiexec /i esstools.msi /qn EULA=1
```

Pour installer et activer Kaspersky Embedded Systems Security à l'aide du fichier clé C:\0000000A.key et configurer Kaspersky Embedded Systems Security conformément aux paramètres du fichier de configuration C:\settings.xml, exécutez la commande suivante :

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1
PRIVACYPOLICY=1
```

Pour installer un correctif de l'application lorsque Kaspersky Embedded Systems Security est protégé par mot de passe, exécutez la commande suivante :

```
msiexec /p "<nom de fichier msp avec le chemin>" UNLOCK_PASSWORD=<mot de passe>
```

Actions à réaliser après l'installation de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si vous sélectionnez l'option **Activer la protection en temps réel après l'installation de l'application** lors de l'installation de Kaspersky Embedded Systems Security, l'application analyse les objets du système de fichiers du périphérique lorsqu'ils sont sollicités. Chaque vendredi à 20h00, Kaspersky Embedded Systems Security exécute la tâche Analyse des zones critiques.

Après l'installation de Kaspersky Embedded Systems Security, il est conseillé de réaliser les actions suivantes :

- Lancer la tâche de mise à jour des bases de l'application de Kaspersky Embedded Systems Security. Une fois installé, Kaspersky Embedded Systems Security analyse les objets à l'aide des bases livrées avec le kit de distribution. Nous conseillons de réaliser une mise à jour immédiate des bases de Kaspersky Embedded Systems Security. Pour ce faire, vous devez lancer la tâche Mise à jour des bases de l'application. Par la suite, la mise à jour des bases de données sera exécutée toutes les heures selon la planification définie par défaut.

  Par exemple, vous pouvez lancer la tâche Mise à jour des bases de l'application à l'aide de l'instruction suivante :

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456 :
  ```

  Dans ce cas, les mises à jour des bases de données de Kaspersky Embedded Systems Security sont téléchargées depuis les serveurs de mise à jour de Kaspersky. La connexion à la source des mises à jour s'opère via le serveur proxy (adresse du proxy : proxy.company.com, port : 8080) et utilise l'authentification intégrée de Microsoft Windows pour accéder au serveur (NTLM-authentication) sous le compte utilisateur (nom d'utilisateur : inetuser ; mot de passe : 123456).

- Lancer une analyse rapide du périphérique si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur l'ordinateur protégé avant l'installation de Kaspersky Embedded Systems Security.

Pour réaliser la tâche Analyse rapide à l'aide d'une ligne de commande, exécutez la commande suivante :

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Cette instruction conserve le journal d'exécution de la tâche dans le fichier scancritical.log du dossier actif.

- Configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Embedded Systems Security.

Ajout et suppression de composants. Exemples de commandes

Le composant Contrôle du lancement des applications est installé automatiquement.

Pour installer le composant Analyse à la demande, exécutez la commande suivante :

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

ou

```
\product\setup.exe /s /p ADDLOCAL=Oas,Ods
```

Une fois que vous avez ajouté les composants à la liste, Kaspersky Embedded Systems Security réinstalle les composants existants et installe les composants indiqués.

Pour supprimer les composants installés, exécutez la commande suivante :

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Pour installer de nouveaux composants, exécutez la commande suivante :

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

Une fois que vous avez répertorié les composants que vous souhaitez installer et supprimer, Kaspersky Embedded Systems Security installe et supprime les composants en conséquence.

Désinstallation de Kaspersky Embedded Systems Security. Exemples de commandes

Pour désinstaller Kaspersky Embedded Systems Security du périphérique protégé, exécutez la commande suivante :

```
msiexec /x ess.msi /qn
```

ou

- Sous un système d'exploitation 32 bits :
  `msiexec /x {2CE8D225-8F60-49C9-82E3-C143D10D3CD4} /qn`

- Sous un système d'exploitation 64 bits :
  `msiexec /x {86D803C7-215D-4B46-A726-ED5AF57FC05D} /qn`

Pour désinstaller la console de Kaspersky Embedded Systems Security, saisissez la commande suivante :

```
msiexec /x esstools.msi /qn
```

ou

```
msiexec /x {71FB9E57-9F23-4D72-B762-E0314EF3C814} /qn
```

Pour désinstaller Kaspersky Embedded Systems Security d'un périphérique protégé sur lequel la protection par mot de passe est activée, exécutez la commande suivante :

- Sous un système d'exploitation 32 bits :
  `msiexec /x {2CE8D225-8F60-49C9-82E3-C143D10D3CD4} UNLOCK_PASSWORD=*** /qn`

- Sous un système d'exploitation 64 bits :
  `msiexec /x {86D803C7-215D-4B46-A726-ED5AF57FC05D} UNLOCK_PASSWORD=*** /qn`

Codes de retour

Le tableau ci-dessous décrit les codes de retour de la ligne de commande.

Codes de retour

Code	Description
1 324	Le nom du dossier d'installation contient des caractères interdits.
25 001	Privilèges insuffisants pour installer Kaspersky Embedded Systems Security. Afin d'installer l'application, lancez l'Assistant d'installation avec les privilèges d'administrateur local.
25 003	Impossible d'installer Kaspersky Embedded Systems Security sur des périphérique tournant sous cette version de Microsoft Windows. Veuillez lancer l'Assistant d'installation de l'application prévu pour la version 64 bits de Microsoft Windows.
25 004	Une application incompatible a été détectée. Avant de poursuivre l'installation, supprimez les applications suivantes de l'ordinateur à protéger : <liste des applications incompatibles>.
25 010	Le chemin d'accès indiqué ne peut être utilisé pour conserver des objets en quarantaine.
25 011	Le nom du dossier de conservation des objets en quarantaine contient des caractères interdits.
26 251	Échec du chargement de la DLL pour les Compteurs de performance.
26 252	Échec du chargement de la DLL pour les Compteurs de performance.
27	Impossible d'installer le pilote.

300	
27 301	Impossible de supprimer le pilote.
27 302	Impossible d'installer le composant réseau. Le seuil maximum d'appareils de filtrage pris en charge a été atteint.
27 303	Les bases antivirus sont introuvables.

Installation et suppression de l'application via Kaspersky Security Center

Cette section contient des informations générales sur l'installation de Kaspersky Embedded Systems Security via Kaspersky Security Center. Elle décrit également la procédure d'installation et de désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center et les actions à réaliser après l'installation de Kaspersky Embedded Systems Security.

Informations générales sur l'installation via Kaspersky Security Center

Vous pouvez installer Kaspersky Embedded Systems Security via Kaspersky Security Center à l'aide d'une tâche d'installation à distance.

Une fois que cette tâche a été exécutée, Kaspersky Embedded Systems Security est installé selon les mêmes paramètres sur plusieurs périphériques protégés.

Vous pouvez rassembler les périphériques protégés dans un seul groupe d'administration et créer une tâche de groupe pour l'installation de Kaspersky Embedded Systems Security sur les périphériques protégés de ce groupe.

Vous pouvez créer une tâche d'installation à distance de Kaspersky Embedded Systems Security pour une sélection de périphériques protégés qui n'appartiennent pas à un groupe d'administration. Lors de la création de cette tâche, vous devez constituer la liste des périphériques protégés distincts sur lesquels il faut installer Kaspersky Embedded Systems Security.

Le *Système d'aide de Kaspersky Security Center* contient des informations supplémentaires sur la tâche d'installation à distance.

Privilèges pour l'installation ou la désinstallation de Kaspersky Embedded Systems Security

Le compte utilisateur que vous spécifiez dans la tâche d'installation (de suppression) à distance doit appartenir au groupe d'administrateurs sur chacun des appareils protégés dans tous les cas, sauf dans les situations suivantes :

- Les périphériques protégés sur lesquels vous souhaitez installer Kaspersky Embedded Systems Security sont déjà dotés de l'Agent d'administration Kaspersky Security Center (quel que soit le domaine où se trouvent les périphériques protégés ou leur appartenance à un domaine quelconque).

Si l'Agent d'administration n'est pas encore installé sur les périphériques protégés, vous pouvez l'installer en même temps que Kaspersky Embedded Systems Security à l'aide d'une tâche d'installation à distance. Avant d'installer l'Agent d'administration, assurez-vous que le compte utilisateur indiqué dans la tâche appartient au groupe d'administrateurs sur chacun des appareils protégés.

- Tous les périphériques protégés sur lesquels vous souhaitez installer Kaspersky Embedded Systems Security se trouvent dans le même domaine que le Serveur d'administration et celui-ci est enregistré sous le compte Administrateur de domaine (**Domain Admin**) (si le compte jouit des privilèges d'administrateur local sur les périphériques protégés du domaine).

Par défaut, la tâche d'installation à distance selon la méthode **Installation forcée** s'exécute sous le compte sous les privilèges duquel le Serveur d'administration fonctionne.

Dans les tâches de groupe, ainsi que dans les tâches pour une sélection d'appareils protégés, en mode d'installation (désinstallation) forcée, le compte utilisateur doit posséder les autorisations suivantes sur l'appareil client :

- autorisation pour l'exécution à distance des applications ;
- autorisations sur le partage **Admin$** ;
- autorisation pour **Se connecter en tant que service**.

Installation de Kaspersky Embedded Systems Security via Kaspersky Security Center

Le Manuel d'implantation de Kaspersky Security Center contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

Si vous comptez administrer plus tard Kaspersky Embedded Systems Security via Kaspersky Security Center, assurez-vous que les conditions suivantes sont remplies :

- Le plug-in d'administration (fichier \product\klcfginst.exe du kit de distribution de Kaspersky Embedded Systems Security) est également installé sur le périphérique protégé sur lequel est installé le Serveur d'administration de Kaspersky Security Center.
- Sur les appareils protégés, l'Agent d'administration de Kaspersky Security Center est installé. Si les périphériques protégés ne sont pas dotés de l'Agent d'administration de Kaspersky Security Center, vous pouvez l'installer en même temps que Kaspersky Embedded Systems Security via une tâche d'installation à distance.

Vous pouvez également réunir au préalable les appareils dans un groupe d'administration afin de pouvoir ultérieurement administrer les paramètres de la protection à l'aide des stratégies ou des tâches de groupe de Kaspersky Security Center.

Pour installer Kaspersky Embedded Systems Security à l'aide d'une tâche d'installation à distance :

1. Lancement de la console d'administration de Kaspersky Security Center
2. Dans Kaspersky Security Center, développez le nœud **Avancé**.
3. Développez le nœud enfant **Installation à distance**.

4. Dans le volet résultats du nœud enfant **Paquets d'installation**, cliquez sur le bouton **Créer un paquet d'installation**.

5. En guise de type de paquet d'installation, sélectionnez l'option **Créer un paquet d'installation pour une application de Kaspersky**.

6. Entrez le nom du paquet d'installation.

7. Spécifiez le fichier ess.kud à partir du kit de distribution de Kaspersky Embedded Systems Security comme fichier du paquet d'installation.

   La fenêtre **Contrat de licence utilisateur final et Politique de confidentialité** s'ouvre.

8. Si vous acceptez les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **Je confirme que j'ai lu, compris et que j'accepte l'intégralité des termes de ce Contrat de licence utilisateur final** et **Je sais que mes données vont être traitées et transmises (y compris vers des pays tiers) conformément aux dispositions de la Politique de confidentialité et je l'accepte. J'ai lu la Politique de confidentialité dans sa totalité et je l'ai comprise** afin de procéder à l'installation.

   Vous devez accepter le Contrat de licence et la Politique de confidentialité.

9. Pour modifier la sélection des composants de Kaspersky Embedded Systems Security à installer et les paramètres d'installation par défaut dans le paquet d'installation :

   a. Dans Kaspersky Security Center, développez le nœud **Installation à distance**.

   b. Dans le panneau des résultats du nœud enfant **Paquets d'installation**, ouvrez le menu contextuel du paquet d'installation créé pour Kaspersky Embedded Systems Security et choisissez l'option **Propriétés**.

   c. Ouvrez la section **Configuration** de la fenêtre **Propriétés : <nom du paquet d'installation>**.

      Dans le groupe de paramètres **Composants installés**, cochez les cases en regard des noms des composants de Kaspersky Embedded Systems Security que vous souhaitez installer.

   d. Pour désigner un dossier de destination différent du dossier sélectionné par défaut, indiquez le nom du dossier et son chemin d'accès dans le champ **Dossier de destination**.

      Le chemin d'accès au répertoire cible peut contenir des variables système. Si le répertoire indiqué n'existe pas sur l'appareil protégé, il sera créé.

   e. Dans le groupe **Paramètres avancés d'installation**, définissez les valeurs suivantes :

      - **Réaliser une recherche de virus sur l'appareil protégé avant l'installation**
      - **Activer la protection en temps réel après l'installation de l'application**
      - **Ajouter les exclusions recommandées par Microsoft**
      - **Ajouter les fichiers recommandés par Kaspersky aux exclusions**
      - **Autoriser le lancement différé du service Kaspersky Security au démarrage du système d'exploitation**

   f. Dans la fenêtre **Propriétés : <nom du paquet d'installation>**, cliquez sur **OK**.

10. Dans le nœud **Paquets d'installation**, créez une tâche pour installer à distance Kaspersky Embedded Systems Security sur les périphériques protégés sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

    L'*Aide de Kaspersky Security Center* contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.

11. Lancez la tâche d'installation à distance de Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security est installé sur les périphériques protégés indiqués dans la tâche.

Actions à réaliser après l'installation de Kaspersky Embedded Systems Security

Après l'installation de Kaspersky Embedded Systems Security, il est conseillé de mettre à jour les bases de Kaspersky Embedded Systems Security sur les périphériques et de lancer l'analyse rapide des périphériques si ceux-ci n'étaient pas dotés d'un logiciel antivirus avec protection en temps réel activée avant l'installation de Kaspersky Embedded Systems Security.

Si les périphériques protégés sur lesquels vous avez installé Kaspersky Embedded Systems Security sont réunis au sein du même groupe d'administration dans Kaspersky Security Center, vous pouvez exécuter ces tâches de la manière suivante :

1. Créez des tâches de mise à jour des bases de l'application pour le groupe de périphériques protégés sur lesquels vous avez installé Kaspersky Embedded Systems Security. Désignez le Serveur d'administration Kaspersky Security Center comme source des mises à jour.

2. Créez une tâche de groupe d'analyse à la demande avec l'état Analyse rapide. Kaspersky Security Center évaluera l'état de la protection de chaque appareil protégé du groupe sur la base des résultats de cette tâche et non pas sur la base des résultats de l'Analyse rapide.

3. Créez une stratégie pour le groupe d'appareils protégés. Dans la section **Paramètres de l'application** des propriétés de la stratégie, désactivez le lancement programmé des tâches d'analyse à la demande système ainsi que des tâches de mise à jour des bases de l'application sur les appareils protégés du groupe d'administration dans la sous-section **Lancer les tâches locales du système**.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Embedded Systems Security.

Installation de la console de l'application via Kaspersky Security Center

Le Manuel d'implantation de Kaspersky Security Center contient des informations supplémentaires sur la création d'un paquet d'installation et de la tâche d'installation à distance.

Pour installer la console de l'application à l'aide d'une tâche d'installation à distance, procédez comme suit :

1. Dans la Console d'administration de Kaspersky Security Center, développez le nœud **Avancé**.

2. Développez le nœud enfant **Installation à distance**.

3. Dans le volet résultats du nœud enfant Paquets d'installation, cliquez sur le bouton **Créer un paquet d'installation**. Création d'un paquet d'installation :

a. Dans la fenêtre **Assistant Nouveau paquet d'installation**, sélectionnez **Créer un paquet d'installation pour le fichier exécutable défini** en tant que type de paquet.

b. Saisissez le nom du nouveau paquet d'installation.

c. Sélectionnez le fichier \console\setup.exe dans le dossier du kit de distribution de Kaspersky Embedded Systems Security, puis cochez la case **Copier tout le dossier dans le paquet d'installation**.

d. Utilisez l'option de ligne de commande ADDLOCAL dans le champ **Paramètres de lancement du fichier exécutable (facultatif)** pour effectuer l'installation de la Console de l'application. La Console de l'application est installée dans le dossier d'installation par défaut. Assurez-vous de définir le paramètre « CLUF=1 ». Sinon, il est impossible d'installer les composants.

```
/s /p "ADDLOCAL=MmcSnapin EULA=1"
```

Dans le champ **Paramètres de lancement du fichier exécutable (facultatif)**, vous pouvez utiliser l'option de ligne de commande ADDLOCAL pour modifier l'ensemble des composants à installer et l'option de ligne de commande INSTALLDIR pour indiquer le dossier de destination autre que default. Par exemple, pour effectuer une installation autonome de la Console de l'application dans le dossier C:\KasperskyConsole, utilisez l'option de ligne de commande suivante :

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
```

4. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la Console de l'application sur les appareils protégés sélectionnés (groupe d'administration). Configurez les paramètres de la tâche.

L'Aide de Kaspersky Security Center contient des informations supplémentaires sur la création et la configuration d'une tâche d'installation à distance.

5. Lancez la tâche d'installation à distance.

La console de l'application est installée sur les appareils protégés désignés dans la tâche.

Désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center

Les fichiers dump et de trace ne sont pas supprimés lors de la désinstallation de Kaspersky Embedded Systems Security. Vous pouvez supprimer manuellement les fichiers dump et de trace dans le dossier spécifié lors de la configuration de l'écriture des fichiers dump et de trace.

Si l'administration de Kaspersky Embedded Systems Security sur les périphérique du réseau est protégée par mot de passe, il faut saisir le mot de passe au moment de la création d'une tâche de désinstallation de plusieurs applications. Si la protection par mot de passe n'est pas gérée centralement par une stratégie de Kaspersky Security Center, Kaspersky Embedded Systems Security est supprimé sur les périphérique si le mot de passe saisi correspond à la valeur définie. Kaspersky Embedded Systems Security n'est pas désinstallé sur les autres périphériques protégés.

Pour désinstaller Kaspersky Embedded Systems Security :

1. Dans la Console d'administration Kaspersky Security Center, créez et lancez une tâche de suppression de l'application.

2. Dans la tâche, sélectionnez la méthode de désinstallation (comme vous aviez choisi la méthode d'installation, cf. section précédente) et désignez le compte utilisateur sous lequel le Serveur d'administration accèdera aux périphériques protégés. Vous pouvez désinstaller Kaspersky Embedded Systems Security uniquement avec les paramètres de désinstallation par défaut.

Installation et suppression via les stratégies de groupe Active Directory

Cette section décrit l'installation et la désinstallation de Kaspersky Embedded Systems Security via des stratégies de groupe d'Active Directory. Elle fournit également des informations sur les actions requises après l'installation de Kaspersky Embedded Systems Security via des stratégies de groupe.

Installation de Kaspersky Embedded Systems Security via des stratégies de groupe d'Active Directory

Vous pouvez installer Kaspersky Embedded Systems Security sur plusieurs périphériques protégés à l'aide d'une stratégie de groupe Active Directory. Vous pouvez, de la même manière, installer la console de l'application.

Les périphériques protégés sur lesquels vous souhaitez installer Kaspersky Embedded Systems Security ou la Console de l'application doivent appartenir au même domaine et à une seule unité d'organisation.

Les systèmes d'exploitation des périphériques protégés sur lesquels vous souhaitez installer Kaspersky Embedded Systems Security à l'aide de la stratégie doivent tous avoir le même nombre de bits (32 ou 64 bits).

Vous devez posséder les autorisations d'administrateur de domaine.

Pour installer Kaspersky Embedded Systems Security, utilisez les paquets d'installation ess_x86.msi ou ess_x64.msi. Pour installer la console de l'application, utilisez le paquet d'installation esstools.msi.

> La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

Pour installer Kaspersky Embedded Systems Security (ou la console de l'application) :

1. Enregistrez le fichier msi du paquet d'installation de la version correspondante du système d'exploitation de Microsoft Windows (32 ou 64 bits) dans un dossier partagé sur le contrôleur de domaine.

2. Enregistrer le fichier clé dans le même dossier partagé sur le contrôleur de domaine.

3. Dans ce dossier partagé sur le contrôleur de domaine, créez un fichier install_props.json contenant les éléments ci-après afin de confirmer que vous acceptez les dispositions du Contrat de licence et de la Politique de confidentialité.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. Sur le contrôleur de domaine, créez une stratégie pour groupe auquel appartiennent les appareils protégés.

5. A l'aide du **Group Policy Object Editor**, créez un nouveau paquet d'installation dans le nœud **Configuration ordinateur**. Saisissez le chemin d'accès au fichier msi pour Kaspersky Embedded Systems Security (de la Console de l'application) au format UNC (Universal Naming Convention).

6. Cochez la case **Toujours installer avec des droits élevés** du service Windows Installer aussi bien dans le nœud **Configuration ordinateur** que dans le nœud **Configuration utilisateur** du groupe sélectionné.

7. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Embedded Systems Security est installé sur les périphériques protégés du groupe après leur redémarrage.

Actions à réaliser après l'installation de Kaspersky Embedded Systems Security

Après l'installation de Kaspersky Embedded Systems Security sur les périphériques protégés, il est recommandé de procéder immédiatement à la mise à jour des bases de l'application et de lancer une analyse rapide. Vous pouvez réaliser ces actions depuis la console de l'application.

Vous pouvez également configurer les notifications destinées à l'administrateur relatives aux événements de Kaspersky Embedded Systems Security.

Désinstallation de Kaspersky Embedded Systems Security via des stratégies de groupe d'Active Directory

Les fichiers dump et de trace ne sont pas supprimés lors de la désinstallation de Kaspersky Embedded Systems Security. Vous pouvez supprimer manuellement les fichiers dump et de trace dans le dossier spécifié lors de la configuration de l'écriture des fichiers dump et de trace.

Si vous installez Kaspersky Embedded Systems Security (ou la Console de l'application) sur le groupe de périphérique protégés à l'aide d'une stratégie de groupe Active Directory, vous pourrez utiliser cette stratégie pour désinstaller Kaspersky Embedded Systems Security (ou la Console de l'application).

La suppression de l'application n'est possible que selon les paramètres de suppression par défaut.

La documentation de Microsoft contient des informations supplémentaires sur l'utilisation des stratégies de groupe Active Directory.

Si l'administration de l'application est protégée par mot de passe, il est impossible de désinstaller Kaspersky Embedded Systems Security à l'aide de stratégies de groupe Active Directory.

Pour désinstaller Kaspersky Embedded Systems Security (ou la Console de l'application) :

1. Sur le contrôleur de domaine, sélectionnez l'unité d'organisation contenant les périphériques protégés sur lesquels vous souhaitez désinstaller Kaspersky Embedded Systems Security ou la Console de l'application.

2. Sélectionnez la stratégie créée pour l'installation de Kaspersky Embedded Systems Security et dans **Éditeur des stratégies de groupe**, nœud **Installation des logiciels** (**Configuration ordinateur** > **Configuration des**

programmes > **Installation des logiciels**) ouvrez le menu contextuel du paquet d'installation de Kaspersky Embedded Systems Security (de la console de l'application) et sélectionnez la commande **Toutes les tâches** > **Supprimer**.

3. Sélectionnez la méthode de suppression **Désinstaller immédiatement le logiciel des ordinateurs des utilisateurs**.

4. Appliquez les modifications à l'aide de l'instruction `gpupdate /force`.

Kaspersky Embedded Systems Security est supprimé des périphériques protégés après leur redémarrage et avant l'ouverture de session dans Microsoft Windows.

Vérification des fonctions de Kaspersky Embedded Systems Security. Utilisation du virus d'essai EICAR

Cette section décrit le virus d'essai EICAR et explique comment l'utiliser pour confirmer le fonctionnement de la Protection des fichiers en temps réel et de l'Analyse à la demande de Kaspersky Embedded Systems Security.

A propos du virus d'essai EICAR

Le virus d'essai vise à vérifier le fonctionnement des logiciels antivirus. Il a été développé par l'organisation The European Institute for Computer Antivirus Research (EICAR).

Le virus d'essai n'est pas un objet malveillant et il ne contient pas un code exécutable qui pourrait nuire à votre appareil mais les logiciels antivirus de la majorité des éditeurs le considèrent comme une menace.

Le fichier qui contient le virus d'essai s'appelle eicar.com. Vous pouvez le télécharger depuis le site Internet du projet EICAR.

Avant d'enregistrer le fichier dans un répertoire sur le disque dur du périphérique, assurez-vous que la Protection des fichiers en temps réel est désactivée sur ce répertoire.

Le fichier eicar.com contient une ligne de texte. Pendant l'analyse, Kaspersky Embedded Systems Security découvre la menace test dans cette ligne de texte, attribue l'état **Infecté** au fichier et le supprime. Les informations sur la menace découverte dans le fichier apparaissent dans la console de l'application, dans le journal d'exécution de la tâche.

Vous pouvez également utiliser le fichier eicar.com afin de voir comment Kaspersky Embedded Systems Security désinfecte les objets infectés et comment il découvre les objets probablement infectés. Pour ce faire, ouvrez le fichier à l'aide d'un éditeur de texte, ajoutez au début de la ligne de texte un des préfixes repris au tableau ci-après et enregistrez le fichier sous un nouveau nom, par exemple eicar_cure.com.

Pour s'assurer que Kaspersky Embedded Systems Security traite le fichier eicar.com avec un préfixe, dans la section des paramètres de sécurité **Protection des objets**, indiquez la valeur **Tous les objets** pour les tâches Protection en temps réel de l'ordinateur et Analyse à la demande de Kaspersky Embedded Systems Security.

Préfixe des fichiers EICAR

Préfixe	État du fichier après l'analyse et l'action de Kaspersky Embedded Systems Security

Sans préfixe	**Kaspersky Embedded Systems Security attribue l'état Infecté à l'objet et le supprime.**
SUSP–	Kaspersky Embedded Systems Security attribue l'état **Probablement infecté** à l'objet découvert à l'aide de l'analyse heuristique et le supprime vu que les objets probablement infectés ne sont pas désinfectés.
WARN–	Kaspersky Embedded Systems Security attribue l'état **Probablement infecté** à l'objet (le code de l'objet correspond en partie à un code malveillant connu) et le supprime vu que les objets probablement infectés ne sont pas désinfectés.
CURE–	Kaspersky Embedded Systems Security attribue l'état **Infecté** à l'objet et le désinfecte. Si la désinfection a réussi, tout le texte du fichier est remplacé par le mot "CURE".

Vérification de la Protection des fichiers en temps réel et de l'Analyse à la demande

Après l'installation de Kaspersky Embedded Systems Security, vous pouvez confirmer que Kaspersky Embedded Systems Security trouve les objets qui contiennent du code malveillant. Pour la vérification, vous pouvez utiliser un virus d'essai EICAR.

Pour vérifier la fonction Protection des fichiers en temps réel :

1. Téléchargez le fichier eicar.com du site Internet d'EICAR. Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel appareil du réseau.

   Avant d'enregistrer le fichier dans un dossier, assurez-vous que la Protection des fichiers en temps réel est désactivée pour ce dossier.

2. Si vous souhaitez également vérifier le fonctionnement des notifications des utilisateurs du réseau, assurez-vous que le service Windows Messenger de Microsoft est activé sur l'appareil protégé et sur l'appareil sur lequel vous avez enregistré le fichier eicar.com.

3. Ouvrez la console de l'application sur l'appareil protégé.

4. Copiez le fichier eicar.com enregistré sur le disque local de l'appareil protégé selon une des méthodes suivantes :

   - Pour vérifier le fonctionnement des notifications via une fenêtre du service des terminaux, copiez le fichier eicar.com sur l'appareil protégé connecté à la console à l'aide du programme "Connexion au poste de travail distant" (Remote Desktop Connection).

   - Pour vérifier le fonctionnement des notifications via le service Windows Messenger, copiez le fichier eicar.com depuis l'appareil sur lequel vous l'avez enregistré via l'environnement de réseau de cet appareil.

La Protection des fichiers en temps réel fonctionne comme il se doit si les événements suivants se produisent :

- Le fichier eicar.com est supprimé de l'appareil protégé.

- Dans la Console de l'application, le journal d'exécution de la tâche reçoit l'état *Critique*. Le journal comporte une nouvelle ligne avec des informations sur une menace dans le fichier eicar.com.

- Un message du service Windows Messenger sur l'appareil d'où vous avez copié le fichier (service de terminal dans la session terminal sur l'appareil) dont le texte est : `Kaspersky Embedded Systems Security a interdit l'accès à <chemin d'accès au fichier eicar.com sur l'appareil>\eicar.com sur l'appareil <nom réseau de l'appareil> à <heure de l'événement>. Cause : menace détectée. Virus : EICAR-Test-File. Nom d'utilisateur : <nom d'utilisateur>. Nom de l'ordinateur : <nom réseau de l'appareil d'où vous avez copié le fichier>`.

  > Assurez-vous que le service Windows Messenger de Microsoft fonctionne sur l'appareil d'où vous avez copié le fichier eicar.com.

Pour vérifier la fonction Analyse à la demande :

1. Téléchargez le fichier eicar.com du site Internet d'EICAR. Enregistrez-le dans un dossier partagé sur le disque local de n'importe quel appareil du réseau.

   > Avant d'enregistrer le fichier dans un dossier, assurez-vous que la Protection des fichiers en temps réel est désactivée pour ce dossier.

2. Ouvrez la Console de l'application et développez le nœud **Analyse à la demande** dans l'arborescence de la Console de l'application.
3. Sélectionnez le nœud enfant **Analyse rapide**.
4. Sous l'onglet **Configuration de la zone d'analyse**, ouvrez le menu contextuel du nœud **Réseau**, puis choisissez **Ajouter un fichier de réseau**.
5. Saisissez le chemin d'accès réseau au fichier eicar.com sur l'appareil distant au format UNC (Universal Naming Convention).
6. Cochez la case **Chemin d'accès à l'objet** afin d'inclure le chemin de réseau dans la zone d'analyse.
7. Lancez la tâche Analyse rapide.

L'analyse à la demande fonctionne correctement si les conditions suivantes sont remplies :

- Le fichier eicar.com est supprimé du disque dur de l'appareil.
- Dans la Console de l'application, le journal d'exécution de la tâche reçoit l'état *Critique*. Le journal de la tâche Analyse des zones critiques comporte une nouvelle ligne avec des informations sur une menace dans le fichier eicar.com.

Interface de l'application

Vous pouvez contrôler Kaspersky Embedded Systems Security à l'aide des interfaces suivantes :

- Console de l'application locale.
- Console d'administration de Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Console d'administration de Kaspersky Security Center

Kaspersky Security Center vous permet d'installer et de désinstaller à distance, de démarrer et d'arrêter Kaspersky Embedded Systems Security, de configurer les paramètres de l'application, de modifier l'ensemble des composants de l'application disponibles, d'ajouter des clés et de lancer et d'arrêter des tâches.

L'application peut être administrée via Kaspersky Security Center à l'aide du plug-in Kaspersky Embedded Systems Security. Vous trouverez toutes les informations détaillées sur l'interface de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

Kaspersky Security Center Web Console et Cloud Console

Kaspersky Security Center Web Console (ci-après également appelé Web Console) est une application Web destinée à l'exécution centralisée des principales tâches d'administration et de maintenance du système de sécurité du réseau d'une organisation. Web Console est un composant de Kaspersky Security Center qui fournit une interface utilisateur. Pour en savoir plus sur Kaspersky Security Center Web Console, reportez-vous à l'*aide de Kaspersky Security Center*.

Kaspersky Security Center Cloud Console (ci-après également appelé Cloud Console) est une solution Cloud pour la protection et l'administration du réseau d'une organisation. Pour en savoir plus sur Kaspersky Security Center Cloud Console, reportez-vous à l'*aide de Kaspersky Security Center Cloud Console*.

Web Console et Cloud Console vous permettent d'effectuer les opérations suivantes :

- Surveiller l'état du système de sécurité de votre organisation.
- Installer les applications de Kaspersky sur les appareils de votre réseau.
- Gérer les applications installées.
- Afficher les rapports sur l'état du système de sécurité.

Licence de l'application

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

A propos du Contrat de licence utilisateur final

Le *Contrat de Licence Utilisateur Final* est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

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

Vous pouvez lire les termes du Contrat de licence utilisateur final et de la Politique de confidentialité, qui décrit le traitement et la transmission des données, de la manière suivante :

- Lors de l' installation de Kaspersky Embedded Systems Security.
- Dans le menu **Démarrer** (**Tous les programmes** > **Kaspersky Embedded Systems Security** > **CLUF et Politique de confidentialité**) après l'installation.
- Lors de l'installation de Kaspersky Fraud Prevention Cloud.
- En lisant le fichier license.txt inclus dans le kit de distribution.
- Sur le site Internet de Kaspersky (https://www.kaspersky.ru/business/eula).

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 et vous ne pouvez pas utiliser l'application.

A propos de la licence

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

Une licence valide vous permet d'utiliser l'application conformément aux termes du Contrat de licence utilisateur final ainsi que de recevoir une assistance technique si nécessaire.

La zone de service et la période d'utilisation de l'application dépendent du type de licence utilisé pour activer l'application.

Vous pouvez activer l'application de deux manières :

- À l'aide d'un fichier clé qui vous permet d'utiliser l'application sous une licence commerciale :
- À l'aide d'un code d'activation pour acheter une licence commerciale.

Vous pouvez acheter une licence standard de Kaspersky Embedded Systems Security ou une licence étendue de Kaspersky Embedded Systems Security Compliance Edition qui inclut trois modules supplémentaires d'inspection du système : Moniteur d'intégrité des fichiers, Inspection des journaux et Moniteur d'accès au registre.

Lorsqu'une licence commerciale expire, l'application continue de s'exécuter, mais les fonctionnalités suivantes deviennent indisponibles :

- Intégration à Kaspersky Security Network ;
- Mise à jour des bases de Kaspersky Embedded Systems Security.

Lorsqu'une clé de licence expire, l'application continue de s'exécuter ; les tâches **Analyse à la demande** et **Protection des fichiers en temps réel** sont toujours disponibles, mais toutes les autres tâches, ainsi que la mise à jour des bases de Kaspersky Embedded Systems Security ne sont plus disponibles. Il en va de même si Kaspersky ajoute votre licence à la liste de refus.

Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky Embedded Systems Security, il faut renouveler votre licence.

Il est conseillé de renouveler la validité de la licence avant sa date d'expiration afin de garantir la protection maximale de l'appareil.

Assurez-vous que la date d'expiration de la clé additionnelle est postérieure à celle de la clé active.

A propos du certificat de licence

Un *certificat de licence* est un document qui vous est remis avec le fichier clé ou le code d'activation (le cas échéant).

Le certificat de licence reprend les informations suivantes relatives à la licence actuelle :

- Numéro de la commande ;
- Informations sur l'utilisateur qui a obtenu la licence ;
- Informations sur l'application qui peut être activée à l'aide de la licence octroyée ;
- Limite du nombre d'unités sous licence (par exemple, les appareils sur lesquels l'application peut être utilisée sous les termes de la licence fournie) ;
- Date de début de validité de la licence ;
- Date d'expiration de la licence ou dispositions de la licence ;
- Type de licence.

A propos de la clé

La *clé* est une séquence d'octets qui permet d'activer l'application en vue de son utilisation dans le respect des dispositions du Contrat de licence utilisateur final. La clé est générée par Kaspersky.

Vous pouvez ajouter une clé à l'application en utilisant un fichier clé. La clé apparaît dans l'interface de l'application sous la forme d'une séquence alphanumérique unique après que vous l'avez ajoutée à l'application.

Kaspersky peut ajouter une clé à la liste de refus suite à une violation du contrat de licence. Si la clé est bloquée, il faudra en ajouter une autre pour pouvoir utiliser l'application.

Une clé peut être active ou additionnelle.

Clé active est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour une licence commerciale ou d'essai peut être ajoutée en tant que clé active. L'application ne peut pas contenir plus d'une clé active.

La *Clé additionnelle* est une clé qui confirme le droit d'utilisation de l'application, non utilisée au moment actuel. Une clé additionnelle devient automatiquement une clé active à l'expiration de la validité de la licence associée à la clé active en cours. Une clé additionnelle ne peut être ajoutée que si une clé active existe.

A propos du fichier clé

Un *fichier clé* est un fichier portant l'extension .key qui vous est remis par Kaspersky. Les fichiers clé permet d'ajouter une clé de licence pour activer l'application.

Le fichier clé est envoyé à l'adresse email que vous avez indiquée au moment de l'achat de Kaspersky Embedded Systems Security ou après avoir sollicité une version d'essai de Kaspersky Embedded Systems Security.

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

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

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

- Contactez le vendeur de la licence.
- Obtenez un fichier clé via le site Internet de Kaspersky en utilisant votre code d'activation.

A propos du code d'activation

Un *code d'activation* est une séquence unique de 20 caractères alphanumériques. Vous devez saisir un code d'activation pour ajouter une clé d'activation de Kaspersky Embedded Systems Security. Le code d'activation est envoyé à l'adresse email que vous avez indiquée au moment de l'achat de Kaspersky Embedded Systems Security ou après avoir sollicité une version d'essai de Kaspersky Embedded Systems Security.

Pour activer l'application avec un code d'activation, vous avez besoin d'un accès Internet pour vous connecter aux serveurs d'activation de Kaspersky.

Si vous avez perdu votre code d'activation après l'installation de l'application, vous pouvez le récupérer. Vous aurez besoin du code d'activation pour ouvrir un Kaspersky CompanyAccount par exemple. Pour récupérer votre code d'activation, contactez le partenaire de Kaspersky Lab auprès duquel vous avez acheté la licence.

A propos de la collecte des données

Le contrat de licence de Kaspersky Embedded Systems Security, notamment la section intitulée "Conditions du traitement des données", spécifie les conditions, la responsabilité et la procédure de traitement des données indiquées dans ce Guide. Avant d'accepter le contrat de licence, révisez attentivement ses conditions, ainsi que tous les documents liés au contrat de licence.

Les données que vous envoyez à Kaspersky lorsque vous utilisez l'application sont protégées et traitées conformément à la Politique de confidentialité disponible à l'adresse www.kaspersky.com/Products-and-Services-Privacy-Policy.

Les termes du Contrat de licence et de la Politique de confidentialité peuvent être consultés lors de l'installation de Kaspersky Embedded Systems Security, dans le kit de distribution, et depuis le menu **Démarrer** (**Tous les programmes** > **Kaspersky Embedded Systems Security** > **CLUF et Politique de confidentialité**) après l'installation.

Lors de la désinstallation de Kaspersky Embedded Systems Security, toutes les données stockées par Kaspersky Embedded Systems Security sur le périphérique protégé sont supprimées.

En acceptant les conditions du contrat de licence, vous acceptez d'envoyer automatiquement les données suivantes à Kaspersky :

- Pour prendre en charge le mécanisme de réception de mises à jour : informations sur l'application installée et son activation : identifiant de l'application en cours d'installation et version complète, y compris le numéro de version, le type et l'identifiant de licence, identifiant d'installation, identifiant de la tâche de mise à jour.
- Pour accéder aux articles de la base de connaissances en cas d'erreurs de l'application (service de redirection) : informations sur le type d'application et de lien : le nom, l'environnement local et le numéro de version complète de l'application, type de lien de redirection et identifiant d'erreur.
- Pour gérer les confirmations du traitement des données : informations sur l'état d'acceptation des contrats de licence et des autres documents, qui stipulent les conditions de transfert des données : identifiant et version du contrat de licence ou des autres documents, comprenant les conditions acceptées ou refusées du traitement des données, attribut désignant l'action de l'utilisateur (confirmation ou rappel de l'acceptation des conditions) ; date et heure des changements d'état de l'acceptation des conditions de traitement des données.

Traitement des données locales

Tout en exécutant les fonctions principales de l'application décrites dans ce Guide, Kaspersky Embedded Systems Security traite et stocke en local une séquence de données sur l'ordinateur protégé.

Le tableau ci-dessous contient des informations sur le traitement local et le stockage par Kaspersky Embedded Systems Security des données contenues dans les rapports.

Traitement et stockage des données contenues dans les rapports

Domaine fonctionnel	Enregistrement des événements
Type d'utilisation	Kaspersky Embedded Systems Security stocke les données localement et les envoie au Serveur d'administration. La base de données du Serveur d'administration stocke des informations sur les événements de l'application qui se produisent sur les périphériques protégés administrés.
Stockage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<version du produit>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx

	• Base de données du Serveur d'administration
Mesures de sécurité	Liste de contrôle de l'accès.
Période de stockage	Kaspersky Embedded Systems Security stocke les données jusqu'à la désinstallation de Kaspersky Embedded Systems Security. Lors de la désinstallation de Kaspersky Embedded Systems Security, toutes les données stockées par Kaspersky Embedded Systems Security sur le périphérique protégé sont supprimées.
Fonction	Fournir une fonctionnalité principale.

Kaspersky Embedded Systems Security ne supprime pas les événements du journal des événements Windows, y compris lors de la désinstallation de Kaspersky Embedded Systems Security.

Afin de fournir une fonctionnalité d'enregistrement d'événement, Kaspersky Embedded Systems Security traite localement les données suivantes :

- Noms, sommes de contrôle (MD5, SHA-256) et attributs des fichiers traités et leurs chemins d'accès complets sur le support numérisé.
- Actions réalisées sur les fichiers analysés par Kaspersky Embedded Systems Security.
- Actions réalisées par l'utilisateur sur les fichiers numérisés sur l'ordinateur protégé.
- Informations sur les comptes d'utilisateurs effectuant des actions sur le réseau protégé ou le périphérique protégé.
- Valeurs du chemin d'accès à l'instance du périphérique pour les périphériques ajoutés aux règles du Contrôle des périphériques.
- Informations sur les processus et scripts exécutés sur le système : sommes de contrôle (MD5, SHA-256) et chemins d'accès complets aux fichiers exécutables, informations relatives aux certificats numériques.
- Paramètres du pare-feu Windows.
- Entrées du journal des événements Windows.
- Noms des comptes utilisateur exécutant des actions sur les fichiers analysés sur l'ordinateur protégé.
- Instances de fichiers exécutables en cours de démarrage et types, noms, sommes de contrôle et attributs de ces fichiers.
- Informations sur l'activité réseau :
  - Adresses IP des périphériques externes bloqués.
  - Adresses IP traitées.
- Informations sur l'état du journal Windows USN.

Le tableau suivant contient des informations sur les données de service traitées par Kaspersky Embedded Systems Security. Les données de service comprennent : les paramètres de l'application, les fichiers mis en quarantaine et placés dans la sauvegarde, les informations dans les bases de données de service de l'application, les données de licence.

Le tableau ci-dessous contient des informations sur le traitement local et le stockage par Kaspersky Embedded Systems Security des données relatives aux paramètres définis par un utilisateur.

Traitement et stockage des données relatives aux paramètres spécifiés par un utilisateur

Domaine fonctionnel	Toutes les fonctionnalités de Kaspersky Embedded Systems Security
Type d'utilisation	Kaspersky Embedded Systems Security stocke les données localement et les envoie au Serveur d'administration. Les données sont stockées dans la base de données du Serveur d'administration. Les données traitées dans l'application en local ne sont pas automatiquement envoyées à Kaspersky ou à d'autres systèmes tiers.
Stockage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<version du produit>\ • Base de données du Serveur d'administration
Mesures de sécurité	Liste de contrôle de l'accès.
Période de traitement	Kaspersky Embedded Systems Security stocke les données jusqu'à la désinstallation de Kaspersky Embedded Systems Security. Lors de la désinstallation de Kaspersky Embedded Systems Security, toutes les données stockées par Kaspersky Embedded Systems Security sur le périphérique protégé sont supprimées. Kaspersky Embedded Systems Security ne supprime pas les données relatives aux paramètres exportés dans le fichier de configuration. Kaspersky Embedded Systems Security ne supprime pas les objets de quarantaine et les objets de sauvegarde si les cases **Exporter les objets de la quarantaine** et **Exporter les objets de la sauvegarde** sont cochées dans l'assistant de configuration.
Fonction	Fournir une fonctionnalité principale.

À des fins spécifiques, Kaspersky Embedded Systems Security traite localement les données suivantes :

- Objets placés en quarantaine ou en sauvegarde.
- Informations sur les comptes utilisateur (nom d'utilisateur et mot de passe) sous lesquels Kaspersky Embedded Systems Security exécute les tâches.
- Mot de passe de Kaspersky Embedded Systems Security.
- Adresses IP et identificateurs des sessions de connexion bloquées.
- Paramètres du pare-feu Windows et paramètres des règles du pare-feu Windows.
- Sommes de contrôle (MD5, SHA-256) et chemins d'accès aux fichiers exécutables ajoutés aux règles de tâche Contrôle du lancement des applications.

- Valeurs du chemin d'accès à l'instance du périphérique pour les périphériques ajoutés aux règles du Contrôle des périphériques.
- Informations sur les fichiers et dossiers inclus dans les zones d'action des tâches de Kaspersky Embedded Systems Security.
- Adresses IP incluses dans la zone de protection ou exclues de celle-ci.
- Informations relatives aux événements du journal des événements Windows.
- Informations sur les détections à l'aide de la technologie iSwift ou iCheker.
- Sommes de contrôle (MD5, SHA-256), chemins d'accès complets et masques définis dans les paramètres d'exclusion.
- Informations sur les processus ajoutés à la zone de confiance.
- Informations sur les clés de licence ajoutées.
- Informations sur les certificats numériques.
- Fichiers décompressés d'une archive ou d'un autre objet composé pendant l'analyse.

Kaspersky Embedded Systems Security traite et stocke les données, ce qui fait partie de la fonctionnalité de base de l'application, notamment pour enregistrer dans le journal les événements de l'application et recevoir des données de diagnostic. Les données traitées en local sont en outre protégées conformément aux paramètres configurés et appliqués de l'application.

Kaspersky Embedded Systems Security vous permet de configurer le niveau de protection des données traitées localement (Gestion des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security, Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security) : vous pouvez modifier les droits d'accès des utilisateurs aux données du processus, modifier les périodes de conservation de ces données, désactiver entièrement ou partiellement la fonctionnalité qui implique l'enregistrement des événements dans le journal des données et modifier le chemin et les attributs du dossier où les données sont enregistrées.

Les données traitées dans l'application en local ne sont pas automatiquement envoyées à Kaspersky ou à d'autres systèmes tiers.

Par défaut, toutes les données traitées localement par l'application en cours de fonctionnement sont retirées après la suppression de Kaspersky Embedded Systems Security du périphérique protégé.

Font exception les fichiers contenant des informations de diagnostic (fichiers de trace et dump), les événements de l'application dans le journal des événements Windows et les fichiers contenant les paramètres exportés de Kaspersky Embedded Systems Security. Il est recommandé de supprimer manuellement ces fichiers.

Vous trouverez des informations détaillées sur l'utilisation de fichiers contenant les données de diagnostic de l'application dans les sections correspondantes de ce guide.

Vous pouvez supprimer les fichiers journaux des événements Windows contenant les événements de l'application Kaspersky Embedded Systems Security via les moyens standard du système d'exploitation.

Traitement des données locales à l'aide des composants auxiliaires de l'application

Le paquet d'installation de Kaspersky Embedded Systems Security comprend des composants auxiliaires de l'application qui peuvent être installés sur votre périphérique même si Kaspersky Embedded Systems Security n'y est pas installé. Ces composants auxiliaires sont les suivants :

- Console de l'application. Ce composant est inclus dans les Outils d'administration de Kaspersky Embedded Systems Security et représenté par un composant logiciel enfichable Microsoft Management Console.

- Plug-in d'administration. Ce composant assure une intégration complète avec l'application Kaspersky Security Center.

Tout en assurant les fonctions principales de l'application décrite dans ce Guide, les composants auxiliaires de l'application traitent et stockent en local un ensemble de données sur le périphérique protégé où ils sont installés même s'ils sont installés séparément de Kaspersky Embedded Systems Security.

Les composants de l'application traitent en local et stockent les données suivantes :

- Console de l'application : nom du périphérique protégé hébergeant Kaspersky Embedded Systems Security (adresse IP ou nom de domaine) auquel la Console de l'application s'est connectée à distance pour la dernière fois ; paramètres d'affichage configurés dans le composant logiciel enfichable Microsoft Management Console ; données concernant le dernier dossier dans lequel l'utilisateur a sélectionné des objets via la Console de l'application (à l'aide d'une boîte de dialogue ouverte via le bouton **Parcourir**). Les fichiers de trace de la Console de l'application peuvent également contenir les données suivantes : nom de l'appareil protégé hébergeant l'application Kaspersky Embedded Systems Security auquel la connexion à distance a été effectuée, nom du compte utilisateur sous lequel la connexion à distance a été établie.

- Le Plug-in d'administration peut traiter et stocker temporairement des données traitées par Kaspersky Embedded Systems Security ; par exemple les paramètres configurés des tâches et des composants de l'application, les paramètres des stratégies de Kaspersky Security Center, les données envoyées dans les listes de réseau.

Le tableau ci-dessous contient des informations sur le traitement local et le stockage par Kaspersky Embedded Systems Security des données écrites dans des fichiers dump et de trace.

Kaspersky Embedded Systems Security traite et stocke localement les données suivantes écrites dans des fichiers dump et de trace :

- Informations sur les actions effectuées par Kaspersky Embedded Systems Security sur le périphérique protégé.

- Informations relatives aux objets traités par Kaspersky Embedded Systems Security.

- Informations sur l'activité sur le périphérique protégé traitées par Kaspersky Embedded Systems Security.

- Informations relatives aux erreurs survenues lors de l'exécution de Kaspersky Embedded Systems Security.

Les données traitées par les composants auxiliaires ne sont pas automatiquement envoyées à Kaspersky ou à d'autres systèmes tiers.

Par défaut, toutes les données traitées en local par les composants auxiliaires de l'application en cours de fonctionnement sont supprimées après la désinstallation de ces composants.

Font exception les fichiers de trace des composants auxiliaires de l'application. Il est recommandé de les supprimer manuellement.

Données dans les fichiers dump et de trace

Kaspersky Embedded Systems Security peut, conformément aux paramètres, écrire des informations de débogage dans les fichiers de trace à des fins d'assistance technique pendant le fonctionnement de Kaspersky Embedded Systems Security.

Les fichiers dump de Kaspersky Embedded Systems Security sont générés par le système d'exploitation lors des pannes d'application et sont écrasés par la panne suivante.

Les fichiers dump et de trace peuvent inclure toutes les données personnelles d'un utilisateur ou les données confidentielles de votre organisation.

N'utilisez pas Kaspersky Embedded Systems Security sur des périphériques pour lesquels la soumission de données est interdite par la politique de votre organisation.

Par défaut, Kaspersky Embedded Systems Security n'enregistre pas les informations de débogage.

Les fichiers dump et de trace et ne sont pas automatiquement envoyés au-delà de l'hôte sur lequel ils ont été générés. Le contenu des fichiers de trace peut être affiché à l'aide des visionneuses de fichiers texte standard. Les fichiers dump et de trace sont conservés indéfiniment et ne sont pas supprimés lors de la désinstallation de Kaspersky Embedded Systems Security.

Les informations de débogage peuvent être utiles pour le Support Technique.

Aucun mécanisme spécial n'est fourni pour limiter l'accès aux fichiers dump et de trace. L'administrateur peut configurer ces données de telle sorte qu'elles soient écrites dans un dossier protégé.

Le chemin d'accès au dossier de fichiers dump et de trace n'est pas configuré par défaut. Pour utiliser le dossier dump et de trace, l'administrateur doit le spécifier.

Les données des fichiers dump et de trace peuvent contenir :

- Des actions effectuées par Kaspersky Embedded Systems Security sur l'hôte.
- Des informations relatives aux objets traités par Kaspersky Endpoint Agent.
- Les erreurs survenues lors du fonctionnement de Kaspersky Endpoint Agent.

Activation de l'application à l'aide d'un fichier clé

Vous pouvez activer Kaspersky Embedded Systems Security en appliquant un fichier clé.

Si Kaspersky Embedded Systems Security possède déjà une clé active et si vous ajoutez une autre clé en tant que clé active, la nouvelle clé remplacera l'ancienne. La clé ajoutée antérieurement est supprimée.

Si Kaspersky Embedded Systems Security possède déjà une clé additionnelle et si vous ajoutez une autre clé en tant que clé additionnelle, la nouvelle clé remplacera l'ancienne. La clé additionnelle ajoutée antérieurement est supprimée.

Si une clé additionnelle et une clé active avaient déjà été ajoutées à Kaspersky Embedded Systems Security et que vous ajoutez une nouvelle clé en tant que clé active, cette nouvelle clé remplace la clé active antérieure et la clé additionnelle n'est pas supprimée.

Pour activer Kaspersky Embedded Systems Security en appliquant un fichier clé :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Licence**.
2. Dans le volet résultats du nœud **Licence**, cliquez sur le lien **Ajouter une clé**.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**.
4. Sélectionnez un fichier clé portant l'extension .key.

   Vous pouvez aussi ajouter une clé en tant que clé additionnelle. Pour ce faire, cochez la case **Utiliser en tant que clé additionnelle**.

5. Cliquez sur le bouton **OK**.

Le fichier clé sélectionné sera appliqué. Les informations sur la clé ajoutée s'affichent dans le nœud **Licence**.

Activation de l'application à l'aide d'un code d'activation

Pour activer l'application à l'aide d'un code d'activation, l'appareil protégé doit être connecté à Internet.

Vous pouvez activer Kaspersky Embedded Systems Security à l'aide d'un code d'activation.

Lors de l'activation de l'application selon cette méthode, Kaspersky Embedded Systems Security envoie des données au serveur d'activation pour vérifier le code saisi :

- Si la vérification du code d'activation réussit, l'application est activée.
- Si la vérification du code d'activation échoue, la notification correspondante apparaît. Dans ce cas, vous devez contacter le fournisseur de logiciels auprès duquel vous avez acheté votre licence Kaspersky Embedded Systems Security.
- Si le nombre d'activations avec le code d'activation est dépassé, la notification correspondante apparaît. La procédure d'activation de l'application est interrompue et l'application vous recommande de contacter le Support Technique de Kaspersky.

Vous pouvez activer Kaspersky Embedded Systems Security à l'aide d'un code d'activation via la Console de l'application ou en créant la tâche de groupe Activation de l'application via le plug-in d'administration ou via le Web Plug-in.

Pour activer Kaspersky Embedded Systems Security à l'aide d'un code d'activation via la Console de l'application :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Licence**.
2. Dans le volet résultats du nœud **Licence**, cliquez sur le lien **Ajouter un code d'activation**.
3. Dans la fenêtre qui s'ouvre, saisissez le code d'activation dans le champ **Code d'activation**.
   - Si vous souhaitez utiliser le code d'activation en tant que clé additionnelle, cochez la case **Utiliser en tant que clé additionnelle**.
   - Si vous souhaitez afficher les informations sur la licence, cliquez sur le bouton **Afficher les informations sur la licence** ; elles apparaîtront dans la zone de groupe **Informations relatives à la licence**.
4. Cliquez sur le bouton **OK**.

   Kaspersky Embedded Systems Security envoie au serveur d'activation des informations sur le code d'activation appliqué.

Consultation des informations sur la licence active

Consultation des informations sur la licence

Les informations sur la licence active s'affichent dans le panneau de détails du nœud **Kaspersky Embedded Systems Security** de la Console de l'application. Une clé peut afficher les états suivants :

- **Vérification de l'état de la clé** : Kaspersky Embedded Systems Security analyse le fichier clé ou le code d'activation appliqué, puis attend une réponse concernant l'état de la clé actuelle.
- **Date d'expiration de la licence** : Kaspersky Embedded Systems Security est actif jusqu'à la date et l'heure indiquées. L'état de la clé est mis en évidence en jaune dans les cas suivants :
  - Il reste 14 jours avant l'expiration de la licence et aucune clé additionnelle n'a été appliquée.
  - La clé ajoutée est inscrite sur la liste de refus et va bientôt être bloquée.
- **Licence expirée** : Kaspersky Embedded Systems Security n'est pas actif parce que la licence a expiré. L'état est mis en évidence en rouge.
- **Violation du Contrat de licence utilisateur final** : Kaspersky Embedded Systems Security n'est pas actif en raison d'une violation des conditions du Contrat de licence utilisateur final. L'état est mis en évidence en rouge.
- **Clé ajoutée à la liste de refus** : la clé ajoutée a été bloquée et inscrite sur la liste de refus par les experts de Kaspersky, par exemple, en cas d'utilisation d'une clé par des tiers pour l'activation illicite d'une application. L'état est mis en évidence en rouge.

Consultation des informations sur la licence active

Pour consulter les informations sur la licence active, procédez comme suit :

Dans l'arborescence de la console de l'application, développez le nœud **Licence**.

Les informations générales relatives à la licence active apparaissent dans le panneau de détails du nœud **Licence** (cf. tableau ci-dessous).

Informations générales sur la licence dans le nœud Licence

Champ	Description
Code d'activation	Le code d'activation. Le champ se remplit si vous activez l'application à l'aide d'un code d'activation.
État de l'activation	Informations sur l'état de l'activation de l'application. La colonne **État de l'activation** du panneau de détails du nœud **Licence** peut afficher les états suivants : • **Appliqué** : si vous avez activé l'application à l'aide d'un code d'activation ou d'un fichier clé. • **Activation** : si vous avez appliqué un code d'activation pour activer l'application et que le processus est toujours en cours. L'état devient **Appliqué** à la fin de l'activation de l'application et le contenu du panneau de détails du nœud est mis à jour. • **Erreur d'activation** : apparaît en cas d'échec de l'activation de l'application. Vous pouvez voir la cause de l'échec de l'activation dans le journal d'exécution de la tâche.

Clé	La clé utilisée pour activer l'application.
Type de licence	Type de licence : commerciale ou d'essai.
Date d'expiration	Date et heure d'expiration de la licence associée à la clé active.
État du code d'activation ou de la clé	État du code d'activation ou état de la clé : *Actif* ou *additionnel*.

Pour voir les informations détaillées relatives à la licence, procédez comme suit :

Pour le nœud **Licence**, ouvrez le menu contextuel de la ligne des informations sur la licence que vous voulez examiner, puis choisissez l'option **Propriétés**.

Dans la fenêtre **Propriétés de la clé**, l'onglet **Général** reprend les détails relatifs à la licence active et l'onglet **Avancé** contient les informations relatives au client et les coordonnées de Kaspersky ou du partenaire chez qui vous avez acheté Kaspersky Embedded Systems Security (cf. tableau ci-dessous).

Informations de licence détaillées dans la fenêtre Propriétés :<État du code d'activation ou de la clé>

Champ	Description
Onglet Général	
Clé	La clé utilisée pour activer l'application.
Date d'ajout de la clé	Date d'ajout de la clé dans l'application.
Type de licence	Type de licence : commerciale ou d'essai.
Expire dans (jours)	Nombre de jours restants avant l'expiration de la licence associée à la clé active.
Date d'expiration	Date et heure d'expiration de la licence associée à la clé active. Si vous activez l'application selon un abonnement illimité, la valeur *Illimité* apparaît dans le champ. Si Kaspersky Embedded Systems Security ne parvient pas à déterminer la date d'expiration de la licence, la valeur *Inconnue* apparaît dans le champ.
Application	Le nom de l'application activée à l'aide du fichier clé ou du code d'activation.
Restrictions d'utilisation de la clé	Restrictions sur l'utilisation de la clé (le cas échéant).
Accès à l'assistance technique	Indique si la licence prévoit une assistance technique offerte par Kaspersky ou par ses partenaires.
Onglet Avancé	
Informations relatives à la licence	Clé de licence en cours.
Informations relatives au support	Coordonnées de Kaspersky ou du partenaire qui offre le Support Technique. Le champ peut être vide en l'absence de Support Technique.

Informations relatives au détenteur	Informations relatives au titulaire de la licence : nom du client ou de l'organisation pour laquelle une licence a été achetée.

Restriction des fonctions à l'expiration de la licence

Une fois que la licence active arrive à échéance, les restrictions suivantes sont appliquées aux composants fonctionnels :

- Toutes les tâches sont arrêtées, à l'exception des tâches Protection des fichiers en temps réel, Analyse à la demande et Vérification de l'intégrité de l'application.
- Aucune tâche ne peut être lancée, à l'exception de la Protection des fichiers en temps réel, de l'Analyse à la demande et de la Vérification de l'intégrité de l'application. Ces tâches sont toujours opérationnelles, mais font intervenir les anciennes bases antivirus.
- La fonction Protection contre les exploits est limitée :
  - Les processus sont protégés jusqu'à leur redémarrage.
  - Il est impossible d'ajouter de nouveaux processus à la zone de protection.

Les autres fonctions (référentiels, journaux, informations de diagnostic) sont toujours disponibles.

Renouvellement de la licence

Par défaut Kaspersky Embedded Systems Security signale l'échéance prochaine de la validité de la licence 14 jours avant sa date d'expiration. Dans ce cas, l'état **Date d'expiration de la licence** est mis en évidence en jaune dans le volet résultats du nœud **Kaspersky Embedded Systems Security**.

Vous pouvez renouveler la licence avant sa date d'expiration avec une clé additionnelle. Ainsi, la protection de l'appareil 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 une licence :

1. Obtenez un nouveau code d'activation de l'application ou un fichier clé.
2. Dans l'arborescence de la console de l'application, développez le nœud **Licence**.
3. Dans le volet résultats du nœud **Licence**, exécutez une des actions suivantes :
   - Si vous souhaitez renouveler la licence à l'aide d'un fichier clé :
     a. Cliquez sur le lien **Ajouter une clé**.
     b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**.
     c. Sélectionnez un nouveau fichier clé portant l'extension .key.
     d. Cochez la case **Utiliser en tant que clé additionnelle**.

- Si vous souhaitez renouveler la licence à l'aide d'un code d'activation :

  a. Cliquez sur le lien **Ajouter un code d'activation**.

  b. Dans la fenêtre qui s'ouvre, saisissez le code d'activation.

  c. Cochez la case **Utiliser en tant que clé additionnelle**.

L'application d'un code d'activation requiert une connexion à Internet.

4. Cliquez sur le bouton **OK**.

La clé additionnelle est ajoutée et appliquée automatiquement à l'expiration de la licence actuelle de Kaspersky Embedded Systems Security.

Suppression de la clé

Vous pouvez supprimer une clé que vous avez ajoutée.

Si Kaspersky Embedded Systems Security possède une clé additionnelle et que vous supprimez la clé active, la clé additionnelle devient automatiquement la clé active.

Si vous supprimez la clé qui avait été ajoutée, vous pourrez la restaurer après avoir appliqué à nouveau le fichier clé.

Pour supprimer la clé ajoutée, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Licence**.
2. Dans le tableau contenant les informations relatives aux clés ajoutées qui figure dans le volet résultats du nœud **Licence**, sélectionnez la clé que vous souhaitez supprimer.
3. Dans le menu contextuel de la ligne contenant les informations sur la clé sélectionnée, choisissez l'option **Supprimer**.
4. Dans la fenêtre de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

La clé sélectionnée sera supprimée.

Utilisation du plug-in d'administration

Cette section fournit des informations sur le plug-in Kaspersky Embedded Systems Security et décrit la procédure d'administration de l'application installée sur un périphérique protégé ou sur un groupe de périphériques protégés.

Gestion de Kaspersky Embedded Systems Security à partir de Kaspersky Security Center

Vous pouvez gérer de manière centralisée plusieurs périphériques protégés dotés de Kaspersky Embedded Systems Security et inclus dans un groupe d'administration au moyen du plug-in Kaspersky Embedded Systems Security. Kaspersky Security Center peut également configurer séparément chaque appareil protégé du groupe d'administration.

Un groupe d'administration est créé manuellement via Kaspersky Security Center. Le groupe contient plusieurs appareils dotés de Kaspersky Embedded Systems Security pour lesquels vous souhaitez configurer des paramètres de contrôle et de protection identiques. Pour en savoir plus sur l'utilisation de groupes d'administration, consultez *l'aide de Kaspersky Security Center*.

Les paramètres de l'application pour un seul périphérique protégé ne peuvent être configurés si le fonctionnement de Kaspersky Embedded Systems Security sur ce périphérique protégé est contrôlé par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Embedded Systems Security depuis Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center**. Les stratégies de Kaspersky Security Center permettent de définir à distance des paramètres de protection uniques pour un groupe d'appareils. Les paramètres de la tâche, définis dans la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la console de l'application ou à distance dans la fenêtre **Propriétés : <nom de l'appareil protégé>** de Kaspersky Security Center.

  Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches Protection en temps réel de l'ordinateur, Contrôle de l'activité locale et les paramètres du lancement des tâches locales planifiées du système.

- **A l'aide de tâches de groupe de Kaspersky Security Center**. Les tâches de groupe de Kaspersky Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai d'exécution limité pour un groupe d'appareils.

  Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche de Génération des règles du Contrôle du lancement des applications.

- **A l'aide de tâches pour une sélection de périphériques**. Les tâches pour une sélection de périphériques permettent de configurer à distance des paramètres de tâches communs ayant un délai d'exécution limité pour les appareil protégés qui ne figurent dans aucun groupe d'administration.

- **A l'aide de la fenêtre de configuration des paramètres d'un périphérique**. La fenêtre **Propriétés : <nom de l'appareil protégé>** permet de configurer à distance les paramètres d'une tâche pour un appareil protégé unique appartenant à un groupe d'administration. Vous pouvez également configurer ainsi les paramètres généraux de fonctionnement de l'application et les paramètres de toutes les tâches de Kaspersky Embedded Systems Security si le périphérique protégé sélectionné n'est pas contrôlé par une stratégie active de Kaspersky Security Center.

Kaspersky Security Center permet de configurer les paramètres de l'application ainsi que les possibilités additionnelles, sans oublier le fonctionnement des journaux et notifications. Vous pouvez configurer ces paramètres aussi bien pour un groupe de périphériques protégés que pour un seul périphérique protégé.

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Embedded Systems Security dans Kaspersky Security Center Web Console.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres généraux via la stratégie

Pour accéder aux paramètres de l'application de Kaspersky Embedded Systems Security via la stratégie :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <Nom de la stratégie>** qui s'ouvre, sélectionnez la section **Paramètres de l'application**.
6. Cliquez sur le bouton **Configuration** dans la sous-section du paramètres que vous souhaitez configurer.

Accès aux paramètres généraux dans la fenêtre des propriétés de l'application

Pour ouvrir la fenêtre des propriétés de Kaspersky Embedded Systems Security pour un seul périphérique protégé :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <Nom du périphérique>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.

- Sélectionnez l'option **Propriétés** dans le menu contextuel du périphérique protégé.

La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.

5. Dans la section **Applications**, sélectionnez **Kaspersky Embedded Systems Security 3.2**.
6. Cliquez sur le bouton **Propriétés**.
   La fenêtre **Kaspersky Embedded Systems Security 3.2** s'ouvre.
7. Sélectionnez la section **Paramètres de l'application**.

Configuration des paramètres généraux de l'application dans Kaspersky Security Center

Vous pouvez configurer les paramètres généraux de Kaspersky Embedded Systems Security depuis Kaspersky Security Center pour un groupe de périphériques protégés ou pour un périphérique protégé individuel.

Configuration de l'optimisation, de l'interface et de l'analyse dans Kaspersky Security Center

Pour configurer les paramètres d'évolutivité, d'interface et d'analyse :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Paramètres de l'application** de la sous-section **Extensibilité, interface et paramètres d'analyse**, cliquez sur **Configuration**.
5. Sous l'onglet **Général** de la fenêtre **Paramètres avancés de l'application**, configurez les paramètres suivants :
   - La section **Paramètres d'optimisation** permet de configurer les paramètres qui définissent le nombre de processus utilisés par Kaspersky Embedded Systems Security.
     - Détecter automatiquement les paramètres de montée en puissance

- Indiquer manuellement le nombre de processus actifs
  - Nombre de processus de protection en temps réel
  - Nombre de processus pour les tâches d'analyse à la demande en arrière-plan
- Dans la section **Interaction avec l'utilisateur**, configurez l'affichage de l'icône de la barre d'état de l'application dans la zone de notification : décochez ou cochez la case **Afficher l'icône de la barre d'état dans la barre des tâches**.

6. Sous l'onglet **Paramètres de l'analyse**, configurez les paramètres suivants :
   - Restaurer les attributs du fichier après l'analyse
   - Limiter l'utilisation du processeur pour les threads d'analyse
     - Limite supérieure (pour cent)
   - Dossier pour les fichiers temporaires créés pendant l'analyse
7. Sous l'onglet **Stockage hiérarchique**, sélectionnez l'option d'accès au stockage hiérarchique.
8. Cliquez sur le bouton **OK**.

Les paramètres d'application définis seront enregistrés.

Configuration des paramètres de sécurité dans Kaspersky Security Center

Pour configurer manuellement les paramètres de sécurité :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Configuration** de la sous-section **Sécurité et fiabilité**.
5. Configurez les paramètres suivants dans la fenêtre **Paramètres de sécurité** :
   - Dans la section **Paramètres de protection par mot de passe**, activez ou désactivez l'option **Protection des processus de l'application contre les menaces externes**.

- Dans la section **Paramètres de protection par mot de passe**, définissez le mot de passe de protection de l'accès aux fonctions de Kaspersky Embedded Systems Security.
- La section **Auto-défense** permet de configurer les paramètres de restauration des tâches de Kaspersky Embedded Systems Security en cas d'échec de l'application ou d'arrêt forcé de celle-ci.
  - **Réaliser la restauration des tâches**
  - **Paramètres de fiabilité**
- La section **Maximum de restaurations des tâches d'analyse à la demande** permet de limiter la charge de Kaspersky Embedded Systems Security sur le périphérique protégé dans le cadre de l'alimentation de secours :
  - **Ne pas lancer les tâches d'analyse programmée**
  - **Arrêter les tâches d'analyse en cours**
- Dans la section **Paramètres de protection par mot de passe**, définissez le mot de passe de protection de l'accès aux fonctions de Kaspersky Embedded Systems Security.

6. Cliquez sur le bouton **OK**.

Les paramètres définis de sécurité et de fiabilité sont enregistrés.

Configuration des paramètres de connexion dans Kaspersky Security Center

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Embedded Systems Security et les serveurs de mise à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services KSN.

Pour configurer les paramètres de la connexion, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Configuration** de la sous-section **Connexions**.

   La fenêtre **Paramètres de connexion** s'ouvre.

5. Configurez les paramètres suivants dans la fenêtre **Paramètres de connexion** :

   - Définissez les paramètres d'utilisation du serveur proxy dans la section **Paramètres du serveur proxy** :

     - Ne pas utiliser de serveur proxy.
     - Utiliser le serveur proxy indiqué.
     - Adresse IP ou nom symbolique du serveur proxy et numéro de port.
     - Ne pas utiliser le serveur proxy pour les adresses locales.

   - Définissez les paramètres d'authentification dans la section **Paramètres d'authentification du serveur proxy** :

     - Sélectionnez les paramètres d'authentification dans la liste déroulante.

       - **Ne pas utiliser l'authentification** : l'authentification n'est pas utilisée. Ce mode est sélectionné par défaut.
       - **Utiliser l'authentification NTLM** : authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft.
       - **Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe** : authentification à l'aide d'un nom d'utilisateur et d'un mot de passe selon le protocole d'authentification réseau NTLM, développé par Microsoft.
       - **Utiliser le nom d'utilisateur et le mot de passe** : authentification à l'aide du nom d'utilisateur et du mot de passe.

     - Si nécessaire, indiquez le nom d'utilisateur et le mot de passe.

   - Dans la section **Licence**, cochez ou décochez la case **Utiliser Kaspersky Security Center comme serveur proxy pour l'activation de l'application**.

6. Cliquez sur le bouton **OK**.

Les paramètres de la connexion définis seront enregistrés.

Configuration du lancement planifié des tâches locales du système prédéfinies

Les stratégies permettent d'autoriser ou d'interdire le lancement des tâches locales du système d'analyse à la demande et de mise à jour programmée localement sur chaque appareil protégé du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'appareil protégé selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.
- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Par défaut, la stratégie interdit le lancement des tâches locales du système.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont administrées via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de groupe de mise à jour ou d'analyse à la demande, autorisez le lancement des tâches locales du système dans la stratégie. Kaspersky Embedded Systems Security réalise la mise à jour des bases de données et des modules de l'application et lance également toutes les tâches locales du système d'analyse à la demande conformément à la programmation par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâche d'analyse à la demande définie : Analyse rapide, Analyse de la quarantaine, Analyse au démarrage du système d'exploitation et Vérification de l'intégrité de l'application, Surveillance de l'intégrité des fichiers.
- Tâches de mise à jour : Mise à jour des bases de l'application, Mise à jour des modules de l'application, Copie des mises à jour.

Si vous excluez l'appareil protégé du groupe d'administration, la planification des tâches locales du système sera automatiquement activée.

Pour autoriser ou interdire le lancement planifié des tâches locales du système de Kaspersky Embedded Systems Security dans une stratégie :

1. Dans l'arborescence de la Console d'administration, déployez le nœud **Périphériques administrés**, déployez ensuite le groupe requis, puis sélectionnez l'onglet **Stratégies** dans le panneau des résultats.
2. Sous l'onglet **Stratégies**, ouvrez le menu contextuel de la stratégie pour laquelle vous souhaitez configurer le lancement planifié des tâches locales du système de Kaspersky Embedded Systems Security sur le groupe d'appareils protégés et choisissez l'option **Propriétés**.
3. Dans la fenêtre **Propriétés : <nom de la stratégie>**, ouvrez la section **Paramètres de l'application**. Cliquez sur le bouton **Configuration** dans la section **Lancer les tâches locales du système** et réalisez une des opérations suivantes :
   - Cochez les cases **Tâches d'analyse à la demande** et **Tâches de mise à jour et de copie des mises à jour** pour autoriser le lancement planifié des tâches citées.
   - Décochez les cases **Tâches d'analyse à la demande** et **Tâches de mise à jour et de copie des mises à jour** pour interdire le lancement planifié des tâches citées.

   L'activation ou la désactivation des cases n'a aucun impact sur les paramètres de lancement des tâches locales définies par l'utilisateur du type indiqué.
4. Assurez-vous que la stratégie que vous configurez est active et appliquée au groupe d'appareils protégés sélectionné.
5. Cliquez sur le bouton **OK**.

Les paramètres de planification du lancement planifié sont appliqués aux tâches sélectionnées.

Configuration des paramètres de la quarantaine et de la sauvegarde dans Kaspersky Security Center

Pour configurer les paramètres de la Sauvegarde dans Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans la sous-section **Stockages**.
5. Sous l'onglet **Sauvegarde** de la fenêtre de paramètres **Paramètres des stockages**, configurez les paramètres de la Sauvegarde suivants :
   - Si vous souhaitez définir le dossier de sauvegarde, sélectionnez, dans le champ **Dossier de sauvegarde**, le dossier requis sur le disque local de l'appareil protégé ou saisissez le chemin d'accès complet à celui-ci.
   - Si vous souhaitez définir la taille maximale de la Sauvegarde, cochez la case **Taille maximale de sauvegarde (Mo)** et saisissez la valeur souhaitée en mégaoctets dans le champ.
   - Pour définir le seuil d'espace libre de Sauvegarde :
     - Définissez la valeur du paramètre **Taille maximale de sauvegarde (Mo)**.
     - Cochez la case **Seuil d'espace disponible (Mo)**.
     - Spécifiez la valeur minimale de l'espace libre dans le dossier de Sauvegarde (en Mo).
   - Pour désigner le dossier des objets restaurés, effectuez l'une des opérations suivantes :
     - Sélectionnez le dossier approprié sur un lecteur local de l'appareil protégé dans la section **Paramètres de restauration**.
     - Saisissez le nom du dossier et son chemin d'accès complet dans le champ **Dossier cible pour la restauration des objets**.
6. Dans la fenêtre **Paramètres des stockages**, choisissez l'onglet **Quarantaine** et configurez les paramètres de la quarantaine :

- Si vous souhaitez modifier le dossier de la quarantaine, indiquez le chemin d'accès au dossier sur le disque local de l'appareil protégé dans le champ **Dossier de quarantaine**.

- Si vous souhaitez définir la taille maximale de la **quarantaine**, cochez la case Taille maximale de la quarantaine (Mo) et saisissez la valeur en Mo dans le champ.

- Si vous souhaitez définir la valeur minimale d'espace disponible dans la quarantaine, cochez les cases **Taille maximale de la quarantaine (Mo)** et **Seuil d'espace disponible (Mo)**, puis saisissez la valeur seuil du paramètre en Mo dans le champ de saisie.

- Si vous souhaitez modifier le dossier dans lequel les fichiers de la quarantaine sont restaurés, saisissez le chemin d'accès complet au dossier sur le disque local de l'appareil protégé dans le champ **Dossier cible pour la restauration des objets**.

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

Les paramètres configurés de la Quarantaine et de la Sauvegarde seront enregistrés.

Création et configuration des stratégies

Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Embedded Systems Security sur plusieurs périphériques protégés.

Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs périphériques sur lesquels Kaspersky Embedded Systems Security est installé.

Une stratégie applique les paramètres de Kaspersky Embedded Systems Security, de ses fonctions et de ses tâches à l'ensemble des périphériques protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la Console d'administration, la stratégie active dans le groupe en ce moment possède l'état *actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Embedded Systems Security. Vous pouvez les consulter dans la console de l'application dans le nœud **Journal d'audit système**.

Kaspersky Security Center offre une méthode pour appliquer les stratégies aux appareils protégés : *interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Embedded Systems Security applique aux périphériques protégés les valeurs des paramètres pour lesquels vous avez sélectionné l'icône dans les propriétés de la stratégie. Dans ce cas, Kaspersky Embedded Systems Security n'utilise pas les valeurs des paramètres en vigueur avant l'application de la stratégie. Les paramètres de la stratégie active accompagnés de l'icône dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Embedded Systems Security.

Si une stratégie est active, les paramètres dans la Console de l'application qui sont accompagnés de l'icône dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres (accompagnés de l'icône dans la stratégie) peuvent être modifiées dans la console de l'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône empêchent également la modification des paramètres dans Kaspersky Security Center pour un appareil protégé depuis la fenêtre **Propriétés : <Nom de l'appareil protégé>**.

Les paramètres configurés et transmis à l'appareil protégé à l'aide de la stratégie active sont enregistrés dans les paramètres de tâche locale après la désactivation de la stratégie active.

Si la stratégie définit les paramètres d'une tâche de protection en temps réel de l'ordinateur et si cette tâche est en exécution, les paramètres définis par la stratégie sont modifiés directement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

Création d'une stratégie

La création d'une stratégie comporte les étapes suivantes :

1. Création d'une stratégie à l'aide de l'Assistant de création de stratégies. Vous pouvez définir les paramètres des tâches Protection en temps réel de l'ordinateur dans les boîtes de dialogue de l'assistant.

2. Configuration des paramètres de la stratégie. La fenêtre **Propriétés : <Nom de la stratégie>** de la stratégie créée permet de configurer les paramètres des tâches de protection en temps réel de l'ordinateur, les paramètres généraux de Kaspersky Embedded Systems Security, les paramètres de la quarantaine et les paramètres de la Sauvegarde, le niveau de détail des journaux d'exécution de la tâche ainsi que les notifications des utilisateurs et de l'administrateur sur les événements de Kaspersky Embedded Systems Security.

Pour créer une stratégie pour un groupe de périphériques protégés sur lesquels Kaspersky Embedded Systems Security est installé, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe d'administration contenant les appareils protégés pour lesquels vous souhaitez créer une stratégie.

2. Dans le panneau de détails du groupe d'administration sélectionné, choisissez l'onglet **Stratégies** et cliquez sur le lien **Créer une stratégie** pour démarrer l'assistant et créer une stratégie.

   La fenêtre **Assistant de création de stratégie** s'ouvre.

3. Dans la fenêtre **Sélection de l'application pour la création d'une stratégie de groupe**, choisissez Kaspersky Embedded Systems Security, puis cliquez sur **Suivant**.

4. Entrez un nom de stratégie de groupe dans le champ **Nom**.

   Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ |` .

5. Pour appliquer une configuration de stratégie employée dans une version antérieure de l'application :

   a. Cochez la case **Utiliser les paramètres de la stratégie pour les versions précédentes de l'application**.

   b. Cliquez sur le bouton **Sélectionner**.

   c. Sélectionnez la stratégie que vous souhaitez appliquer.

   d. Cliquez sur **Suivant**.

6. Sélectionnez une des options suivantes dans la fenêtre **Sélection du type d'opération** :

   - **Créer**, pour créer une nouvelle stratégie avec les paramètres par défaut.

   - **Importer une stratégie créée à l'aide de versions antérieures de Kaspersky Embedded Systems Security** pour utiliser la stratégie importée en tant que modèle.

- Cliquez sur le bouton **Parcourir** et sélectionnez un fichier de configuration contenant une stratégie existante.

7. Dans la fenêtre **Protection en temps réel de l'ordinateur**, configurez les tâches Protection des fichiers en temps réel, Utilisation du KSN, Protection contre les exploits et le Monitoring des scripts en fonction de vos besoins. Autorisez ou interdisez l'application des tâches configurées de la stratégie sur les appareils protégés du réseau :

   - Cliquez sur le bouton pour débloquer la configuration des paramètres d'une tâche sur les appareils protégés du réseau et interdire l'application des paramètres de la tâche configurés dans la stratégie.

   - Cliquez sur le bouton pour interdire la configuration des paramètres d'une tâche sur les appareils protégés du réseau et autoriser l'application des paramètres de la tâche configurés dans la stratégie.

   Dans une stratégie recréée, les paramètres des tâches de protection en temps réel de l'ordinateur sont définis par défaut.

   - Si vous souhaitez modifier les paramètres d'une tâche Protection des fichiers en temps réel définis par défaut, cliquez sur le bouton **Configuration** dans la sous-section **Protection des fichiers en temps réel**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos exigences. Cliquez sur le bouton **OK**.

   - Si vous souhaitez modifier les paramètres par défaut d'une tâche Utilisation du KSN, cliquez sur le bouton **Configuration** dans la sous-section **Utilisation du KSN**. Dans la fenêtre qui s'ouvre, configurez la tâche en fonction de vos exigences. Cliquez sur le bouton **OK**.

     Pour démarrer la tâche d'Utilisation du KSN, vous devez accepter la Déclaration KSN dans la fenêtre Traitement des données KSN.

   - Pour modifier les paramètres par défaut du composant Protection contre les exploits, cliquez sur le bouton **Configuration** dans la sous-section **Protection contre les exploits**. Dans la fenêtre qui s'ouvre, configurez la fonctionnalité en fonction de vos exigences. Cliquez sur le bouton **OK**.

8. Sélectionnez un des états suivants de la stratégie suivants dans la fenêtre **Créer la stratégie de groupe pour l'application** :

   - **Stratégie active** si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, celle-ci est désactivée et une nouvelle stratégie est appliquée.

   - **Stratégie inactive**, si vous ne voulez pas appliquer immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.

   - Cochez la case **Ouvrir les propriétés de la stratégie uniquement après leur création** pour fermer automatiquement l'**assistant de création de stratégie** et configurez la stratégie récemment créée après avoir cliqué sur le bouton **Suivant**.

9. Cliquez sur le bouton **Terminer**.

La stratégie créée sera affichée dans la liste des stratégies sous l'onglet **Stratégies** du groupe d'administration sélectionné. La fenêtre **Propriétés : <nom de la stratégie>** permet de configurer d'autres paramètres, tâches et fonctions de Kaspersky Embedded Systems Security.

Une fois que vous avez créé une stratégie, un ensemble de règles d'autorisation est créé pour empêcher le blocage des applications et garantir leur fonctionnement continu. Les règles par défaut figurent dans les paramètres de la tâche. Voici les détails et les limites.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau entrant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le processus Partage du bureau Windows de l'Agent d'administration de Kaspersky Security Center, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Deux règles d'autorisation pour le port local 15000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau sortant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour Kaspersky Embedded Systems Security Service, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Deux règles d'autorisation pour le processus de flux de travail de Kaspersky Embedded Systems Security, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Deux règles d'autorisation pour le port local 13000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Sections contenant les paramètres de stratégie de Kaspersky Embedded Systems Security

Général

La section **Général** permet de configurer les paramètres de stratégie suivants :

- Indiquez l'état de la stratégie.
- Configurez l'héritage des paramètres des stratégies parent pour les stratégies fille.

Notification sur les événements

La section **Notification sur les événements** permet de configurer les paramètres pour les catégories d'événements suivants :

- *Événements critiques*
- *Panne de fonction*
- *Avertissement*
- *Message d'information*

Le bouton **Propriétés** permet de configurer les paramètres suivants pour les événements sélectionnés :

- Définissez l'emplacement et la durée de conservation des informations sur l'événement enregistré ;
- Indiquez la méthode de notification pour les événements consignés.

Paramètres de l'application

Paramètres de la section Paramètres de l'application

Section	Options
Extensibilité, interface et paramètres d'analyse	Le bouton **Configuration** de la sous-section **Extensibilité, interface et paramètres d'analyse** permet de configurer les paramètres suivants : • choisir la configuration automatique ou manuelle des paramètres de montée en puissance. • configurer l'affichage de l'icône de l'application.
Sécurité et fiabilité	Le bouton **Configuration** de la sous-section **Sécurité et fiabilité** permet de configurer les paramètres suivants : • Configurez les paramètres de lancement de la tâche. • Actions de l'application en cas de passage à l'alimentation de l'appareil protégé via un onduleur. • Activation ou désactivation de la protection par mot de passe des fonctions de l'application.
Connexions	Le bouton **Configuration** de la sous-section **Connexions** permet de configurer les paramètres suivants du serveur proxy pour la connexion aux serveurs de mise à jour, aux serveurs d'activation et à KSN : • définition des paramètres du serveur proxy. • définition des paramètres d'authentification sur le serveur proxy.
Lancer les tâches locales du système	Le bouton **Configuration** de la sous-section **Lancer les tâches locales du système** permet d'interdire ou d'autoriser le lancement des tâches système planifiées suivantes, configurées sur les appareils protégés : • Tâche Analyse à la demande. • Tâches de mise à jour et tâche de copie des mises à jour.

Complémentaire

Paramètres de la section Complémentaire

Section	Options
Zone de confiance	Le bouton **Configuration** de la sous-section **Zone de confiance** permet de configurer les paramètres suivants d'application d'une zone de confiance : • Composer la liste des exclusions de la zone de confiance.

	• Activer ou désactiver l'analyse des opérations de sauvegarde des fichiers. • Composer une liste des processus de confiance.
Analyse des disques amovibles	La section **Analyse des disques amovibles** contient le bouton **Configuration** qui permet de configurer les paramètres d'analyse des disques amovibles.
Autorisations d'accès de l'utilisateur pour l'administration de l'application	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** permet de configurer les paramètres des droits des utilisateurs et des groupes d'utilisateurs à l'administration de Kaspersky Embedded Systems Security.
Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** permet de configurer les droits des utilisateurs et des groupes d'utilisateurs à l'administration du service Kaspersky Security.
Stockages	Dans la sous-section **Stockages**, cliquez sur le bouton **Configuration** pour configurer les paramètres suivants de la quarantaine, de la Sauvegarde et de la liste des ordinateurs douteux : • chemin d'accès du dossier dans lequel vous souhaitez placer les objets en quarantaine ou dans la sauvegarde ; • taille maximale de la Sauvegarde ou de la quarantaine et seuil d'espace disponible ; • dossier où seront placés les objets restaurés depuis la sauvegarde ou la quarantaine ; • Configurez la durée de blocage des hôtes.

Protection en temps réel de l'ordinateur

Paramètres de la section Protection en temps réel de l'ordinateur

Section	Options
Protection des fichiers en temps réel	Le bouton **Configuration** de la sous-section **Protection des fichiers en temps réel** permet de configurer les paramètres suivants d'exécution de la tâche : • Indiquez le mode de protection. • Configurez l'utilisation de l'analyse heuristique. • Configurez l'application de la Zone de confiance. • composition de la zone de protection ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de sécurité ; • Configurez les paramètres de lancement de la tâche.
Utilisation du	Le bouton **Configuration** de la sous-section **Utilisation du KSN** permet de configurer

KSN	les paramètres suivants d'exécution de la tâche : • actions à réaliser sur les objets considérés comme douteux par KSN ; • Configurez le transfert de données et l'utilisation de Kaspersky Security Center en tant que serveur proxy du KSN. Cliquez sur le bouton **Traitement des données en cours** pour accepter ou refuser la Déclaration de KSN, puis configurez les paramètres d'échange de données fiables.
Protection contre les exploits	Le bouton **Configuration** de la sous-section **Protection contre les exploits** permet de configurer les paramètres suivants d'exécution de la tâche : • sélection du mode de protection de la mémoire du processus ; • définition de l'action de réduction de l'impact de l'exploitation des vulnérabilités ; • enrichissement et modification de la liste des processus à protéger.

Contrôle de l'activité locale

Paramètres de la section Contrôle de l'activité locale

Section	Options
Contrôle du lancement des applications	Le bouton **Configuration** de la sous-section **Contrôle du lancement des applications** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • configuration des paramètres du contrôle du nouveau lancement des applications ; • Indiquez la zone d'application des règles du contrôle du lancement des applications. • configuration de l'utilisation du KSN ; • Configurez les paramètres de lancement de la tâche.
Contrôle des périphériques	Le bouton **Configuration** de la sous-section **Contrôle des périphériques** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • Configurez les paramètres de lancement de la tâche.

Contrôle de l'activité réseau

Paramètres de la section Contrôle de l'activité réseau

Section	Options
Gestion du pare-feu	Le bouton **Configuration** de la sous-section **Gestion du pare-feu** permet de configurer les paramètres suivants d'exécution de la tâche : • règles du pare-feu ;

	• Configurez les paramètres de lancement de la tâche.

Diagnostic du système

Paramètres de la section Diagnostic du système

Section	Options
Moniteur d'intégrité des fichiers	La sous-section **Moniteur d'intégrité des fichiers** permet de configurer le contrôle sur les modifications dans les fichiers qui peuvent indiquer un cas d'atteinte à la sécurité sur un périphérique protégé.
Inspection des journaux	La section **Inspection des journaux** permet de configurer le contrôle de l'intégrité d'un périphérique protégé sur la base des résultats de l'analyse du journal des événements Windows.

Journaux et notifications

Paramètres de la section Journaux et notifications

Section	Options
Journaux d'exécution de la tâche	Le bouton **Configuration** de la sous-section **Journaux d'exécution de la tâche** permet de configurer les paramètres suivants : • Définition du niveau d'importance des événements enregistrés pour les composants de l'application sélectionnés ; • Définition des paramètres de conservation des journaux d'exécution de la tâche. • Spécifiez l'intégration de SIEM avec les paramètres de Kaspersky Security Center.
Notifications sur les événements	Le bouton **Configuration** de la sous-section **Notifications sur les événements** permet de configurer les paramètres suivants : • Définissez les paramètres de notification des utilisateurs pour l'événement Objet détecté ; pour les événements *Objet détecté*, *Périphérique externe douteux détecté et restreint* et *Session réseau ajoutée à la liste des sessions douteuses*. • paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements de la section **Configuration des notifications**.
Interaction avec le serveur d'administration	Le bouton **Configuration** de la section **Interaction avec le serveur d'administration** permet de choisir les types d'objets -y compris les objets de la quarantaine et de la sauvegarde) que Kaspersky Embedded Systems Security va signaler au Serveur d'administration.

Diagnostic des échecs

Paramètres de la section Diagnostic des échecs.

Section	Options
Paramètres de	La section **Paramètres de dépannage** permet de configurer les paramètres suivants :

dépannage	• Sélectionnez l'option **Activer le traçage**. • Définissez le paramètre **Dossier pour les fichiers de traçage**. • Spécifiez le **Niveau de détails**. • Définissez la **Taille maximale du fichier de traçage**. • Sélectionnez l'option **Supprimer les fichiers de traçage les plus anciens**. • Spécifiez le **Nombre maximal de fichiers pour un journal de traçage**. Les paramètres de stratégie de groupe et les paramètres locaux introduisent des paramètres correspondants. Pour en savoir plus sur les options et leurs limites, consultez la configuration des paramètres locaux. Vous pouvez définir différentes valeurs pour les paramètres sur l'appareil local et dans la stratégie de groupe pour plusieurs appareils, avec les conditions suivantes. • Les paramètres de la stratégie de groupe configurés sur le serveur Kaspersky Security Center ont la priorité sur les paramètres locaux. • La priorité des paramètres de stratégie de groupe configurés sur l'appareil local est inférieure à celle des paramètres locaux.
Paramètres du fichier dump	La sous-section **Paramètres du fichier dump** permet de configurer les options suivantes, le cas échéant : • Sélectionnez l'option **Créer le fichier dump**. • Définissez le **Dossier du fichier dump**. Les paramètres de stratégie de groupe et les paramètres locaux introduisent des paramètres correspondants. Pour en savoir plus sur les options et leurs limites, consultez la configuration des paramètres locaux. Vous pouvez définir différentes valeurs pour les paramètres sur l'appareil local et dans la stratégie de groupe pour plusieurs appareils, avec les conditions suivantes. • Les paramètres de la stratégie de groupe configurés sur le serveur Kaspersky Security Center ont la priorité sur les paramètres locaux. • La priorité des paramètres de stratégie de groupe configurés sur l'appareil local est inférieure à celle des paramètres locaux.

Historique des révisions

La section **Historique des révisions** permet d'administrer les révisions : comparer à la révision actuelle ou à une autre stratégie, ajouter des descriptions de révisions, enregistrer les révisions dans un fichier ou revenir à l'état antérieur à la révision.

Configuration d'une stratégie

La fenêtre **Propriétés:<nom de la stratégie>** d'une stratégie existante permet de configurer les éléments suivants :

- Paramètres généraux de Kaspersky Embedded Systems Security.

- Paramètres de la Quarantaine et de la Sauvegarde.
- Paramètres de la zone de confiance, de la protection en temps réel de l'ordinateur et du contrôle de l'activité locale.
- Niveau de détail des journaux d'exécution des tâches.
- Notifications destinées à l'utilisateur et à l'administrateur relatives aux événements de Kaspersky Embedded Systems Security.
- Droits d'accès à l'administration de l'application et du service Kaspersky Security.

Pour configurer les paramètres d'une stratégie, procédez comme suit :

1. Développez le nœud **Périphériques administrés** dans l'arborescence de la Console d'administration de Kaspersky Security Center.
2. Développez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de la stratégie associée et ouvrez l'onglet **Stratégies** dans le panneau de détails.
3. Sélectionnez la stratégie que vous souhaitez configurer et ouvrez la fenêtre **Propriétés :<nom de la stratégie>** d'une des méthodes suivantes :
   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.
   - Dans le panneau de droite des détails de la stratégie sélectionnée, cliquez sur le lien **Configurer la stratégie**.
   - Double-cliquez sur la stratégie sélectionnée.
4. Activez ou désactivez l'application de la stratégie dans la section **État de la stratégie** de l'onglet **Général**. Pour ce faire, sélectionnez l'une des options suivantes :
   - **Stratégie active** si vous souhaitez que la stratégie s'applique à tous les appareils protégés appartenant au groupe d'administration sélectionné.
   - **Stratégie inactive** si vous souhaitez activer la stratégie plus tard sur tous les appareils protégés appartenant au groupe d'administration sélectionné.

   Le paramètre **Stratégie hors du bureau** n'est pas disponible dans le cadre de la gestion de Kaspersky Embedded Systems Security.
5. Dans les sections **Configuration d'événement**, **Paramètres de l'application**, **Complémentaire**, **Journaux et notifications** et **Historique des révisions**, vous pouvez modifier la configuration de l'application (cf. tableau ci-dessous).
6. Dans les sections **Protection en temps réel de l'ordinateur**, **Contrôle de l'activité locale**, **Contrôle de l'activité réseau** et **Diagnostic du système**, configurez les paramètres de l'application et de leur lancement (cf. tableau ci-dessous).

   Vous pouvez activer ou désactiver l'exécution de n'importe quelle tâche sur tous les appareils protégés appartenant au groupe d'administration à l'aide d'une stratégie de Kaspersky Security Center.

Vous pouvez configurer l'application des paramètres définis dans la stratégie sur tous les appareils protégés du réseau pour chaque composant distinct de l'application.

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

Les paramètres définis seront appliqués dans la stratégie.

Création et configuration de tâches via Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Embedded Systems Security, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

A propos de la création de tâches dans Kaspersky Security Center

Vous pouvez créer des tâches de groupe pour des groupes d'administration et pour des sélections d'appareils protégés. Vous pouvez créer les types de tâches suivants via Kaspersky Security Center :

- Activation de l'application
- Copie des mises à jour
- Mise à jour des bases de l'application
- Mise à jour des modules de l'application
- Annulation de la mise à jour des bases de l'application
- Analyse à la demande
- Vérification de l'intégrité de l'application
- Surveillance de l'intégrité des fichiers
- Génération des règles du Contrôle du lancement des applications
- Générateur de règles pour le Contrôle des périphériques

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- Pour un appareil protégé : dans la fenêtre **Propriétés <nom de l'appareil protégé>** dans la section **Tâches**.
- Pour un groupe d'administration : dans le volet résultats du nœud du groupe d'appareils protégés sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'appareils protégés : dans le volet résultats du nœud **Sélection de périphériques**.

Les stratégies permettent de désactiver les planifications pour la mise à jour et les tâches système locale d'analyse à la demande sur tous les appareils protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

Création d'une tâche dans Kaspersky Security Center

Pour créer une tâche dans la console d'administration de Kaspersky Security Center, procédez comme suit :

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :

   - Pour créer une tâche locale :

     a. Dans l'arborescence de la Console d'administration, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe auquel appartient l'appareil protégé.

     b. Dans le volet résultats, sous l'onglet **Périphériques**, ouvrez le menu contextuel de l'appareil protégé et sélectionnez **Propriétés**.

     c. Dans la section **Tâches** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

   - Pour créer une tâche de groupe :

     a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

     b. Sélectionnez le groupe d'administration pour lequel vous souhaitez créer une tâche.

     c. Dans le volet résultats, ouvrez l'onglet **Tâches** et choisissez l'option **Créer une tâche**.

   - Pour créer une tâche pour un ensemble d'appareils protégés défini par l'utilisateur :

     a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

     b. Sélectionnez le groupe d'administration contenant les appareils protégés.

     c. Sélectionnez un appareil protégé ou un ensemble personnalisé d'appareils protégés.

     d. Dans la liste déroulante **Exécuter une action**, sélectionnez l'option **Créer une tâche**.

   La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la fenêtre **Sélectionnez le type de tâche**, sous le titre **Kaspersky Embedded Systems Security 3.2**, sélectionnez le type de la tâche à créer.

3. Si vous avez choisi n'importe quel type de tâche, sauf Annulation de la mise à jour des bases de l'application, Vérification de l'intégrité de l'application ou Activation de l'application, la fenêtre **Configuration** s'ouvre. Les paramètres peuvent varier en fonction du type de tâche :

   - Création d'une tâche d'analyse à la demande.

   - Si vous créez une des tâches de mise à jour, définissez les paramètres de la tâche conformément à vos exigences :

     a. Sélectionnez la source de mise à jour dans la fenêtre **Source des mises à jour**.

b. Cliquez sur le bouton **Paramètres de connexion**. Dans la fenêtre **Paramètres de connexion**, configurez les paramètres d'accès au serveur proxy lors de la connexion à la source de mise à jour.

- Pour créer une tâche Mise à jour des modules de l'application, configurez les paramètres requis de la mise à jour des modules de l'application dans la fenêtre **Paramètres de mise à jour des modules de l'application** :

  a. Décidez si vous souhaitez copier et installer les mises à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles sans installation.

  b. Si vous avez choisi **Copier et installer les mises à jour critiques des modules de l'application**, le redémarrage de l'appareil protégé peut être requis pour terminer l'installation des modules de l'application. Pour que Kaspersky Embedded Systems Security relance automatiquement le périphérique protégé après la fin de la tâche, cochez la case **Autoriser le redémarrage du système d'exploitation**.

  c. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour des modules de Kaspersky Embedded Systems Security, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

  Kaspersky ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky. Il est possible de configurer une notification pour l'administrateur au sujet de l'événement **Nouvelle mise à jour prévue des modules de l'application disponible**. Cette notification reprend l'adresse Internet de notre site depuis lequel il est possible de télécharger les mises à jour planifiées.

- Pour créer la tâche Copie des mises à jour, indiquez, dans la fenêtre **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.

- Pour créer la tâche d'Activation de l'application, procédez comme suit :

  a. Dans la fenêtre **Paramètres d'activation**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application.

  b. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez créer une tâche pour renouveler la licence.

- Créez la tâche Génération des règles du Contrôle du lancement des applications.

- Créez la tâche Générateur de règles pour le Contrôle des périphériques.

4. Programmez l'exécution de la tâche.

   Vous pouvez configurer la planification des tâches de tous les types à l'exception de la tâche Annulation de la mise à jour des bases de l'application.

5. Cliquez sur le bouton **OK**.

6. Si la tâche est créée pour une sélection d'appareils protégés, sélectionnez le réseau (ou le groupe) d'appareils protégés sur lesquels elle sera exécutée.

7. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser pour exécuter la tâche.

8. Dans la fenêtre **Définition du nom de la tâche**, saisissez le nom de la tâche (100 caractères maximum) qui ne peut pas contenir les caractères " * < > ? \ | :.

   Nous vous conseillons d'ajouter le type de tâche à son nom (par exemple, « Analyse à la demande des dossiers partagés »).

9. La fenêtre **Terminer la création de la tâche** s'ouvre :

a. Cochez la case **Exécuter la tâche après la fin de l'assistant** si vous souhaitez que la tâche démarre dès sa création.

b. Cliquez sur **Terminer**.

La tâche créée apparaît dans la liste **Tâches**.

Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center

Pour configurer les tâches locales ou les paramètres généraux de l'application pour un appareil protégé unique du réseau :

1. Dans l'arborescence du Serveur d'administration de Kaspersky Security Center, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe auquel appartient l'appareil protégé.
2. Dans le volet résultats, choisissez l'onglet **Périphériques**.
3. Ouvrez la fenêtre **Propriétés : <Nom du périphérique>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - Ouvrez le menu contextuel du nom de l'appareil protégé et sélectionnez l'option **Propriétés**.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
4. Pour configurer les paramètres de la tâche locale, procédez comme suit :
   a. Passez à la section **Tâches**.
   b. Dans la liste des tâches, sélectionnez la tâche locale dont vous souhaitez configurer les paramètres :
      - Double-cliquez sur le nom de la tâche dans la liste des tâches.
      - Sélectionnez le nom de la tâche et cliquez sur le bouton **Propriétés**.
      - Puis, choisissez l'option **Propriétés** dans le menu contextuel de la tâche choisie.

        La fenêtre **Propriétés : <Nom de la tâche>** s'ouvre.
5. Pour configurer les paramètres de l'application, procédez comme suit :
   a. Passez à la section **Applications**.
   b. Dans la liste des applications installées, sélectionnez une application à configurer :
      - Double-cliquez sur le nom de l'application dans la liste des applications installées.
      - Sélectionnez le nom de l'application dans la liste, puis cliquez sur le bouton **Propriétés**.
      - Ouvrez le menu contextuel du nom de l'application dans la liste des applications installées, puis choisissez l'option **Propriétés**.

        La fenêtre **Paramètres <nom de l'application>** s'ouvre.

Si l'application est soumise à une stratégie de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, vous ne pourrez pas modifier ces paramètres via la fenêtre **Paramètres <nom de l'application>**.

Configuration des tâches de groupe dans Kaspersky Security Center

Lors de la gestion de Kaspersky Embedded Systems Security à partir de Kaspersky Security Center Cloud Console, vous ne pouvez pas ajouter manuellement des serveurs HTTP et FTP personnalisés ou des dossiers réseau.

Pour configurer une tâche de groupe pour plusieurs appareils protégés, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

   Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Pour en savoir plus sur la configuration des paramètres dans cette section, consultez le *Système d'aide de Kaspersky Security Center*.
5. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
   - Si vous configurez une tâche d'analyse à la demande :
     - Dans la section **Zone d'analyse**, créez une zone d'analyse.
     - Dans la section **Options**, configurez l'intégration aux autres modules de l'application et le niveau de priorité de la tâche.
   - Si vous configurez l'une des tâches de mise à jour, définissez les paramètres de la tâche en fonction de vos besoins :
     - Dans la section **Configuration**, configurez les paramètres de la source des mises à jour et l'optimisation du sous-système disque.

- Cliquez sur le bouton **Paramètres de connexion** pour configurer les paramètres de connexion de la source des mises à jour.

- Pour configurer les paramètres de la tâche Mise à jour des modules de l'application, procédez comme suit :

  - Accédez à la section **Paramètres de mise à jour des modules de l'application**.

  - Choisissez une action à effectuer : copiez et installez les mises à jour critiques des modules de l'application ou uniquement vérifier leur présence.

- Pour configurer la tâche Copie des mises à jour, indiquez, dans la section **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.

- Pour configurer la tâche d'Activation de l'application :

  - Dans la section **Paramètres d'activation**, appliquez le fichier clé à l'aide duquel vous souhaitez activer l'application.

  - Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter un code d'activation ou un fichier clé pour renouveler la licence.

- Pour configurer la génération automatique des règles d'autorisation pour le Contrôle des périphériques, définissez dans la section **Configuration** les valeurs qui seront utilisées pour créer la liste des règles d'autorisation.

6. Configurez la planification des tâches dans la section **Planification**. Vous pouvez planifier les tâches de tous les types à l'exception de la tâche Annulation de la mise à jour des bases de l'application.

7. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le *Système d'aide de Kaspersky Security Center*.

9. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Les paramètres de tâche de groupe qui peuvent être configurés sont repris dans le tableau ci-dessous.

Paramètre de tâches de groupe de Kaspersky Embedded Systems Security

Types de tâche de Kaspersky Embedded Systems Security	Section dans la fenêtre Propriétés : <nom de la tâche>	Paramètres de la tâche
Génération des règles du Contrôle du lancement des applications	**Configuration**	Lors de la configuration des paramètres de la tâche Génération des règles du Contrôle du lancement des applications, vous pouvez choisir comment créer les règles d'autorisation : • **Créer des règles d'autorisation sur la base des applications en cours d'exécution** • **Créer des règles d'autorisation pour les applications des dossiers**

	Options	Vous pouvez indiquer les actions lors de la création des règles d'autorisation du contrôle du lancement des applications : • **Utiliser un certificat numérique** • **Utiliser l'objet et l'empreinte du certificat numérique** • **En cas d'absence de certificat, utiliser** • **Utiliser le hash SHA256** • **Créer des règles pour un utilisateur ou un groupe d'utilisateurs** Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes de règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.
	Planification	Vous pouvez configurer les paramètres pour planifier une tâche.
Générateur de règles pour le Contrôle des périphériques	**Configuration**	• Sélectionnez le mode de fonctionnement : tenir compte des données système sur tous les appareils externes jamais connectés ou tenir compte uniquement des appareils externes connectés actuellement. • Configurez les paramètres pour les fichiers de configuration contenant les listes de règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Activation de l'application	**Paramètres d'activation**	Vous pouvez ajouter un fichier clé pour l'activation de l'application ou le renouvellement la licence.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Copie des mises à jour	**Source des mises à jour**	Vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.
	Fenêtre **Paramètres de connexion**	Dans la fenêtre **Paramètres de connexion** accessible depuis la section **Source des mises à jour**, indiquez s'il convient d'utiliser un serveur proxy pour établir la connexion avec les serveurs de mise à jour de Kaspersky ou tout autre serveur.
	Paramètres de copie des mises à jour	Vous pouvez indiquer le contenu des mises à jour à copier. Dans le champ **Dossier de conservation locale des mises à jour copiées**, indiquez le chemin d'accès au dossier dans lequel Kaspersky Embedded Systems Security va conserver les mises à jour copiées.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Mise à jour des bases de l'application	**Configuration**	Dans la zone de groupe **Source des mises à jour**, vous pouvez indiquer le serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement. La section Optimisation de l'utilisation du sous-système de disque vous permet de configurer les paramètres de la fonction de réduction de la charge sur le sous-système disque : • **Réduire la charge sur les I/O du disque** • **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**
	Fenêtre **Paramètres de connexion**	Dans la fenêtre **Paramètres de connexion** accessible depuis la section **Source des mises à jour**, indiquez s'il convient d'utiliser un serveur proxy pour établir la connexion avec les serveurs de mise à jour de Kaspersky ou tout autre serveur.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Mise à jour des modules de l'application	**Source des mises à jour**	Vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour. Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.
	Fenêtre **Paramètres de connexion**	Dans le groupe **Paramètres de connexion à la source des mises à jour**, indiquez s'il convient d'utiliser un serveur proxy pour établir la connexion avec les serveurs de mise à jour de Kaspersky ou tout autre serveur.
	Paramètres de mise à jour des modules de l'application	Vous pouvez indiquer les actions que Kaspersky Embedded Systems Security devrait réaliser quand des mises à jour critiques des modules de l'application sont disponibles ou ont déjà été installées et si Kaspersky Embedded Systems Security doit obtenir des informations sur les mises à jour planifiées.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Paramètres d'analyse à la demande	**Zone d'analyse**	Vous pouvez définir une zone d'analyse pour la tâche d'analyse à la demande et accéder à la configuration du niveau de sécurité.
	Fenêtre **Paramètres de l'analyse à la demande**	Dans la fenêtre **Paramètres de l'analyse à la demande** ouverte via le lien de la section **Zone d'analyse**, sélectionnez un des niveaux de sécurité prédéfinis ou personnalisez manuellement les paramètres du niveau de sécurité.
	Options	La zone de groupe **Analyse heuristique** vous permet d'activer ou de désactiver l'utilisation de l'analyseur heuristique pour la tâche d'analyse à la

		demande et de configurer le niveau d'analyse à l'aide d'un curseur. Vous pouvez configurer les paramètres suivants dans la zone de groupe **Intégration aux autres composants** : • Appliquer la zone de confiance pour les tâches d'analyse à la demande. • Utilisation du KSN pour les tâches d'analyse à la demande. • Niveau de priorité de la tâche d'analyse à la demande : exécuter la tâche en arrière-plan (priorité basse) ou considérer l'exécution de la tâche comme un tâche d'analyse rapide.
	Planification	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Vérification de l'intégrité de l'application	**Planification**	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
Surveillance de l'intégrité des fichiers	**Planification**	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

S'agissant de la tâche Annulation de la mise à jour des bases de l'application, vous pouvez configurer uniquement les paramètres de tâche standard contrôlée par Kaspersky Security Center dans les sections **Notifications** et **Exclusions de la zone d'analyse**.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

Tâche Activation de l'application

Pour configurer la tâche d'Activation de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Pour en savoir plus sur la configuration des paramètres dans cette section, consultez le *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Paramètres d'activation**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter une clé pour renouveler la licence.

6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

7. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

9. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Tâches de mise à jour

Pour configurer la tâche Copie des mises à jour, Mise à jour des bases de l'application ou Mise à jour des modules de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.

4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Pour en savoir plus sur la configuration des paramètres dans cette section, consultez le *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Source des mises à jour**, procédez comme suit :

   a. Sélectionnez la source de mise à jour :

   - Serveur d'administration Kaspersky Security Center.
   - Serveurs de mise à jour de Kaspersky.
   - Serveurs HTTP, FTP ou dossiers réseau personnalisés.

   > Pour utiliser un dossier SMB partagé comme source de mise à jour, vous devez renseigner un compte utilisateur pour démarrer une tâche.

   Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

   b. Cliquez sur le bouton **Paramètres de connexion**.

   c. Dans la fenêtre **Paramètres de connexion** qui s'ouvre, configurez l'utilisation d'un serveur proxy pour la connexion aux serveurs de mise à jour de Kaspersky et à d'autres serveurs.

   d. Pour la tâche Mise à jour des bases de l'application, la section **Optimisation de l'utilisation des I/O du disque** permet de configurer les paramètres de la fonction réduisant la charge sur le sous-système disque :

   > La section **Optimisation de l'utilisation des I/O du disque** est disponible uniquement pour la tâche Mise à jour des bases de l'application.

   - **Réduire la charge sur les I/O du disque**
   - **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**

6. Pour la tâche Mise à jour des modules de l'application, définissez, dans la section **Paramètres de mise à jour des modules de l'application**, les actions que Kaspersky Embedded Systems Security doit exécuter lorsque des mises à jour critiques des modules de l'application sont disponibles ou que des informations sur les mises à jour planifiées sont disponibles.

   Vous pouvez également définir les actions que Kaspersky Embedded Systems Security doit exécuter lorsque des mises à jour critiques sont installées.

   > La section **Paramètres de mise à jour des modules de l'application** est disponible uniquement pour la tâche Mise à jour des modules de l'application.

7. Pour la tâche Copie des mises à jour, définissez, dans la section **Paramètres de copie des mises à jour**, l'ensemble des mises à jour et le dossier de destination.

   > La section **Paramètres de copie des mises à jour** est disponible uniquement pour la tâche Copie des mises à jour.

8. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

9. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

10. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres de la tâche de groupe définis seront enregistrés.

S'agissant de la tâche Annulation de la mise à jour des bases de l'application, vous pouvez configurer uniquement les paramètres de tâche standard contrôlée par Kaspersky Security Center dans les sections **Notifications** et **Exclusions de la zone d'analyse**. Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

Vérification de l'intégrité de l'application

Pour configurer la tâche de groupe Vérification de l'intégrité de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.

4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Pour en savoir plus sur la configuration des paramètres dans cette section, consultez le *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Périphériques**, choisissez les périphériques pour lesquels vous souhaitez configurer la tâche Vérification de l'intégrité de l'application.

6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

7. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

9. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

   Les paramètres de la tâche de groupe définis seront enregistrés.

Configuration des paramètres de diagnostic des échecs dans Kaspersky Security Center

En cas de problème lors de l'utilisation de Kaspersky Embedded Systems Security (par exemple, l'application plante), vous pouvez poser un diagnostic. Pour ce faire, vous pouvez activer la création de fichiers de traçage et d'un fichier dump pour le processus de Kaspersky Embedded Systems Security et envoyer ces fichiers pour analyse au Support Technique de Kaspersky.

Kaspersky Embedded Systems Security n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par un utilisateur doté des autorisations adéquates.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Embedded Systems Security. Vous pouvez configurer les autorisations d'accès et permettre l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs qui en ont besoin.

Pour configurer les paramètres de Diagnostic des échecs dans Kaspersky Security Center :

1. Dans la console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application**.
2. Ouvrez la section **Diagnostic des échecs**.
3. Si vous souhaitez que l'application consigne les informations de débogage dans un fichier, cochez la case **Activer le traçage** dans la sous-section **Paramètres de diagnostic des échecs**.
4. Dans le champ **Dossier des fichiers de traçage**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage.

   Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.
5. Configurez le niveau de détail des informations de débogage.
6. Définissez la **Taille maximale d'un fichier de traçage (Mo)**.

   Valeurs disponibles : de 1 à 4 095 Mo. Par défaut, la taille maximale des fichiers de traçage est de 50 Mo.
7. Si vous souhaitez que l'application supprime les fichiers les plus anciens une fois que le nombre maximal de fichiers de traçage a été atteint, cochez la case **Supprimer les fichiers de traçage les plus anciens**.
8. Définissez le paramètre **Nombre maximum de fichiers pour un journal de traces**.

Valeurs disponibles : de 1 à 999. Par défaut, le nombre maximal de fichiers est de 5. Le champ est accessible uniquement si la case **Supprimer les fichiers de traçage les plus anciens** est cochée.

9. Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump**.
10. Dans le champ **Dossier des fichiers dump**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera le fichier dump.

    Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.
11. Cliquez sur le bouton **OK**.

Les paramètres configurés de l'application seront appliqués sur l'appareil protégé.

Programmation des tâches

Vous pouvez planifier les tâches de Kaspersky Embedded Systems Security.

Planification des tâches

La Console de l'application permet de configurer la planification du lancement des tâches locales du système et des tâches définies par l'utilisateur. L'administration des tâches de groupe via la Console de l'application est impossible.

Pour planifier des tâches de groupe à l'aide du plug-in d'administration :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.
2. Sélectionnez le groupe auquel appartient l'appareil protégé.
3. Dans le volet résultats, choisissez l'onglet **Tâches**.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche.
   - Ouvrez le menu contextuel du nom de la tâche et sélectionnez l'option Propriétés.
5. Sélectionnez la section **Planification**.
6. Dans le groupe **Paramètres de planification**, cochez la case **Exécuté selon la planification**.

   Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée de ces tâches est interdite par une stratégie de Kaspersky Security Center.
7. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
   a. Choisissez une des options suivantes dans la liste **Fréquence** :

- **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
- **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
- **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. Précisez les jours de la semaine où la tâche sera lancée (par défaut, les tâches sont exécutées le lundi).
- **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Embedded Systems Security.
- **À la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.

b. Indiquez, dans le champ **Heure de lancement**, l'heure du premier lancement de la tâche.

c. Indiquez, dans le champ **Date de lancement**, la date d'entrée en vigueur de la planification.

Après avoir planifié la date et l'heure de lancement ainsi que la fréquence de la tâche, l'heure estimée du prochain lancement est affichée.

Accédez à l'onglet **Planification** et ouvrez la fenêtre **Paramètres de la tâche**. L'heure estimée de lancement s'affiche dans le champ **Prochain démarrage** en haute de la fenêtre. Chaque fois que vous ouvrez la fenêtre, l'estimation est mise à jour.

Le champ **Prochain démarrage** affiche la valeur **Interdit par la stratégie** si les paramètres de Kaspersky Security Center interdisent le lancement d'une tâche du système planifiée.

8. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.
   - Dans la section **Paramètres d'arrêt de la tâche** :
     a. Cochez la case **Durée**, puis dans les champs à droite, saisissez le nombre maximum d'heures et de minutes pour l'exécution de la tâche.
     b. Cochez la case **Pause à partir de**, puis saisissez dans les champs de droite les heures de début et de fin de l'intervalle par 24 heures au cours duquel la tâche sera suspendue.
   - Dans la section **Paramètres avancés** :
     a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.
     b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.
     c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.
9. Cliquez sur le bouton **OK**.
10. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

Si vous souhaitez configurer les paramètres de l'application pour une tâche unique à l'aide de Kaspersky Security Center, consultez la section Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center.

Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver le lancement des tâches planifiées après ou avant la configuration de la planification.

Pour activer ou désactiver la planification du lancement de la tâche :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.
2. Sélectionnez le groupe auquel appartient l'appareil protégé.
3. Dans le volet résultats, choisissez l'onglet **Tâches**.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche.
   - Ouvrez le menu contextuel du nom de la tâche et sélectionnez l'option Propriétés.
5. Sélectionnez la section **Planification**.
6. Réalisez une des opérations suivantes :
   - Cochez la case **Exécuté selon la planification** si vous souhaitez activer l'exécution planifiée d'une tâche.
   - Décochez la case **Exécuté selon la planification** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

     Les paramètres de la planification du lancement de la tâche ne sont pas supprimés. Ils sont appliqué au prochain lancement planifié de la tâche.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur **Appliquer**.

Les paramètres configurés de la planification du lancement de la tâche sont enregistrés.

Rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils sont basés sur les informations stockées sur le serveur d'administration.

A partir de la version Kaspersky Security Center 11, les types de rapport suivants sont disponibles pour Kaspersky Embedded Systems Security :

- Rapport sur l'état des composants de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Consultez l'*aide de Kaspersky Security Center* pour obtenir des informations détaillées sur tous les rapports de Kaspersky Security Center et la manière de les configurer.

Rapport sur l'état des composants de Kaspersky Embedded Systems Security

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée de l'ensemble de composants défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque composant : *Exécution en cours*, *En pause*, *Arrêté*, *Dysfonctionnement*, *Pas installé*, *Démarrage en cours*.

L'état *Non installé* désigne le composant, et non l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de composants et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de composants et leur état.

Cf. *Aide de Kaspersky Security Center* pour plus de détails sur la création et l'utilisation de sélections.

Pour consulter les états de composant dans les paramètres de l'application :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Sélectionnez l'onglet **Périphériques**, puis ouvrez la fenêtre **Paramètres de l'application**.
3. Sélectionnez la section **Composants**.
4. Consultez le tableau d'état.

Pour consulter un rapport standard Kaspersky Security Center :

1. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.
2. Ouvrez l'onglet **Rapports**.
3. Double-cliquez sur l'élément de liste **Rapport sur l'état des composants de l'application**.

   Un rapport est généré.
4. Consultez les détails de rapport suivants :
   - Diagramme graphique.

- Tableau récapitulatif des composants et nombres totaux d'appareils de réseau où chacun des composants est installé et groupes auxquels ils appartiennent.
- Tableau détaillé spécifiant l'état des composants, la version, le périphérique et le groupe.

Rapports sur les applications interdites dans les modes actifs et d'essai

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications, deux types de rapports peuvent être générés : un rapport sur les applications interdites (si la tâche est démarrée en mode Actif) et un rapport sur les applications interdites en mode test (si la tâche est démarrée en mode Statistiques seulement). Ces rapports affichent des informations sur les applications interdites sur les appareils protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky installées sur les périphériques protégés.

Pour afficher un rapport sur les applications interdites en mode Statistiques seulement :

1. Démarrez la tâche Contrôle du lancement des applications en mode Statistiques seulement.
2. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur l'élément **Rapport sur les applications interdites en mode test**.

   Un rapport est généré.
5. Consultez les détails de rapport suivants :
   - Diagramme graphique qui affiche les dix applications avec le plus grand nombre de démarrages bloqués.
   - Tableau récapitulatif des interdictions d'applications spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
   - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

Pour afficher un rapport sur les applications interdites en mode Actif :

1. Lancez la tâche Contrôle du lancement des applications en mode Actif.
2. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.
3. Ouvrez l'onglet **Rapports**.
4. Double-cliquez sur l'option **Rapport sur les applications interdites**.

   Un rapport est généré.

Ce rapport comprend les mêmes données au sujet des blocs que le rapport sur les applications interdites en mode test.

Utilisation de la console de Kaspersky Embedded Systems Security

Cette section fournit des informations sur la console de Kaspersky Embedded Systems Security et sur l'administration de l'application via la console de l'application installée sur le périphérique protégé ou sur un autre périphérique.

A propos de la console de Kaspersky Embedded Systems Security

La Console de Kaspersky Embedded Systems Security est un composant logiciel enfichable isolé que vous pouvez ajouter à la console Microsoft Management Console.

Vous pouvez administrer l'application via la Console de l'application installée sur le périphérique protégé ou sur un autre périphérique du réseau de l'organisation.

Après que la Console de l'application a été installée sur un autre appareil, il faut réaliser une configuration avancée.

Vous pouvez installer la Console de l'application et Kaspersky Embedded Systems Security sur différents périphériques protégés attribués à différents domaines. Dans ce cas, il peut y avoir des limitations sur l'envoi d'informations depuis l'application vers la Console de l'application. Par exemple, après le démarrage d'une tâche quelconque de l'application, il se peut que l'état de cette tâche reste inchangé dans la console de l'application.

Lors de l'installation de la Console de l'application, l'assistant d'installation crée le fichier kavfs.msc dans le dossier d'installation et ajoute le composant logiciel enfichable Kaspersky Embedded Systems Security à la liste des composants logiciels enfichables isolés de Microsoft Windows.

Vous pouvez démarrer la Console de l'application depuis le menu **Démarrer**. Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Embedded Systems Security ou l'ajouter à la console Microsoft Management Console en tant que nouvel élément de son arborescence.

Sous la version 64 bits de Microsoft Windows, vous pouvez ajouter le composant logiciel enfichable de Kaspersky Embedded Systems Security uniquement dans la console Microsoft Management Console de la version 32 bits. Pour ajouter le composant logiciel enfichable Kaspersky Embedded Systems Security, ouvrez Microsoft Management Console via la ligne de commande en exécutant la commande mmc.exe /32.

Plusieurs composants logiciels enfichables de Kaspersky Embedded Systems Security peuvent être ajoutés à une Microsoft Management Console ouverte en mode auteur. Vous pouvez ensuite administrer la protection de plusieurs périphériques sur lesquels Kaspersky Embedded Systems Security est installé.

Interface de la console de Kaspersky Embedded Systems Security

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

Fenêtre de la console de Kaspersky Embedded Systems Security

La Console de Kaspersky Embedded Systems Security s'affiche dans l'arborescence de Microsoft Management Console en tant que nœud nommé Kaspersky Security.

Après la connexion à la copie de Kaspersky Embedded Systems Security installée sur un autre périphérique protégé, le nom du nœud reprend le nom du périphérique protégé sur lequel l'application est installée ainsi que le nom du compte utilisateur sous les privilèges duquel la connexion a été réalisée : **Kaspersky Embedded Systems Security <nom du périphérique protégé> sous <nom du compte utilisateur>**. En cas de connexion à une instance de Kaspersky Embedded Systems Security installée sur le même périphérique protégé que la console de l'application, le nom du nœud devient **Kaspersky Embedded Systems Security**.

Arborescence de la console de l'application

L'arborescence de la console de l'application affiche le nœud **Kaspersky Embedded Systems Security** et les nœuds enfants correspondant aux composants opérationnels de l'application.

Le nœud **Kaspersky Embedded Systems Security** inclut les nœuds enfants suivants :

- **Protection en temps réel de l'ordinateur** : administration des tâches de protection en temps réel de l'ordinateur et des services KSN. Le nœud **Protection en temps réel de l'ordinateur** permet de configurer les tâches suivantes :
  - **Protection des fichiers en temps réel**
  - **Utilisation du KSN**
  - **Protection contre les exploits**
- **Contrôle de l'ordinateur** : contrôle les lancements des applications installées sur un périphérique protégé ainsi que les connexions des périphériques externes. Le nœud **Contrôle de l'ordinateur** permet de configurer les tâches suivantes :
  - **Contrôle du lancement des applications**
  - **Contrôle des périphériques**
  - **Gestion du pare-feu**
- **Génération automatique de règles** : configuration de la création automatique des règles de groupe et système pour les tâches Contrôle du lancement des applications et Contrôle des périphériques.
  - **Génération des règles du Contrôle du lancement des applications**
  - **Générateur de règles pour le Contrôle des périphériques**
  - Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).

    Des tâches de groupe sont créées dans Kaspersky Security Center. Il est impossible d'administrer des tâches de groupe via la console de l'application.
- **Diagnostic du système** : configuration des paramètres du contrôle des opérations réalisées sur les fichiers et de l'inspection des journaux des événements Windows.
  - **Moniteur d'intégrité des fichiers**
  - **Inspection des journaux**

- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Un nœud séparé existe pour chacune des tâches :
  - **Analyse au démarrage du système d'exploitation**
  - **Analyse rapide**
  - **Analyse de la quarantaine**
  - **Vérification de l'intégrité de l'application**
  - Tâches définies par l'utilisateur **<Nom des tâches>** (le cas échéant)

  Le nœud affiche les tâches système créées lors de l'installation de l'application, les tâches définies par l'utilisateur et les tâches d'analyse à la demande de groupe créées et transmises à un périphérique protégé à l'aide de Kaspersky Security Center.

- **Mise à jour** : gère la mise à jour des bases de données et des modules de Kaspersky Embedded Systems Security ainsi que la copie des mises à jour dans le dossier de la source locale de mises à jour. Le nœud contient des nœuds enfants permettant d'administrer chacune des tâches de mise à jour et la dernière tâche **Annulation de la mise à jour des bases de l'application** :
  - **Mise à jour des bases de l'application**
  - **Mise à jour des modules de l'application**
  - **Copie des mises à jour**
  - **Annulation de la mise à jour des bases de l'application**

  Le nœud affiche toutes les tâches définies par l'utilisateur et les tâches de groupe de mise à jour créées et transmises au périphérique protégé via Kaspersky Security Center.

- **Stockages** : gestion des paramètres de quarantaine et de sauvegarde.
  - **Quarantaine**
  - **Sauvegarde**

- **Journaux et notifications** : gestion des journaux d'exécution de la tâche locale, du journal de sécurité et du journal d'audit système de Kaspersky Embedded Systems Security.
  - **Journaux de sécurité**
  - **Journal d'audit système**
  - **Journaux d'exécution de la tâche**

- **Licence** : ajout et suppression de clés de licence pour Kaspersky Embedded Systems Security, consultation des informations relatives aux licences.

Panneau des résultats

Le panneau de détails reprend les informations relatives au nœud sélectionné. Si vous avez choisi le nœud **Kaspersky Embedded Systems Security**, le panneau de détails affiche les informations relatives à l'état actuel de la protection du périphérique, les informations relatives à Kaspersky Embedded Systems Security, l'état de la protection de ses composants fonctionnels et la date d'expiration de la licence.

Menu contextuel du nœud Kaspersky Embedded Systems Security

À l'aide des options du menu contextuel du nœud **Kaspersky Embedded Systems Security**, vous pouvez exécuter les opérations suivantes :

- **Se connecter à un autre ordinateur**. Se connecter à un autre périphérique pour administrer la version de Kaspersky Embedded Systems Security installée sur cet périphérique. Pour effectuer cette opération, vous pouvez également cliquer sur le lien situé dans le coin inférieur droit du panneau de détails du nœud **Kaspersky Embedded Systems Security**.
- **Démarrer le service** / **Arrêter le service**. Lancez ou arrêtez l'application ou une tâche sélectionnée. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. L'exécution de ces opérations est également disponible dans les menus contextuels des tâches de l'application.
- **Configurer l'analyse des disques amovibles**. Configurez l'analyse des disques amovibles connectés via le port USB au périphérique protégé.
- **Configurer les paramètres de la zone de confiance**. Consultez et configurez les paramètres de la zone de confiance.
- **Modifier les droits de l'utilisateur pour l'administration de l'application**. Consultez et configurez les privilèges d'accès aux fonctions de Kaspersky Embedded Systems Security.
- **Modifier les droits d'utilisateurs pour l'administration du Service Kaspersky Security**. Consultez et configurez les privilèges d'accès à l'administration du Service Kaspersky Security.
- **Exporter les paramètres**. Enregistrez les paramètres de l'application dans un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Importer les paramètres**. Importez les paramètres de l'application depuis un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Données sur les mises à jour disponibles pour l'application et ses modules**. Affiche les informations relatives à Kaspersky Embedded Systems Security et aux mises à jour des modules de l'application disponibles.
- **Rafraîchir**. Actualisez le contenu de la fenêtre de la console de l'application. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Propriétés**. Consultez et configurez les paramètres de fonctionnement de Kaspersky Embedded Systems Security ou d'une tâche sélectionnée. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

  Pour exécuter cette opération, vous pouvez également utiliser le lien **Propriétés de l'application** dans le panneau de détails du nœud **Kaspersky Embedded Systems Security** ou le bouton dans la barre d'outils.

- **Aide**. Consultez les informations reprises dans l'aide de Kaspersky Embedded Systems Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Barre d'outils et menu contextuel des tâches de Kaspersky Embedded Systems Security

Vous pouvez administrer les tâches de Kaspersky Embedded Systems Security à l'aide des options du menu contextuel de chaque tâche dans l'arborescence de la console de l'application.

A l'aide des options du menu contextuel de la tâche sélectionnée, vous pouvez exécuter les opérations suivantes :

- **Démarrer** / **Arrêter**. Démarrer ou arrêter l'exécution de la tâche. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils.
- **Reprendre** / **Suspendre**. Reprenez ou suspendez l'exécution de la tâche. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches Protection en temps réel de l'ordinateur et Analyse à la demande.
- **Ajouter une tâche**. Créez une nouvelle tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.
- **Ouvrir le journal**. Consultez et administrez un journal d'exécution de la tâche. Cette opération est disponible pour toutes les tâches.
- **Supprimer la tâche**. Supprimez une tâche définie par l'utilisateur. L'opération est disponible pour les tâches d'analyse à la demande.
- **Modèles des paramètres**. Administrez les modèles. Cette opération est disponible pour les tâches Protection des fichiers en temps réel et Analyse à la demande.

Icône de la barre d'état système dans la zone de notification

Chaque fois que Kaspersky Embedded Systems Security se lance automatiquement après le redémarrage d'un périphérique protégé, l'icône de la barre d'état système apparaît dans la zone de notification de la barre d'outils  . L'icône est affichée par défaut si vous avez installé le composant Icône dans la barre d'état système lors de l'installation de l'application.

L'aspect de l'icône de la barre d'état système indique l'état actuel de la protection du périphérique. Il existe deux types d'état :

	Actif (icône colorée) : au moins une des tâches suivantes est en cours d'exécution : Protection des fichiers en temps réel ou Contrôle du lancement des applications
	Inactif (icône grisée) : aucune des tâches suivantes n'est en cours d'exécution : Protection des fichiers en temps réel ou Contrôle du lancement des applications

Vous pouvez ouvrir le menu contextuel de l'icône de la barre d'état système d'un clic droit de la souris.

Le menu contextuel contient plusieurs commandes d'affichage de fenêtre de l'application (cf. tableau ci-après).

Commandes du menu contextuel de l'icône de la barre d'état système

Instruction	Description
Ouvrir la Console de l'application	Ouvrez la console de Kaspersky Embedded Systems Security (si celle-ci est installée).
Ouvrir l'interface de diagnostic compacte	Ouvre l'interface de diagnostic compacte.

A propos de l'application	Ouvre la fenêtre **A propos de l'application** qui contient des informations sur Kaspersky Embedded Systems Security. Si vous êtes un utilisateur enregistré de Kaspersky Embedded Systems Security, la fenêtre **A propos de l'application** contient des informations sur les mises à jour urgentes installées.
Fermer	Masque l'icône de la barre d'état système dans la zone de notification de la barre des tâches.

Vous pouvez à tout moment restaurer l'icône masquée de la barre d'état système.

Pour afficher à nouveau l'icône dans la barre d'état,

dans le menu **Démarrer** de Microsoft Windows, sélectionnez **Tous les programmes** > **Kaspersky Embedded Systems Security** > **Icône dans la barre d'état système**.

Les noms des paramètres peuvent varier selon les versions du système d'exploitation installé.

Lors de la configuration des paramètres généraux de Kaspersky Embedded Systems Security, vous pouvez activer ou désactiver l'affichage de l'icône de la barre d'état système lors de chaque lancement automatique de l'application après un redémarrage d'un périphérique protégé.

Administration de Kaspersky Embedded Systems Security via la Console de l'application sur un autre périphérique

Il est possible d'administrer Kaspersky Embedded Systems Security via la console de l'application installée sur un périphérique distant.

Pour administrer l'application via la console de Kaspersky Embedded Systems Security sur un périphérique distant, confirmez que :

- Les utilisateurs de la Console de l'application sur le périphérique distant sont ajoutés au groupe ESS Administrators sur le périphérique protégé.
- Les connexions réseau sont autorisées pour le processus du service Kaspersky Security Management (kavfsgt.exe), si le Pare-feu Windows est activé sur l'appareil protégé.
- La case **Autoriser l'accès à distance** a été cochée dans la fenêtre de l'Assistant d'installation lors de l'installation de Kaspersky Embedded Systems Security.

Si Kaspersky Embedded Systems Security sur le périphérique distant est protégé par un mot de passe, vous devez le saisir pour accéder à l'administration de l'application via la console de l'application.

Configuration des paramètres généraux de l'application via la Console de l'application

Les paramètres généraux et les paramètres du diagnostic des échecs de Kaspersky Embedded Systems Security définissent les conditions générales de fonctionnement de l'application. Ils déterminent le nombre de processus que Kaspersky Embedded Systems Security va utiliser, ils permettent d'activer la reprise des tâches de Kaspersky Embedded Systems Security après un arrêt inopiné de leur fonctionnement, de tenir un journal, d'activer la création d'un fichier dump des processus de Kaspersky Embedded Systems Security lorsqu'ils sont arrêtés en raison d'une erreur et de configurer d'autres paramètres généraux.

La configuration des paramètres du fonctionnement de l'application dans la console de l'application n'est pas disponible si la modification de ces paramètres est interdite dans la stratégie active de Kaspersky Security Center.

Pour configurer les paramètres de Kaspersky Embedded Systems Security :

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et réalisez l'une des actions suivantes :

   - Dans le panneau de détails du nœud, suivez le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application** s'ouvre.

2. Dans la fenêtre qui s'ouvre, configurez les paramètres généraux de Kaspersky Embedded Systems Security en fonction de vos préférences :

   - L'onglet **Montée en puissance et interface** permet de configurer les paramètres suivants :
     - Dans la section **Paramètres d'optimisation** :
       - Nombre de processus pour la protection en temps réel de l'ordinateur
       - Nombre de processus de travail pour les tâches d'analyse à la demande en arrière-plan
   - Dans la section **Interaction avec l'utilisateur**, décidez si l'icône de l'application doit apparaître dans la barre des tâches après le lancement de l'application.
   - L'onglet **Sécurité et fiabilité** permet de configurer les paramètres suivants :
     - Dans la section **Paramètres de protection par mot de passe**, configurez la protection des processus de l'application.
     - Dans la section **Paramètres de protection par mot de passe**, configurez les paramètres pour la protection par mot de passe des fonctions de l'application.
     - Dans la section **Auto-défense**, indiquez le nombre de tentatives de restauration des tâches d'analyse à la demande en cas d'échec suite à une erreur.
   - La section **Maximum de restaurations des tâches d'analyse à la demande** permet de choisir les actions de Kaspersky Embedded Systems Security après le passage à l'alimentation de secours.
   - Sous l'onglet **Paramètres de l'analyse** :
     - **Restaurer les attributs du fichier après l'analyse**
     - **Limiter l'utilisation du processeur pour les threads d'analyse**

- **Limite supérieure (pour cent)**
- **Dossier pour les fichiers temporaires créés pendant l'analyse**

- Sous l'onglet **Paramètres de connexion** :
  - Définissez les paramètres d'utilisation du serveur proxy dans la section **Paramètres du serveur proxy**.
  - Dans la section **Paramètres d'authentification du serveur proxy**, indiquez le type d'authentification et les données requises pour l'authentification sur le serveur proxy.
  - Dans la section **Licence**, indiquez si Kaspersky Security Center doit être utilisé en guise de serveur proxy pour l'activation de l'application.
- Sous l'onglet **Diagnostic des échecs** :
  - Si vous souhaitez que l'application consigne les informations de débogage dans un fichier, cochez la case **Activer le traçage** dans la sous-section **Paramètres de débogage**.
  - Dans le champ **Dossier des traces**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage.

    Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.
  - Configurez le niveau de détail des informations de débogage.
  - Définissez la **Taille maximale du fichier de traçage**.

    Valeurs disponibles : de 1 à 4 095 Mo. Par défaut, la taille maximale des fichiers de traçage est de 50 Mo.
  - Si vous souhaitez que l'application supprime les fichiers les plus anciens une fois que le nombre maximal de fichiers de traçage est atteint, cochez la case **Supprimer les fichiers de traçage les plus anciens**.
  - Définissez le paramètre **Nombre maximal de fichiers pour un journal de traçage**.

    Valeurs disponibles : de 1 à 999. Par défaut, le nombre maximal de fichiers est de 5. Le champ est accessible uniquement si la case **Supprimer les fichiers de traçage les plus anciens** est cochée.
  - Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump**.
  - Dans le champ **Dossier des fichiers dump**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera le fichier dump.

    Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et les fichiers dump en clair. Le dossier d'enregistrement des fichiers est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Embedded Systems Security. Vous pouvez configurer les autorisations d'accès et permettre l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement aux utilisateurs qui en ont besoin.

3. Cliquez sur le bouton **OK**.

Les paramètres de Kaspersky Embedded Systems Security sont enregistrés.

Administration des tâches de Kaspersky Embedded Systems Security

Cette section contient des informations sur la création, la configuration, le lancement et l'arrêt des tâches de Kaspersky Embedded Systems Security.

Catégories de tâche de Kaspersky Embedded Systems Security

Les fonctions de la protection en temps réel de l'ordinateur, de contrôle de l'ordinateur, de l'analyse à la demande et de la mise à jour de Kaspersky Embedded Systems Security sont réalisées sous forme de tâches.

Ces tâches peuvent être administrées via les options du menu contextuel du nom de la tâche dans l'arborescence de la console de l'application, de la barre d'outils et de la barre d'accès rapide. Vous pouvez consulter les informations sur l'état d'une tâche dans le volet résultats. Les opérations d'administration des tâches sont enregistrées dans le journal d'audit système.

Il existe deux types de tâches de Kaspersky Embedded Systems Security : *local* et *groupe*

Tâches locales

Les tâches locales ne peuvent être exécutées que sur le périphérique protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- **Tâches locales du système**. Ces tâches sont créées automatiquement lors de l'installation de Kaspersky Embedded Systems Security. Vous pouvez modifier les paramètres de toutes les tâches locales du système à l'exception des tâches Analyse de la quarantaine et Annulation de la mise à jour des bases de l'application. Il est impossible de renommer ou de supprimer les tâches locales du système. Vous pouvez lancer les tâches locales du système d'analyse à la demande en même temps que les tâches définies par l'utilisateur.

- **Tâches locales définies par l'utilisateur**. Vous pouvez créer des tâches d'analyse à la demande dans la console de l'application. Kaspersky Security Center permet de créer des tâches d'analyse à la demande, de mise à jour des bases de l'application, d'annulation de la mise à jour des bases de l'application et de copie des mises à jour. Vous pouvez renommer, configurer et supprimer les tâches définies par l'utilisateur. Vous pouvez exécuter simultanément plusieurs tâches définies par l'utilisateur.

Tâches de groupe

Vous pouvez gérer les tâches de groupe et les tâches pour des ensembles d'appareils protégés à partir de Kaspersky Security Center. Toutes les tâches de groupe sont des tâches définies par l'utilisateur. Les tâches de groupe sont également affichées dans la Console de l'application. La console de l'application permet uniquement de consulter l'état des tâches de groupe. Vous ne pouvez pas utiliser la Console de l'application pour administrer ou configurer des tâches de groupe.

Lancement, suspension, rétablissement et arrêt manuels des tâches

Vous ne pouvez suspendre et reprendre que les tâches Protection en temps réel de l'ordinateur et Analyse à la demande. Aucune autre tâche ne peut être suspendue ou relancée manuellement.

Pour démarrer, suspendre, reprendre ou arrêter une tâche :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel de la tâche.
2. Sélectionnez l'une des options suivantes : **Démarrer**, **Suspendre**, **Reprendre** ou **Arrêter**.

L'opération sera réalisée et enregistrée dans le journal d'audit système.

Lorsque vous reprenez une tâche d'analyse à la demande, Kaspersky Embedded Systems Security reprend l'opération à partir de l'objet analysé au moment de l'interruption.

Programmation des tâches

Vous pouvez planifier les tâches de Kaspersky Embedded Systems Security.

Configuration des paramètres de planification d'une tâche

La Console de l'application permet de planifier le lancement des tâches système locales et des tâches définies par l'utilisateur. Cependant, il n'est pas possible de planifier le lancement des tâches de groupe.

Pour planifier une tâche :

1. Ouvrez le menu contextuel de la tâche à planifier.
2. Choisissez l'option **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la planification**.
4. Suivez ces étapes pour définir les paramètres de planification :
   a. Dans la liste déroulante **Fréquence**, sélectionnez une des options :
      - **Toutes les heures** : pour exécuter la tâche toutes les heures ; précisez le nombre d'heures dans le champ **Chaque** <chiffre> **heure(s)**.
      - **Tous les jours** : pour exécuter selon un intervalle en jours ; précisez le nombre de jours dans le champ **Chaque <chiffre> jour(s)**.
      - **Toutes les semaines** : pour exécuter la tâche selon un intervalle en semaines ; précisez le nombre de semaines dans le champ **Chaque les <chiffre> semaine(s) le**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi).
      - **Au lancement de l'application** : pour exécuter la tâche à chaque lancement de Kaspersky Embedded Systems Security.
      - **À la mise à jour des bases de l'application** : pour exécuter la tâche après chaque mise à jour des bases de l'application.
   b. Renseignez dans le champ **Heure de lancement** l'heure du premier lancement de la tâche.

c. Renseignez dans le champ **Date de lancement** la date du premier lancement de la tâche.

Après avoir indiqué la fréquence d'exécution de la tâche, l'heure de la première exécution et la date d'entrée en vigueur de la planification, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

Le champ **Prochain démarrage** affiche la valeur **Interdit par la stratégie** si les paramètres de la stratégie active de Kaspersky Security Center interdisent le lancement d'une tâche locales du système planifiée.

5. Utilisez l'onglet **Avancé** pour définir les paramètres de planification suivants :

- Dans la section **Paramètres d'arrêt de la tâche** :

  a. Cochez la case **Durée**. Dans les champs de droite, saisissez la durée maximale de la tâche en heures et en minutes.

  b. Cochez la case **Pause à partir de**. Dans les champs de droite, saisissez quand il faudra interrompre et reprendre la tâche (sous 24 heures).

- Dans la section **Paramètres avancés** :

  a. Cochez la case **Suspendre la planification à partir du** et renseignez la date de fin de la planification de la tâche.

  b. Cochez la case **Lancer les tâches non exécutées** pour lancer les tâches ignorées.

  c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.

6. Cliquez sur le bouton **OK**.

Les paramètres de la planification de la tâche sont enregistrés.

Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver les tâches planifiées après ou avant la configuration de la planification.

Pour activer ou désactiver le lancement d'une tâche planifiée :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel de la tâche planifiée.
2. Choisissez l'option **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez une des options suivantes sous l'onglet **Planification** :

- Cochez la case **Exécuté selon la planification** pour activer l'exécution planifiée d'une tâche.
- Décochez la case **Exécuté selon la planification** pour désactiver l'exécution planifiée d'une tâche.

Les paramètres de planification des tâches ne sont pas supprimés, mais appliqués la prochaine fois que vous activez le lancement d'une tâche planifiée.

4. Cliquez sur le bouton **OK**.

Les paramètres de la planification de la tâche sont enregistrés.

Utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez lancer les tâches sous un compte système ou sous un autre compte utilisateur que vous désignerez.

A propos de l'utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez spécifier le compte pour exécuter les tâches de Kaspersky Embedded Systems Security suivantes :

- Génération des règles du Contrôle du lancement des applications
- Générateur de règles pour le Contrôle des périphériques
- Analyse à la demande
- Mise à jour

Par défaut, les tâches désignées sont exécutées avec les autorisations du compte système.

Il est recommandé de définir un autre compte avec les privilèges suffisants dans les cas suivants :

- Tâche **Mise à jour** : si la source de mise à jour est un dossier partagé sur un autre périphérique du réseau.
- Tâche **Mise à jour** : si l'accès à la source des mises à jour s'opère via un serveur proxy doté de la vérification intégrée de l'authenticité Microsoft Windows (authentification NTLM).
- Tâche **Analyse à la demande** : si le compte système ne possède pas les autorisations d'accès aux objets à analyser (par exemple, aux fichiers dans les dossiers partagés du périphérique protégé).
- Tâche **Génération des règles du Contrôle du lancement des applications** : si les règles générées sont exportées vers un fichier de configuration inaccessible au compte système (par exemple, dans un des dossiers partagés du périphérique protégé).

Vous pouvez lancer les tâches de Mise à jour, d'Analyse à la demande et de Génération des règles du Contrôle du lancement des applications avec les autorisations du compte système. Kaspersky Embedded Systems Security exécute ces tâches et accède aux dossiers partagés sur l'autre périphérique du réseau si ce périphérique est enregistré dans le même domaine que le périphérique protégé. Dans ce cas, le compte système doit posséder les autorisations d'accès à ces dossiers. Kaspersky Embedded Systems Security accède à ce périphérique avec les privilèges du compte **<Nom_de_domaine \ nom_du_périphérique>**.

Définition du compte utilisateur pour l'exécution de la tâche

Pour désigner un compte pour démarrer une tâche :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel de la tâche que vous souhaitez lancer sous un compte spécifique.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Exécuter en tant que** , procédez comme suit :

   a. Choisissez l'option **Nom d'utilisateur**.

   b. Saisissez le nom et le mot de passe de l'utilisateur dont vous souhaitez utiliser le compte.

   L'utilisateur que vous sélectionnez doit être enregistré sur l'appareil protégé ou dans le même domaine.

   c. Confirmez le mot de passe.
4. Cliquez sur le bouton **OK**.

Les modifications apportées aux paramètres seront enregistrées.

Importation et exportation des paramètres

Cette section explique comment exporter les paramètres de Kaspersky Embedded Systems Security. Vous apprendrez également comment exporter des paramètres logiciels spécifiques vers un fichier de configuration XML et comment importer ces paramètres à partir d'un fichier de configuration dans l'application.

A propos de l'importation et de l'exportation des paramètres

Vous pouvez exporter les paramètres de Kaspersky Embedded Systems Security dans un fichier de configuration au format XML et importer les paramètres de Kaspersky Embedded Systems Security depuis le fichier de configuration. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des composants distincts dans un fichier de configuration.

Quand vous exportez tous les paramètres de Kaspersky Embedded Systems Security, le fichier reprend les paramètres généraux de l'application et les paramètres des fonctions et modules suivants de Kaspersky Embedded Systems Security :

- Protection des fichiers en temps réel
- Utilisation du KSN
- Contrôle des périphériques
- Contrôle du lancement des applications
- Générateur de règles pour le Contrôle des périphériques
- Génération des règles du Contrôle du lancement des applications

- Tâche d'analyse à la demande définie par l'utilisateur
- Moniteur d'intégrité des fichiers
- Inspecteur des journaux
- Mise à jour des bases de données et des modules de l'application Kaspersky Embedded Systems Security
- Quarantaine
- Sauvegarde
- Journaux.
- Notifications de l'administrateur et des utilisateurs
- Zone de confiance
- Protection contre les exploits
- Protection par mot de passe

Vous pouvez également enregistrer les paramètres généraux de Kaspersky Embedded Systems Security dans un fichier, avec les privilèges des comptes utilisateur.

Vous ne pouvez pas exporter les paramètres des tâches de groupe.

Kaspersky Embedded Systems Security exporte tous les mots de passe qui sont utilisés par l'application, par exemple, les paramètres du compte utilisateur sous lequel l'exécution des tâches ou la connexion au serveur proxy a lieu. Les mots de passe exportés dans le fichier de configuration sont chiffrés. Vous pouvez importer les mots de passe uniquement à l'aide d'une version de Kaspersky Embedded Systems Security installée sur ce périphérique protégé, si elle n'a pas été réinstallée ou mise à jour.

Vous ne pouvez pas importer des mots de passe préalablement enregistrés à l'aide d'une version de Kaspersky Embedded Systems Security installée sur un autre périphérique protégé. Après l'importation des paramètres sur un autre appareil protégé, vous devez saisir tous les mots de passe manuellement.

Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, l'application exporte les valeurs appliquées par la stratégie.

Vous pouvez importer les paramètres depuis le fichier de configuration qui contient les paramètres uniquement de certains composants de Kaspersky Embedded Systems Security (par exemple, créé dans une version de Kaspersky Embedded Systems Security sans la totalité des composants). Après l'importation des paramètres, seuls les paramètres de Kaspersky Embedded Systems Security repris dans le fichier de configuration sont modifiés. Les autres paramètres demeurent inchangés.

Les paramètres verrouillés de la stratégie active de Kaspersky Security Center ne sont pas modifiés lors de l'importation des paramètres.

Exportation des paramètres

Pour exporter les paramètres vers un fichier de configuration :

1. Dans l'arborescence de la console de l'application, réalisez une des opérations suivantes :

   - Dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**, sélectionnez **Exporter les paramètres** pour exporter tous les paramètres de Kaspersky Embedded Systems Security.
   - Dans le menu contextuel d'une tâche spécifique, choisissez l'option **Exporter les paramètres** afin d'exporter les paramètres d'un module individuel de l'application.
   - Pour exporter les paramètres de la zone de confiance :

     a. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

     b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

     La fenêtre **Zone de confiance** s'ouvre.

     c. Cliquez sur le bouton **Exporter**.

     L'assistant d'exportation des paramètres s'ouvre.

2. Suivez les instructions de l'**Assistant Exportation des paramètres** : indiquez le nom du fichier de configuration dans lequel vous souhaitez enregistrer les paramètres ainsi que le chemin d'accès à celui-ci.

   Vous pouvez utiliser des variables d'environnement système lors de la spécification du chemin, mais pas des variables d'environnement utilisateur.

   Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, l'application exporte les paramètres de la stratégie.

3. Dans la fenêtre **Exportation des paramètres de l'application terminée**, cliquez sur le bouton **Fermer**.

L'assistant d'exportation des paramètres se ferme et enregistre les paramètres d'exportation.

Importation des paramètres

Pour importer des paramètres à partir d'un fichier de configuration enregistré :

1. Dans l'arborescence de la console de l'application, réalisez une des opérations suivantes :

   - Dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**, sélectionnez **Importer les paramètres** pour importer tous les paramètres de Kaspersky Embedded Systems Security.
   - Dans le menu contextuel d'une tâche spécifique, choisissez l'option **Importer les paramètres**, afin d'importer les paramètres d'un module individuel de l'application.
   - Pour importer les paramètres de la zone de confiance :

     a. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

     b. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

     La fenêtre **Zone de confiance** s'ouvre.

     c. Cliquez sur **Importer**.

L'assistant d'importation de paramètres s'ouvre.

2. Suivez les instructions affichées dans l'**Assistant Importation des paramètres** : identifiez le fichier de configuration contenant les paramètres que vous souhaitez importer.

   Une fois que les paramètres généraux de Kaspersky Embedded Systems Security ou de ses composants auront été importés sur le périphérique protégé, vous ne pourrez plus revenir aux paramètres antérieurs.

3. Dans la fenêtre **Importation des paramètres de l'application terminée**, cliquez sur le bouton **Fermer**.

   L'assistant d'importation de paramètres se ferme et enregistre les paramètres importés.

4. Dans la barre d'outils de la Console de l'application, cliquez sur le bouton **Actualiser**.

La fenêtre Console de l'application affiche les paramètres importés.

Kaspersky Embedded Systems Security n'importe pas les mots de passe (identifiants pour l'exécution de tâches ou la connexion au serveur proxy) d'un fichier créé sur un autre appareil protégé ou sur ce même appareil protégé après une réinstallation ou de mise à jour de Kaspersky Embedded Systems Security sur celui-ci. Après la fin de l'importation, il faudra saisir les mots de passe manuellement.

Utilisation des modèles de paramètres de sécurité

Cette section explique l'utilisation des modèles de paramètres de sécurité dans les tâches de protection et d'analyse de Kaspersky Embedded Systems Security.

A propos des modèles de paramètres de sécurité

Vous pouvez configurer manuellement les paramètres de sécurité d'un nœud dans l'arborescence ou dans la liste des ressources fichier du périphérique protégé et enregistrer les valeurs définies dans un modèle. Vous pourrez ensuite appliquer ce modèle pour préciser les paramètres de sécurité d'autres entrées dans les tâches de protection et d'analyse de Kaspersky Embedded Systems Security.

Vous pouvez configurer les paramètres de sécurité à l'aide de modèles pour les tâches suivantes de Kaspersky Embedded Systems Security :

- Protection des fichiers en temps réel
- Analyse au démarrage du système d'exploitation
- Analyse rapide
- Tâche d'analyse à la demande définie par l'utilisateur

Les paramètres de sécurité d'un modèle appliqué à un nœud parent dans l'arborescence des ressources de fichier de l'appareil protégé sont appliqués à tous les nœuds enfants. Le modèle d'un nœud parent n'est pas appliqué aux nœuds enfants dans les cas suivants :

- Si vous avez spécifié les paramètres de sécurité des nœuds enfants séparément.
- Si les nœuds enfants sont virtuels. Il faudra alors dans ce cas appliquer le modèle à chaque nœud virtuel séparément.

Création d'un modèle de paramètres de sécurité

Pour enregistrer manuellement les paramètres de sécurité du nœud dans un modèle, procédez comme suit :

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez créer un modèle de paramètres de sécurité.
2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.
3. Dans l'arborescence ou dans la liste des ressources de fichier réseau de du périphérique protégé, sélectionnez le modèle que vous souhaitez consulter.
4. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Enregistrer comme modèle**.

   La fenêtre **Propriétés du modèle** s'ouvre.
5. Dans le champ **Nom du modèle**, saisissez le nom du modèle.
6. Dans le champ **Description**, saisissez des informations supplémentaires sur le modèle.
7. Cliquez sur le bouton **OK**.

Le modèle de paramètres de sécurité est enregistré.

Consultation des paramètres de sécurité du modèle

Pour afficher les paramètres de sécurité dans un modèle que vous avez créé :

1. Dans l'arborescence de la Console de l'application, sélectionnez la tâche avec le modèle de paramètres de sécurité que vous souhaitez afficher.
2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

   La fenêtre **Modèles** s'ouvre.
3. Dans la liste des modèles de la fenêtre, sélectionnez le modèle que vous souhaitez consulter.
4. Cliquez sur le bouton **Voir**.

La fenêtre **<Nom du modèle>** s'ouvre. L'onglet **Général** affiche le nom du modèle et des informations supplémentaires sur le modèle. L'onglet **Options** reprend les paramètres de sécurité enregistrés dans le modèle.

Application du modèle de paramètres de sécurité

Pour appliquer les paramètres de sécurité du modèle au nœud sélectionné, procédez comme suit :

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez appliquer un modèle de paramètres de sécurité.

2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.

3. Dans l'arborescence ou dans la liste des ressources de fichier réseau du périphérique protégé, ouvrez le menu contextuel du nœud ou de l'élément auquel vous souhaitez appliquer le modèle.

4. Sélectionnez **Appliquer un modèle → <Nom du modèle>**.

5. Cliquez sur le bouton **Enregistrer**.

Cette action applique le modèle de paramètres de sécurité au nœud sélectionné dans l'arborescence des ressources de fichiers de l'appareil protégé. La valeur de l'onglet **Niveau de sécurité** pour le nœud sélectionné passe à **Personnalisé**.

Si les paramètres de sécurité d'un modèle sont appliqués à un nœud parent dans l'arborescence des ressources de fichiers de l'appareil protégé, ces paramètres sont également appliqués à tous les nœuds enfants.

Vous pouvez configurer séparément la protection ou la zone d'analyse des nœuds enfants dans l'arborescence des ressources de fichiers de l'appareil protégé. Dans ce cas, les paramètres de sécurité du modèle appliqué au nœud parent ne sont pas automatiquement appliqués aux nœuds enfants.

Pour appliquer les paramètres de sécurité du modèle à tous les nœuds sélectionnés :

1. Dans l'arborescence de la console de l'application, sélectionnez la tâche pour laquelle vous souhaitez appliquer le modèle de paramètres de sécurité.

2. Dans le panneau de détails de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.

3. Dans l'arborescence ou dans la liste des ressources de fichier réseau de l'appareil protégé, choisissez un nœud parent pour appliquer le modèle au nœud sélectionné et à ses nœuds enfants.

4. Dans le menu contextuel, sélectionnez **Appliquer un modèle →<Nom du modèle>**.

5. Cliquez sur le bouton **Enregistrer**.

Les modèles de paramètres de sécurité sont appliqués au parent et à tous les nœuds enfants dans l'arborescence des ressources de fichier de l'appareil protégé. La valeur de l'onglet **Niveau de sécurité** pour le nœud sélectionné passe à **Personnalisé**.

Suppression du modèle de paramètres de sécurité

Pour supprimer un modèle de paramètres de sécurité :

1. Dans l'arborescence de la Console de l'application, sélectionnez la tâche avec le modèle de paramètres de sécurité que vous souhaitez supprimer.

2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

La fenêtre **Modèles** s'ouvre.

Le volet résultats du nœud parent **Analyse à la demande** permet de consulter les modèles de paramètres pour les tâches d'analyse à la demande.

3. Dans la liste des modèles, sélectionnez le modèle que vous souhaitez supprimer.
4. Cliquez sur le bouton **Supprimer**.
   La fenêtre de confirmation de la suppression s'ouvre.
5. Cliquez sur **Oui** dans la fenêtre qui s'ouvre.

Le modèle sélectionné sera supprimé.

Vous pouvez appliquer le modèle de paramètres de sécurité pour protéger ou analyser les nœuds dans l'arborescence des ressources de fichiers du périphérique protégé. Dans ce cas, les paramètres de sécurité de ces nœuds restent inchangés une fois le modèle supprimé.

Consultation de l'état de la protection et des informations de Kaspersky Embedded Systems Security

Pour lire les informations relatives à l'état de la protection du périphérique dans Kaspersky Embedded Systems Security,

Sélectionnez le nœud **Kaspersky Embedded Systems Security** dans l'arborescence de la Console de l'application.

Par défaut, les informations du panneau de détails de la console de l'application sont automatiquement actualisées :

- Toutes les 10 secondes en cas de connexion locale.
- Toutes les 15 secondes en cas de connexion distante.

Vous pouvez actualiser les informations manuellement.

*Pour actualiser manuellement les informations du nœud **Kaspersky Embedded Systems Security**,*

choisissez l'option **Actualiser** dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

Le panneau de détails de la console de l'application affiche les informations suivantes sur la console de l'application :

- État d'utilisation de Kaspersky Security Network.
- État de la protection de l'appareil.
- Données sur la mise à jour des bases de données et des modules de l'application.

- Données de diagnostic réel.
- Données relatives aux tâches de contrôle des périphériques protégés.
- Informations relatives à la licence.
- État de l'intégration à Kaspersky Security Center : données du serveur doté de Kaspersky Security Center auquel l'application est connectée ; informations sur les tâches de l'application contrôlées par la stratégie active.

Différentes couleurs sont utilisées pour indiquer l'état de la protection :

- *Vert*. La tâche est exécutée conformément aux paramètres définis. La protection est active.
- *Jaune*. La tâche n'a pas été lancée, a été suspendue ou est arrêtée. Des menaces pour la sécurité peuvent apparaître. Il est conseillé de lancer la tâche.
- *Rouge*. La tâche s'est soldée sur une erreur ou une menace pour la sécurité a été détectée pendant l'exécution de la tâche. Il est conseillé de lancer la tâche ou d'adopter les mesures d'élimination de la menace détectée.

Une partie des informations du groupe (par exemple, les noms des tâches ou le nombre de menaces détectées) se présente sous la forme de liens qui permettent d'accéder au nœud de la tâche correspondante ou d'ouvrir le journal d'exécution de la tâche.

La section **Utilisation du Kaspersky Security Network** indique l'état actuel de la tâche, par exemple, *Exécution en cours*, *Arrêtée* ou *Jamais exécutée*. L'indicateur peut prendre les valeurs suivantes :

- La couleur verte signifie que la tâche Utilisation du KSN est en cours d'exécution et les demandes de fichier pour les états sont envoyées à KSN.
- La couleur jaune signifie qu'une des déclarations est acceptée, mais que la tâche n'est pas en cours d'exécution ou qu'elle est en cours d'exécution, mais que les demandes de fichier ne sont pas envoyées à KSN.

Protection de l'ordinateur

La section **Protection de l'ordinateur** (cf. tableau ci-après) affiche les informations sur l'état actuel de la protection du périphérique.

Informations sur l'état de la protection du périphérique

Section Protection	Informations
Indicateur d'état de la protection de l'appareil	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes : • Verte : cette couleur s'affiche par défaut et indique que le composant Protection des fichiers en temps réel est installé et que la tâche est en cours d'exécution. • Jaune : le composant Protection des fichiers en temps réel n'est pas installé et la tâche Analyse rapide n'a pas été exécutée depuis longtemps. • Rouge : la tâche de protection des fichiers en temps réel n'est pas en cours d'exécution.
Protection des fichiers	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*).

en temps réel	**Détecté** : nombre d'objets détectés par Kaspersky Embedded Systems Security. Par exemple, si Kaspersky Embedded Systems Security a découvert une application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité. Si le nombre d'applications malveillantes détectées dépasse 0, la valeur est mise en évidence en rouge.
Analyse rapide	**Date de la dernière analyse** : date et heure de la dernière Analyse des zones critiques à la recherche de virus et autres menaces informatiques. *Jamais exécutée* : événement qui survient quand la tâche Analyse rapide a été effectuée il y a 30 jours ou plus (par défaut). Vous pouvez modifier le seuil de déclenchement de l'événement.
Protection contre les exploits	**État** : état actuel des techniques de protection contre les exploits, par exemple *Appliqué* ou *Pas appliquée*. **Mode de prévention** : un des deux modes à sélectionner lors de la configuration de la protection de la mémoire du processus : **Terminer en cas d'exploit** ou **Statistiques seulement**. **Processus protégés** : total des processus ajoutés à la zone de protection et traités selon le mode sélectionné.
Objets sauvegardés	*Dépassement du seuil d'espace disponible dans la sauvegarde* : cet événement se produit si la quantité d'espace disponible dans la Sauvegarde approche la limite indiquée. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en jaune. *Dépassement de la taille maximale de la sauvegarde* : cet événement se produit si la taille de la Sauvegarde a atteint la limite indiquée. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en rouge. **Objets sauvegardés** : nombre d'objets présents actuellement dans la Sauvegarde. **Espace utilisé** : volume d'espace occupé dans la Sauvegarde.

Mise à jour

La section **Mise à jour** (cf. tableau ci-dessous) affiche les informations sur l'actualité des bases antivirus et des modules de l'application.

Informations sur l'état des bases et des modules de Kaspersky Embedded Systems Security

Section Mise à jour	Informations
Témoin de l'état des bases et des modules de l'application	La couleur du panneau portant le nom de la section indique l'état des bases de l'application et des modules. L'indicateur peut prendre les valeurs suivantes : • Verte : cette couleur s'affiche par défaut et indique que les bases de l'application sont à jour et que la dernière tâche de mise à jour des bases de l'application a réussi. • Jaune : les bases de données sont dépassées ou la dernière tâche de mise à jour des bases de l'application a échoué. • Rouge : l'événement *Bases de l'application fortement dépassées* ou *Bases de l'application endommagées* s'est produit.
Mise à jour des bases de l'application et **Mise à jour des**	**État des bases de l'application** : évaluation de l'état de mise à jour des bases de l'application. Le paramètre peut prendre les valeurs suivantes :

modules de l'application	• **Bases de l'application à jour** : les bases de l'application ont été mises à jour il y a 7 jours maximum (par défaut). • **Bases de l'application dépassées** : les bases de l'application ont été mises à jour il y a 7 à 14 jours (par défaut). • **Bases de l'application fortement dépassées** : les bases de l'application ont été mises à jour il y a plus de 14 jours (par défaut). Vous pouvez modifier les seuils de déclenchement des événements *Bases de l'application à jour* et *Bases de l'application fortement dépassées*. **Date de publication des bases de l'application** : date et heure de la publication de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées en TU. **État de la tâche Mise à jour des bases de l'application la plus récente** : date et heure de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées selon l'heure locale de l'appareil protégé. Le champ est rouge si l'événement *Échec* s'est produit. **Des mises à jour des modules de l'application sont disponibles** : nombre de mises à jour des modules de Kaspersky Embedded Systems Security prêtes à être téléchargées et installées. **Mises à jour des modules de l'application installées** : nombre de mises à jour des modules de Kaspersky Embedded Systems Security installées.

Contrôle

La section **Contrôle** (cf. tableau ci-dessous) affiche les informations sur l'état des tâches Contrôle du lancement des applications, Contrôle des périphériques et Gestion du pare-feu.

Informations sur l'état du contrôle des périphériques protégés

Section Contrôle	Informations
Indicateur d'état pour le contrôle des périphériques protégés	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes : • Vert : cette couleur s'affiche par défaut et indique que le composant Contrôle du lancement des applications est installé et que la tâche s'exécute en mode **Actif**. • Jaune : le contrôle du lancement des applications est en cours d'exécution en mode **Statistiques seulement**. • Rouge : la tâche Contrôle du lancement des applications est à l'arrêt ou a échoué.
Contrôle du lancement des applications	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Mode de fonctionnement** : un des deux modes disponibles pour la tâche Contrôle du lancement des applications : **Actif** ou **Statistiques seulement**. **Lancements des applications bloqués** : nombre de tentatives de lancement d'applications bloquées par Kaspersky Embedded Systems Security au cours de l'exécution de la tâche Contrôle du lancement des applications. Si le nombre de lancements d'applications bloquées dépasse 0, le champ est rouge. **Durée de traitement moyenne (en ms)** : temps nécessaire à Kaspersky Embedded Systems Security pour le traitement des tentatives de lancement d'applications sur le périphérique protégé.

Contrôle des périphériques	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Mode de fonctionnement** : un des deux modes disponibles pour la tâche Contrôle des périphériques : **Actif** ou **Statistiques seulement** **Appareils bloqués** : nombre de tentatives de connexion à un périphérique externe bloquées par Kaspersky Embedded Systems Security au cours de l'exécution de la tâche Contrôle des périphériques. Si le nombre de périphériques externes bloqués dépasse 0, le champ est rouge.
Gestion du pare-feu	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Tentatives de connexion bloquées** : nombre de connexions à un appareil protégé qui ont été bloquées par les règles du pare-feu définies.

Diagnostic

La section **Diagnostic** (cf. tableau ci-après) affiche les informations relatives à l'état des tâches Moniteur d'intégrité des fichiers et Inspection des journaux.

Informations sur l'état du diagnostic du système

Section Diagnostic	Informations
Indicateur d'état du diagnostic	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans la section. L'indicateur peut prendre les valeurs suivantes : • Vert : cette couleur s'affiche par défaut et indique qu'un des composants de diagnostic du système ou les deux sont installés et que des tâches sont en cours d'exécution. • Jaune : les deux composants sont installés mais une des tâches de diagnostic du système n'est pas en cours d'exécution ; l'événement *A l'arrêt* se produit. • Rouge : une des tâches a échoué.
Moniteur d'intégrité des fichiers	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Opérations sur les fichiers non autorisées** : nombre de modifications dans les fichiers au sein de la zone de surveillance. Ces modifications peuvent signaler une violation de la sécurité d'un appareil protégé.
Inspection des journaux	**État de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Arrêtée*). **Violations des règles configurées** : nombre de violations enregistrées d'après les données du journal des événements Windows. Ce nombre est déterminé sur la base des règles définies de la tâche ou via l'analyseur heuristique

Les informations relatives à la licence de Kaspersky Embedded Systems Security sont affichées sur la ligne du coin inférieur gauche du panneau de détails du nœud **Kaspersky Embedded Systems Security**.

Vous pouvez configurer les propriétés de Kaspersky Embedded Systems Security en suivant le lien **Propriétés de l'application**.

Vous pouvez vous connecter à un autre périphérique protégé en suivant le lien **Se connecter à un autre ordinateur**.

Utilisation du Plug-in Web depuis Web Console et Cloud Console

Cette section fournit des informations sur le plug-in Kaspersky Embedded Systems Security et décrit la procédure d'administration de l'application installée sur un périphérique protégé ou sur un groupe de périphériques protégés.

Gestion de Kaspersky Embedded Systems Security à partir de Web Console ou de Cloud Console

Vous pouvez gérer de manière centralisée plusieurs périphériques protégés dotés de Kaspersky Embedded Systems Security et inclus dans un groupe d'administration au moyen du Web Plug-in de Kaspersky Embedded Systems Security. Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console vous permettent également de configurer séparément chaque périphérique protégé dans le groupe d'administration.

Un *groupe d'administration* est créé manuellement Kaspersky Security Center Web Console. Le groupe contient plusieurs appareils dotés de Kaspersky Embedded Systems Security pour lesquels vous souhaitez configurer des paramètres de contrôle et de protection identiques. Pour en savoir plus sur l'utilisation de groupes d'administration, consultez *l'aide de Kaspersky Security Center*.

Les paramètres de l'application pour un seul périphérique protégé ne peuvent être configurés si le fonctionnement de Kaspersky Embedded Systems Security sur ce périphérique protégé est contrôlé par une stratégie active de Kaspersky Security Center.

Vous pouvez choisir une des méthodes suivantes pour administrer Kaspersky Embedded Systems Security Web Console depuis Kaspersky Security Center :

- **A l'aide de stratégies de Kaspersky Security Center**. Les stratégies de Kaspersky Security Center permettent de configurer à distance des paramètres de protection uniques pour un groupe d'appareils. Les paramètres de la tâche, définis dans la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la Console de l'application ou à distance dans la fenêtre des propriétés du périphérique dans Kaspersky Security Center Web Console. Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches Protection en temps réel de l'ordinateur, Contrôle de l'activité locale et les paramètres du lancement des tâches locales planifiées du système.

- **A l'aide de tâches de groupe de Kaspersky Security Center**. Les tâches de groupe de Kaspersky Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai d'exécution limité pour un groupe d'appareils. Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche de Génération des règles du Contrôle du lancement des applications.

- **A l'aide de tâches pour une sélection de périphériques**. Les tâches pour une sélection de périphériques permettent de configurer à distance des paramètres de tâches communs ayant un délai d'exécution limité pour les appareil protégés qui ne figurent dans aucun groupe d'administration.

- **A l'aide de la fenêtre de configuration des paramètres d'un périphérique**. La fenêtre des propriétés du périphérique permet de configurer à distance les paramètres d'une tâche pour un appareil protégé unique appartenant à un groupe d'administration. Vous pouvez également configurer ainsi les paramètres généraux de fonctionnement de l'application et les paramètres de toutes les tâches de Kaspersky Embedded Systems Security si le périphérique protégé sélectionné n'est pas contrôlé par une stratégie active de Kaspersky Security Center.

Kaspersky Security Center Web Console et Kaspersky Security Center Cloud Console permettent de configurer les paramètres de l'application ainsi que les possibilités additionnelles. Elles donnent également accès aux journaux et notifications. Vous pouvez configurer ces paramètres aussi bien pour un groupe de périphériques protégés que pour des périphériques protégés individuels.

Limitations du Plug-in Web

Le plug-in Web de Kaspersky Embedded Systems Security présente les limitations suivantes par rapport au plug-in Kaspersky Embedded Systems Security :

- Pour ajouter des utilisateurs ou des groupes d'utilisateur, vous devez spécifier la chaîne de descripteur de sécurité à l'aide de la syntaxe SDDL.
- Le niveau de sécurité prédéfini ne peut pas être modifié pour la tâche de protection des fichiers en temps réel.
- Les règles de tâche Contrôle du lancement des applications ne peuvent pas être créées à l'aide d'un certificat numérique ou d'événements Kaspersky Security Center.
- Les règles de la tâche Contrôle des périphériques ne peuvent pas être générées en fonction des périphériques connectés ou des données système.

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Embedded Systems Security dans Kaspersky Security Center Web Console.

Configuration des paramètres généraux de l'application dans le Plug-in Web

Vous pouvez configurer les paramètres généraux de Kaspersky Embedded Systems Security dans Web Plug-in pour un groupe de périphériques protégés ou pour un périphérique protégé individuel.

Configuration de l'optimisation, de l'interface et de l'analyse dans Web Plug-in

Pour configurer les paramètres d'optimisation et l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configuration** dans la sous-section **Extensibilité, interface et paramètres d'analyse**.

6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de montée en puissance

Paramètre	Description
Détecter automatiquement les paramètres de montée en puissance	Kaspersky Embedded Systems Security contrôle automatiquement le nombre de processus utilisés. Cette valeur est définie par défaut.
Indiquer manuellement le nombre de processus actifs	Kaspersky Embedded Systems Security contrôle le nombre de processus de travail actifs en fonction des valeurs indiquées.
Nombre de processus de protection en temps réel	Nombre maximum de processus utilisés par les composants de tâche de protection en temps réel de l'ordinateur. Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.
Nombre de processus pour les tâches d'analyse à la demande en arrière-plan	Nombre maximum de processus utilisés par le module d'analyse à la demande quand cette analyse est réalisée en arrière-plan. Le champ de saisie est accessible si l'option **Indiquer manuellement le nombre de processus actifs** a été sélectionnée.
Afficher l'icône de la barre d'état dans la barre des tâches	Indique si l'icône de la barre d'état système sera affichée dans la zone de notification.
Restaurer les attributs du fichier après l'analyse	Lorsque Kaspersky Embedded Systems Security exécute des tâches d'analyse à la demande, l'heure du dernier accès à chaque fichier analysé est mise à jour. Après l'analyse, Kaspersky Embedded Systems Security rétablit la valeur initiale de l'heure du dernier accès au fichier. Ce comportement peut affecter le fonctionnement des systèmes de sauvegarde, car il provoque la création de copies de sauvegarde pour des fichiers qui n'ont pas été modifiés. Il peut également provoquer de fausses détections dans les applications de suivi des modifications de fichiers. L'option est activée par défaut.
Limiter l'utilisation du processeur pour les threads d'analyse	Kaspersky Embedded Systems Security n'utilise jamais le processeur de l'appareil protégé dans les tâches d'analyse à la demande au-delà de la valeur du champ **Limite supérieure (pour cent)**. L'activation de cette option peut avoir une incidence négative sur les performances de Kaspersky Embedded Systems Security. Cette option est désactivée par défaut.
Limite supérieure (en pourcentage)	Valeur maximale autorisée pour l'utilisation du processeur par Kaspersky Embedded Systems Security. Le champ de saisie est disponible si l'option **Limiter l'utilisation du processeur pour les threads d'analyse** est sélectionnée.
Dossier pour les fichiers temporaires créés	Dossier dans lequel Kaspersky Embedded Systems Security doit décompresser l'archive lors de l'analyse. Il s'agit par défaut du dossier C:\Windows\Temp.

pendant l'analyse	
paramètres du système HSM	Sélectionnez l'option pour accéder au stockage hiérarchique.

Configuration des paramètres de sécurité dans le Plug-in Web

Pour configurer les paramètres de sécurité manuellement, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configuration** dans la sous-section **Sécurité et fiabilité**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de sécurité

Paramètre	Description
Protection des processus de l'application contre les menaces externes	Si la case **Protection des processus de l'application contre les menaces externes** est cochée, l'application protège ses processus contre l'injection de code ou l'accès aux données de processus. Lors de l'activation ou de la désactivation de l'option, il n'est pas nécessaire de redémarrer les services d'application pour appliquer la modification. Cette option est activée par défaut.
Réaliser la restauration des tâches	La case active ou désactive la restauration des tâches de Kaspersky Embedded Systems Security après un échec de l'application ou un arrêt forcé de celle-ci. Si la case est cochée, Kaspersky Embedded Systems Security restaure automatiquement ses tâches après un échec de l'application ou un arrêt forcé de celle-ci. Si la case est décochée, Kaspersky Embedded Systems Security ne restaure pas ses tâches après un échec de l'application ou un arrêt forcé de celle-ci. Cette case est cochée par défaut.
Ne pas réaliser la restauration des tâches d'analyse à la demande plus de (fois) dans une plage de 1 à 10 tentatives	Nombre de tentatives de restauration des tâches d'analyse à la demande après un échec de Kaspersky Embedded Systems Security. Le champ de saisie est accessible si la case **Réaliser la restauration des tâches** a été cochée.
Ne pas lancer les tâches d'analyse programmée	Cette case active ou désactive le lancement d'une tâche d'analyse programmée entre l'entrée en action de l'alimentation de secours de l'appareil protégé et le rétablissement de l'alimentation normale.

	Si la case est cochée, Kaspersky Embedded Systems Security ne lance pas les tâches d'analyse programmée entre l'entrée en action de l'alimentation de secours du périphérique protégé et le rétablissement de l'alimentation standard. Si la case est décochée, Kaspersky Embedded Systems Security lance les tâches d'analyse programmée quelle que soit la source d'alimentation employée. Cette case est cochée par défaut.
Arrêter les tâches d'analyse en cours	La case active ou désactive la suspension des tâches d'analyse en cours d'exécution lors du passage du périphérique protégé à une source d'alimentation de secours. Si la case est cochée, Kaspersky Embedded Systems Security arrête l'exécution des tâches d'analyse en cours lors du passage du périphérique protégé à une source d'alimentation de secours. Si la case est décochée, Kaspersky Embedded Systems Security poursuit l'exécution des tâches d'analyse en cours après que le périphérique protégé est passé à une source d'alimentation de secours. Cette case est cochée par défaut.
Utiliser la protection par mot de passe	Définit u nmot de passe pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security.

Configuration des paramètres de connexion dans le Plug-in Web

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Embedded Systems Security et les serveurs de mise à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services KSN.

Pour configurer les paramètres de la connexion, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configuration** dans la sous-section **Extensibilité, interface et paramètres d'analyse**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de connexion

Paramètre	Description
Ne pas utiliser de serveur proxy	Si cette option est sélectionnée, Kaspersky Embedded Systems Security n'utilise pas le serveur proxy pour la connexion aux services du KSN et effectue la connexion directement.
Utiliser les paramètres du serveur proxy indiqué	Si cette option est sélectionnée, Kaspersky Embedded Systems Security utilise les paramètres du serveur proxy indiqués manuellement pour la connexion au KSN.

Ne pas utiliser le serveur proxy pour les adresses locales	La case active ou désactive l'utilisation du serveur proxy lors des échanges avec les autres périphériques du réseau auquel appartient le périphérique protégé disposant de Kaspersky Embedded Systems Security. Si la case est cochée, les échanges avec les autres périphériques du réseau auquel appartient le périphérique protégé disposant de Kaspersky Embedded Systems Security se font directement. Le serveur proxy n'est pas utilisé. Si la case est décochée, les appareils locaux sont sollicités via un serveur proxy. Cette case est cochée par défaut.
Paramètres d'authentification du serveur proxy	Spécifiez les paramètres d'authentification
Ne pas utiliser l'authentification	L'authentification n'a pas lieu. Ce mode est sélectionné par défaut.
Utiliser l'authentification NTLM	Authentification à l'aide du protocole d'authentification réseau NTLM, développé par Microsoft.
Utiliser l'authentification NTLM avec nom d'utilisateur et mot de passe	L'authentification est effectuée avec un nom d'utilisateur et un mot de passe à l'aide du protocole d'authentification réseau NTLM développé par Microsoft.
Utiliser le nom d'utilisateur et le mot de passe	L'authentification est effectuée à l'aide du nom d'utilisateur et du mot de passe.

Configuration du lancement planifié des tâches locales du système prédéfinies

Vous pouvez utiliser des stratégies pour autoriser ou interdire le lancement de la tâche locale du système d'analyse à la demande et de la tâche de mise à jour. Cela s'opère selon la planification configurée localement sur chaque périphérique protégé du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'appareil protégé selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.
- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Le lancement des tâches locales du système est interdit par défaut par la stratégie.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont administrées via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de mise à jour de groupe ou d'analyse à la demande, autorisez le lancement des tâches locales du système dans la stratégie : Kaspersky Embedded Systems Security réalise la mise à jour des bases de l'application et des modules et lance également toutes les tâches locales du système d'analyse à la demande conformément à la programmation par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâche d'analyse à la demande définie : Analyse rapide, Analyse de la quarantaine, Analyse au démarrage du système d'exploitation et Vérification de l'intégrité de l'application, Surveillance de l'intégrité des fichiers.
- Tâches de mise à jour : Mise à jour des bases de l'application, Mise à jour des modules de l'application, Copie des mises à jour.

Si vous excluez l'appareil protégé du groupe d'administration, la planification des tâches locales du système sera automatiquement activée.

Pour autoriser ou interdire le lancement planifié des tâches locales du système de Kaspersky Embedded Systems Security dans une stratégie :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configuration** dans la sous-section **Lancer les tâches locales du système**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de lancement planifié des tâches locales du système

Paramètre	Description
Autoriser le lancement des tâches d'analyse à la demande	Cochez ou décochez la case pour autoriser ou interdire le lancement planifié des tâches d'analyse à la demande.
Autoriser l'exécution des tâches de mise à jour et de copie des mises à jour	Cochez ou décochez la case pour autoriser ou interdire le lancement planifié des tâches de mise à jour et de la tâche de copie de la mise à jour.

Configuration des paramètres de la quarantaine et de sauvegarde dans le Plug-in Web

Pour configurer les paramètres généraux de la quarantaine et de la sauvegarde dans Kaspersky Security Center :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Complémentaire**.

5. Cliquez sur **Configuration** dans la sous-section **Stockages**.

6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la Quarantaine et de la Sauvegarde

Paramètre	Description
Dossier de sauvegarde	Désignez le dossier de sauvegarde.
Taille maximale de sauvegarde (Mo)	Définissez la taille maximale de la Sauvegarde.
Seuil d'espace disponible (Mo)	Spécifiez la valeur minimale de l'espace libre dans le dossier de Sauvegarde.
Dossier cible pour la restauration des objets	Spécifiez un dossier pour les objets restaurés.
Dossier de quarantaine	Désignez le dossier de sauvegarde.
Taille maximale de la quarantaine (Mo)	Définissez la taille maximale de la Sauvegarde.
Seuil d'espace disponible (Mo)	Spécifiez la valeur minimale de l'espace libre dans le dossier de Sauvegarde.
Dossier cible pour la restauration des objets	Spécifiez un dossier pour les objets restaurés.
Condition de blocage des sessions réseau	Indiquez le nombre de jours, d'heures et de minutes au terme desquels les sessions réseau bloquées ont à nouveau accès aux ressources de fichier réseau.

Création et configuration des stratégies

Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Embedded Systems Security sur plusieurs périphériques protégés.

Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs périphériques sur lesquels Kaspersky Embedded Systems Security est installé.

Une stratégie applique les paramètres indiqués de Kaspersky Embedded Systems Security ainsi que ses fonctions et ses tâches à l'ensemble des périphériques protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la Console d'administration, la stratégie active dans le groupe en ce moment possède l'état *actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Embedded Systems Security. Vous pouvez les consulter dans la console de l'application dans le nœud **Journal d'audit système**.

Kaspersky Security Center offre une méthode pour appliquer les stratégies aux appareils protégés : *interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Embedded Systems Security applique aux périphériques protégés les paramètres pour lesquels vous avez sélectionné l'icône dans les propriétés de la stratégie. Dans ce cas, les paramètres sélectionnés sont utilisés à la place des paramètres en vigueur avant l'application de la stratégie. Les paramètres de la stratégie active accompagnés de l'icône dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Embedded Systems Security.

Si une stratégie est active, les paramètres dans la Console de l'application qui sont accompagnés de l'icône dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres (accompagnés de l'icône dans la stratégie) peuvent être modifiées dans la console de l'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône empêchent également la modification des paramètres dans Kaspersky Security Center pour un appareil protégé depuis la fenêtre **Propriétés : <Nom de l'appareil protégé>**.

Les paramètres configurés et transmis à l'appareil protégé à l'aide de la stratégie active sont enregistrés dans les paramètres de tâche locale après la désactivation de la stratégie active.

Si la stratégie définit les paramètres d'une tâche quelconque de protection en temps réel de l'ordinateur et si cette tâche est en exécution, les paramètres définis par la stratégie sont modifiés directement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

Création d'une stratégie

Pour créer une stratégie :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur **Ajouter**.
3. La fenêtre **Nouvelle stratégie** s'ouvre.
4. Dans la section **Sélectionner une application**, sélectionnez Kaspersky Embedded Systems Security, puis cliquez sur **Suivant**.
5. L'onglet **Général** permet de réaliser les opérations suivantes :
   - Modifiez le nom de la stratégie.

     Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ |` .
   - Sélectionnez l'état de la stratégie :
     - **Actif**. Après la synchronisation suivante, la stratégie est utilisée comme stratégie active sur l'ordinateur.
     - **Inactive**. Stratégie de sauvegarde. Si nécessaire, une stratégie inactive peut être permutée en stratégie active.
     - **Hors du bureau**. La stratégie est activée lorsqu'un ordinateur quitte le périmètre du réseau de l'organisation.

- Configurez l'héritage des paramètres :

  - **Hériter des paramètres de la stratégie parent**. Si ce bouton bascule est activé, les valeurs des paramètres de la stratégie sont héritées de la stratégie de niveau supérieur. Les paramètres de la stratégie ne peuvent pas être modifiés si est défini pour la stratégie parent.

  - **Forcer l'héritage des paramètres dans les stratégies enfants**. Si le bouton bascule est activé, les valeurs des paramètres de la stratégie sont propagées aux stratégies enfants. Dans les paramètres de stratégie enfant, la case **Hériter des paramètres de la stratégie parent** est automatiquement activée. Les paramètres de stratégie enfant sont hérités de la stratégie parent, à l'exception des paramètres accompagnés de . Les paramètres de stratégie enfant ne peuvent pas être modifiés si est défini pour la stratégie parent.

6. Dans l'onglet **Paramètres de l'application**, configurez les paramètres de la stratégie selon vos besoins.

7. Cliquez sur **Enregistrer**.

La **stratégie créée** sera affichée dans la liste des stratégies sous l'onglet **Stratégies et profils** du groupe d'administration sélectionné. La fenêtre **<Nom de la stratégie>** permet de configurer d'autres paramètres, tâches et fonctions de Kaspersky Embedded Systems Security.

Une fois que vous avez créé une stratégie, un ensemble de règles d'autorisation est créé pour empêcher le blocage des applications et garantir leur fonctionnement continu. Les règles par défaut figurent dans les paramètres de la tâche. Voici les détails et les limites.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau entrant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le processus Partage du bureau Windows de l'Agent d'administration de Kaspersky Security Center, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

- Deux règles d'autorisation pour le port local 15000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau sortant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour Kaspersky Embedded Systems Security Service, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

- Deux règles d'autorisation pour le processus de flux de travail de Kaspersky Embedded Systems Security, dans %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

- Deux règles d'autorisation pour le port local 13000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Sections contenant les paramètres de stratégie de Kaspersky Embedded Systems Security

Général

La section **Général** permet de configurer les paramètres de stratégie suivants :

- Indiquez l'état de la stratégie.
- Configurez l'héritage des paramètres des stratégies parent pour les stratégies fille.

Configuration d'événement

La section **Configuration d'événement** permet de configurer les paramètres pour les catégories d'événements suivants :

- *Événements critiques*
- *Panne de fonction*
- *Avertissement*
- *Message d'information*

Le bouton **Propriétés** permet de configurer les paramètres suivants pour les événements sélectionnés :

- Définissez l'emplacement et la durée de conservation des informations sur l'événement enregistré ;
- Indiquez la méthode de notification pour les événements consignés.

Paramètres de l'application

Paramètres de la section Paramètres de l'application

Section	Options
Extensibilité, interface et paramètres d'analyse	Le bouton **Configuration** de la sous-section **Extensibilité, interface et paramètres d'analyse** permet de configurer les paramètres suivants : • choisir la configuration automatique ou manuelle des paramètres de montée en puissance. • configurer l'affichage de l'icône de l'application.
Sécurité et fiabilité	Le bouton **Configuration** de la sous-section **Sécurité et fiabilité** permet de configurer les paramètres suivants : • Configurez les paramètres de lancement de la tâche. • Actions de l'application en cas de passage à l'alimentation de l'appareil protégé via un onduleur. • Activation ou désactivation de la protection par mot de passe des fonctions de l'application.
Connexions	Le bouton **Configuration** de la sous-section **Connexions** permet de configurer les paramètres suivants du serveur proxy pour la connexion aux serveurs de mise à jour, aux serveurs d'activation et à KSN :

	• définition des paramètres du serveur proxy. • définition des paramètres d'authentification sur le serveur proxy.
Lancer les tâches locales du système	Le bouton **Configuration** de la sous-section **Lancer les tâches locales du système** permet d'interdire ou d'autoriser le lancement des tâches système planifiées suivantes, configurées sur les appareils protégés : • Tâche Analyse à la demande. • Tâches de mise à jour et tâche de copie des mises à jour.

Complémentaire

Paramètres de la section Complémentaire

Section	Options
Zone de confiance	Le bouton **Configuration** de la sous-section **Zone de confiance** permet de configurer les paramètres suivants d'application d'une zone de confiance : • Composer la liste des exclusions de la zone de confiance. • Activer ou désactiver l'analyse des opérations de sauvegarde des fichiers. • Composer une liste des processus de confiance.
Analyse des disques amovibles	La section **Analyse des disques amovibles** contient le bouton **Configuration** qui permet de configurer les paramètres d'analyse des disques amovibles.
Autorisations d'accès de l'utilisateur pour l'administration de l'application	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** permet de configurer les paramètres des droits des utilisateurs et des groupes d'utilisateurs à l'administration de Kaspersky Embedded Systems Security.
Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security	La sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** permet de configurer les droits des utilisateurs et des groupes d'utilisateurs à l'administration du service Kaspersky Security.
Stockages	Dans la sous-section **Stockages**, cliquez sur le bouton **Configuration** pour configurer les paramètres suivants de la quarantaine, de la Sauvegarde et de la liste des ordinateurs douteux : • chemin d'accès du dossier dans lequel vous souhaitez placer les objets en quarantaine ou dans la sauvegarde ; • taille maximale de la Sauvegarde ou de la quarantaine et seuil d'espace disponible ; • dossier où seront placés les objets restaurés depuis la sauvegarde ou la quarantaine ; • transmission au Serveur d'administration des informations relatives aux objets dans la sauvegarde ou la quarantaine. • Configurez la durée de blocage des hôtes.

Protection en temps réel de l'ordinateur

Paramètres de la section Protection en temps réel du serveur

Section	Options
Protection des fichiers en temps réel	Le bouton **Configuration** de la sous-section **Protection des fichiers en temps réel** permet de configurer les paramètres suivants d'exécution de la tâche : • Indiquez le mode de protection. • Configurez l'utilisation de l'analyse heuristique. • Configurez l'application de la Zone de confiance. • composition de la zone de protection ; • niveau de sécurité de la zone de protection sélectionnée : vous pouvez sélectionner un niveau de sécurité prédéfini ou configurer manuellement les paramètres de sécurité ; • Configurez les paramètres de lancement de la tâche.
Utilisation du KSN	Le bouton **Configuration** de la sous-section **Utilisation du KSN** permet de configurer les paramètres suivants d'exécution de la tâche : • actions à réaliser sur les objets considérés comme douteux par KSN ; • Configurez le transfert de données et l'utilisation de Kaspersky Security Center en tant que serveur proxy du KSN.
Protection contre les exploits	Le bouton **Configuration** de la sous-section **Protection contre les exploits** permet de configurer les paramètres suivants d'exécution de la tâche : • sélection du mode de protection de la mémoire du processus ; • définition de l'action de réduction de l'impact de l'exploitation des vulnérabilités ; • enrichissement et modification de la liste des processus à protéger.

Contrôle de l'activité locale

Paramètres de la section Contrôle de l'activité locale

Section	Options
Contrôle du lancement des applications	Le bouton **Configuration** de la sous-section **Contrôle du lancement des applications** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • configuration des paramètres du contrôle du nouveau lancement des applications ;

	• Indiquez la zone d'application des règles du contrôle du lancement des applications. • configuration de l'utilisation du KSN ; • Configurez les paramètres de lancement de la tâche.
Contrôle des périphériques	Le bouton **Configuration** de la sous-section **Contrôle des périphériques** permet de configurer les paramètres suivants d'exécution de la tâche : • Sélectionnez le mode de fonctionnement de la tâche. • Configurez les paramètres de lancement de la tâche.

Contrôle de l'activité réseau

Paramètres de la section Contrôle de l'activité réseau

Section	Options
Gestion du pare-feu	Le bouton **Configuration** de la sous-section **Gestion du pare-feu** permet de configurer les paramètres suivants d'exécution de la tâche : • règles du pare-feu ; • Configurez les paramètres de lancement de la tâche.

Diagnostic du système

Paramètres de la section Diagnostic du système

Section	Options
Moniteur d'intégrité des fichiers	La sous-section **Moniteur d'intégrité des fichiers** permet de configurer le contrôle sur les modifications dans les fichiers qui peuvent indiquer un cas d'atteinte à la sécurité sur un périphérique protégé.
Inspection des journaux	La section **Inspection des journaux** permet de configurer le contrôle de l'intégrité d'un périphérique protégé sur la base des résultats de l'analyse du journal des événements Windows.

Journaux et notifications

Paramètres de la section Journaux et notifications

Section	Options
Journaux d'exécution de la tâche	Le bouton **Configuration** de la sous-section **Journaux d'exécution de la tâche** permet de configurer les paramètres suivants : • Définition du niveau d'importance des événements enregistrés pour les composants de l'application sélectionnés ; • Définition des paramètres de conservation des journaux d'exécution de la tâche.

	• Spécifiez l'intégration de SIEM avec les paramètres de Kaspersky Security Center.
Notifications sur les événements	Le bouton **Configuration** de la sous-section **Notifications sur les événements** permet de configurer les paramètres suivants : • Définissez les paramètres de notification des utilisateurs pour l'événement Objet détecté ; pour les événements *Objet détecté*, *Stockage de masse douteux détecté et restreint* et *Ordinateur ajouté à la liste des ordinateurs douteux*. • paramètres de notification de l'administrateur pour n'importe quel événement sélectionné dans la liste des événements de la section **Configuration des notifications**.
Interaction avec le serveur d'administration	Le bouton **Configuration** de la section **Interaction avec le serveur d'administration** permet de choisir les types d'objets que Kaspersky Embedded Systems Security va signaler au Serveur d'administration.

Historique des révisions

La section **Historique des révisions** permet d'administrer les révisions : comparer à la révision actuelle ou à une autre stratégie, ajouter des descriptions de révisions, enregistrer les révisions dans un fichier ou revenir à l'état antérieur à la révision.

Création et configuration de tâches via Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Embedded Systems Security, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

À propos de la création de tâches dans le Plug-in Web

Vous pouvez créer des tâches de groupe pour des groupes d'administration et pour des sélections d'appareils protégés. Les types de tâches suivants peuvent être créés :

- Activation de l'application
- Copie des mises à jour
- Mise à jour des bases de l'application
- Mise à jour des modules de l'application
- Annulation de la mise à jour des bases de l'application
- Analyse à la demande
- Vérification de l'intégrité de l'application
- Surveillance de l'intégrité des fichiers
- Génération des règles du Contrôle du lancement des applications

- Générateur de règles pour le Contrôle des périphériques

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- Pour un appareil protégé : dans la fenêtre **Propriétés <nom de l'appareil protégé>** dans la section **Tâches**.
- Pour un groupe d'administration : dans le panneau de détails du nœud du groupe d'appareils protégés sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'appareils protégés : dans le panneau de détails du nœud **Sélection de périphériques**.

Les stratégies permettent de désactiver les planifications pour la mise à jour et les tâches système locale d'analyse à la demande sur tous les appareils protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

Création d'une tâche dans le Plug-in Web

Pour créer une tâche dans la console d'administration de Kaspersky Security Center, procédez comme suit :

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :
   - Pour créer une tâche locale :
     a. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique → Périphériques administrés**.
     b. Cliquez sur l'onglet **Groupes** pour sélectionner le groupe d'administration auquel appartient l'appareil protégé.
     c. Cliquez sur le nom de l'appareil protégé.
     d. Dans la fenêtre **<nom du périphérique>** qui s'ouvre, sélectionnez l'onglet **Tâches**.
     e. Cliquez sur **Ajouter**.
   - Pour créer une tâche de groupe :
     a. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique → Périphériques administrés**.
     b. Cliquez sur l'onglet **Groupes** pour sélectionner le groupe d'administration pour lequel vous souhaitez créer une tâche.
     c. Cliquez sur **Ajouter**.
   - Pour créer une tâche pour un ensemble d'appareils protégés défini par l'utilisateur :
     a. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique → Sélections de périphériques**.
     b. Sélectionnez la sélection pour laquelle vous souhaitez créer une tâche.
     c. Cliquez sur **Démarrer**.

d. Dans la fenêtre **Résultats de la sélection**, sélectionnez les périphériques pour lesquels vous souhaitez créer une tâche.

e. Cliquez sur **Nouvelle tâche**.

La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.

3. Dans la liste déroulante **Type de tâche**, sélectionnez le type de la tâche à créer.

   Si vous avez choisi n'importe quel type de tâche, sauf Annulation de la mise à jour des bases de l'application, Vérification de l'intégrité de l'application ou Activation de l'application, la fenêtre Configuration s'ouvre.

4. En fonction du type de tâche sélectionné, réalisez une des opérations suivantes :

   - Création d'une tâche d'analyse à la demande.

   - Si vous créez une des tâches de mise à jour, définissez les paramètres de la tâche conformément à vos exigences :

     a. Sélectionnez la source de mise à jour dans la section **Source de mise à jour des bases de l'application**.

     b. Configurez les paramètres du serveur proxy dans la fenêtre **Paramètres de connexion**.

   - Après avoir créé une tâche Mise à jour des modules de l'application, configurez les paramètres requis de la mise à jour des modules de l'application dans la fenêtre **Mise à jour des modules de l'application** :

     a. Décidez si vous souhaitez copier et installer les mises à jour critiques des modules de l'application ou uniquement vérifier si elles sont disponibles sans installation.

     b. Si vous avez choisi **Copier et installer les mises à jour critiques des modules de l'application**, le redémarrage de l'appareil protégé peut être requis pour terminer l'installation des modules de l'application. Pour que Kaspersky Embedded Systems Security relance automatiquement le périphérique protégé après la fin de la tâche, cochez la case **Autoriser le redémarrage du système d'exploitation**.

     c. Si vous souhaitez obtenir des informations sur la diffusion des mises à jour des modules de Kaspersky Embedded Systems Security, cochez la case **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

     Kaspersky ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky. Il est possible de configurer une notification pour l'administrateur au sujet de l'événement **Nouvelle mise à jour prévue des modules de l'application disponible**. Cette notification reprend l'adresse Internet de notre site depuis lequel il est possible de télécharger les mises à jour planifiées.

   - Pour créer la tâche Copie des mises à jour, indiquez, dans la fenêtre **Copie des mises à jour**, la composition des mises à jour et le dossier de destination.

   - Pour créer la tâche d'Activation de l'application, procédez comme suit :

     a. Dans la fenêtre de **Liste des clés dans le stockage de Kaspersky Security Center**, indiquez le fichier clé que vous souhaitez utiliser pour activer l'application.

     b. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez créer une tâche pour renouveler la licence.

- Créez et configurez la tâche Génération des règles du Contrôle du lancement des applications et configurer ses paramètres, procédez comme suit :
- Créez et configurez la tâche Générateur de règles pour le Contrôle des périphériques.

5. Cliquez sur **Suivant**.
6. Si la tâche est créée pour une sélection d'appareils protégés, sélectionnez le réseau (ou le groupe) d'appareils protégés sur lesquels elle sera exécutée.
7. Cliquez sur **Suivant**.
8. Dans la fenêtre **Fin de la création**, cochez la case **Ouvrir les détails de la tâche à la fin de la création** si vous souhaitez configurer les paramètres de la tâche.
9. Cliquez sur le bouton **Terminer**.

La tâche créée apparaît dans la liste **Tâches**.

Configuration des tâches de groupe dans le Plug-in Web

Pour configurer une tâche de groupe pour plusieurs appareils protégés, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.
   La fenêtre **<Nom de la tâche>** s'ouvre.
3. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
   - Si vous configurez une tâche d'analyse à la demande :
     a. Dans la section **Zone d'analyse**, créez une zone d'analyse.
     b. Dans la section **Options**, configurez l'intégration aux autres modules de l'application et le niveau de priorité de la tâche.
   - Si vous configurez l'une des tâches de mise à jour, définissez les paramètres de la tâche en fonction de vos besoins :
     a. Dans la section **Sources des mises à jour**, configurez les paramètres de la source des mises à jour et du serveur proxy.
     b. Dans la section **Optimisation**, configurez l'optimisation du sous-système de disque.
   - Pour configurer la tâche Mise à jour des modules de l'application, sélectionnez dans la section **Paramètres avancés** une action à effectuer : copier et installer les mises à jour critiques des modules de l'application ou simplement les rechercher.
   - Pour configurer la tâche Copie des mises à jour, indiquez, dans la section **Paramètres de copie des mises à jour**, la composition des mises à jour et le dossier de destination.
   - Pour configurer la tâche Activation de l'application, appliquez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter un code d'activation ou un fichier clé pour renouveler la licence.

- Pour configurer la génération automatique des règles d'autorisation pour le Contrôle des périphériques, définissez les valeurs qui seront utilisées pour créer la liste des règles d'autorisation.

4. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

5. Dans la section **Compte** de l'onglet **Configuration**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le *Système d'aide de Kaspersky Security Center*.

6. Cliquez sur **Enregistrer**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Configuration de la tâche Activation de l'application dans le Plug-in Web

Pour configurer la tâche d'Activation de l'application, procédez comme suit :

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

2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.

3. Dans la section **Général**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser en tant que clé additionnelle** si vous souhaitez ajouter une clé pour renouveler la licence.

4. Configurez la planification des tâches dans la section **Planification**.

5. Dans la fenêtre **<Nom de la tâche>**, cliquez sur le bouton **OK**.

Configuration des tâches de mise à jour dans le Plug-in Web

Pour configurer la tâche Copie des mises à jour, Mise à jour des bases de l'application ou Mise à jour des modules de l'application, procédez comme suit :

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

2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.

3. Dans la section **Sources des mises à jour**, configurez les paramètres de la source des mises à jour :

   - Dans la section **Source de mise à jour des bases de l'application**, indiquez le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.

     Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

Pour utiliser un dossier SMB partagé comme source de mise à jour, vous devez renseigner un compte utilisateur pour démarrer une tâche.

Lors de la configuration d'une tâche de mise à jour via Cloud Console, seuls les paramètres **Points de distribution** et **Serveurs de mise à jour de Kaspersky** sont disponibles pour spécifier la source des mises à jour.

- Dans la section **Paramètres de connexion**, configurez l'utilisation d'un serveur proxy pour la connexion aux serveurs de mise à jour de Kaspersky et à d'autres serveurs.

4. La section **Optimisation** permet de configurer les paramètres de la fonction réduisant la charge sur le sous-système disque pour la tâche Mise à jour des bases de l'application :
   - **Optimisation de l'utilisation des I/O du disque**
   - **RAM utilisée pour l'optimisation (400 à 9 999 Mo)**
5. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
6. Dans la fenêtre **<Nom de la tâche>**, cliquez sur le bouton **OK**.

Configuration des paramètres de diagnostic des échecs dans le plug-in Web

Quand un problème survient pendant le fonctionnement de Kaspersky Embedded Systems Security (par exemple, Kaspersky Embedded Systems Security se bloque), vous pouvez le diagnostiquer. Pour ce faire, vous pouvez activer la création de fichiers de traçage et d'un fichier dump pour le processus de Kaspersky Embedded Systems Security et envoyer ces fichiers pour analyse au Support Technique de Kaspersky.

Kaspersky Embedded Systems Security n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par un utilisateur doté des autorisations adéquates.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Embedded Systems Security. Vous pouvez configurer les autorisations d'accès et permettre l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs qui en ont besoin.

Pour configurer les paramètres de Diagnostic des échecs dans Kaspersky Security Center :

1. Dans la console d'administration de Kaspersky Security Center, ouvrez la fenêtre **Paramètres de l'application**.
2. Ouvrez la section **Diagnostic des échecs**.
3. Si vous souhaitez que l'application consigne les informations de débogage dans un fichier, cochez la case **Activer le traçage** dans la sous-section **Paramètres de diagnostic des échecs**.

4. Dans le champ **Dossier des fichiers de traçage**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage.

   Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.

5. Configurez le niveau de détail des informations de débogage.

6. Définissez la **Taille maximale d'un fichier de traçage (Mo)**.

   Valeurs disponibles : de 1 à 4 095 Mo. Par défaut, la taille maximale des fichiers de traçage est de 50 Mo.

7. Si vous souhaitez que l'application supprime les fichiers les plus anciens une fois que le nombre maximal de fichiers de traçage a été atteint, cochez la case **Supprimer les fichiers de traçage les plus anciens**.

8. Définissez le paramètre **Nombre maximum de fichiers pour un journal de traces**.

   Valeurs disponibles : de 1 à 999. Par défaut, le nombre maximal de fichiers est de 5. Le champ est accessible uniquement si la case **Supprimer les fichiers de traçage les plus anciens** est cochée.

9. Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump**.

10. Dans le champ **Dossier des fichiers dump**, indiquez le chemin d'accès absolu au dossier local dans lequel Kaspersky Embedded Systems Security enregistrera le fichier dump.

    Le dossier doit déjà exister et doit être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque et des variables d'environnement.

11. Cliquez sur le bouton **OK**.

Les paramètres configurés de l'application seront appliqués sur l'appareil protégé.

Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Embedded Systems Security et configurer les paramètres de la planification.

Planification des tâches

La Console de l'application permet de configurer la planification du lancement des tâches locales du système et des tâches définies par l'utilisateur. L'administration des tâches de groupe via la Console de l'application est impossible.

Pour planifier des tâches de groupe à l'aide du Web Plug-in :

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

2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.

3. Sélectionnez la section **Paramètres de l'application**.

4. Dans la section **Planification**, cochez la case **Exécuté selon la planification**.

Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée de ces tâches est interdite par une stratégie de Kaspersky Security Center.

5. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :

   a. Choisissez une des options suivantes dans la liste **Fréquence** :

   - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
   - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
   - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi).
   - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Embedded Systems Security.
   - **À la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.

   b. Indiquez, dans le champ **Heure de lancement**, l'heure du premier lancement de la tâche.

   c. Indiquez, dans le champ **Date de lancement**, la date d'entrée en vigueur de la planification.

6. Dans la section **Paramètres d'arrêt de la tâche** :

   a. Cochez la case **Durée**, puis dans les champs à droite, saisissez le nombre maximum d'heures et de minutes pour l'exécution de la tâche.

   b. Cochez la case **Pauser la tâche**, puis saisissez dans les champs de droite les heures de début et de fin de l'intervalle par 24 heures au cours duquel la tâche sera suspendue.

7. Dans la section **Paramètres de planification avancés** :

   a. Cochez la case **Annuler la planification** et indiquez la date à partir de laquelle la planification ne sera plus active.

   b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.

   c. Cochez la case **Heure de lancement de la tâche aléatoire dans l'intervalle** et indiquez la valeur du paramètre en minutes.

8. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres de lancement de la tâche.

Activation et désactivation du lancement programmé

Vous pouvez activer ou désactiver le lancement des tâches planifiées après ou avant la configuration de la planification.

Pour activer ou désactiver la planification du lancement de la tâche :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.
   La fenêtre **<Nom de la tâche>** s'ouvre.
3. Sélectionnez la section **Paramètres de l'application**.
4. Sélectionnez la section **Planification**.
5. Réalisez une des opérations suivantes :
   - Cochez la case **Exécuté selon la planification** si vous souhaitez activer l'exécution planifiée d'une tâche.
   - Décochez la case **Exécuté selon la planification** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

     Les paramètres de la planification du lancement de la tâche ne sont pas supprimés. Ils sont appliqué au prochain lancement planifié de la tâche.
6. Cliquez sur **Enregistrer**.

Les paramètres configurés de la planification du lancement de la tâche sont enregistrés.

Rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils sont basés sur les informations stockées sur le serveur d'administration.

A partir de la version Kaspersky Security Center 11, les types de rapport suivants sont disponibles pour Kaspersky Embedded Systems Security :

- Rapport sur l'état des composants de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Consultez l'*aide de Kaspersky Security Center* pour obtenir des informations détaillées sur tous les rapports de Kaspersky Security Center et la manière de les configurer.

Rapport sur l'état des composants de Kaspersky Embedded Systems Security

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée de l'ensemble de composants défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque composant : *Exécution en cours*, *En pause*, *Arrêté*, *Dysfonctionnement*, *Pas installé*, *Démarrage en cours*.

L'état *Non installé* fait référence au composant, et non à l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center Web Console attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de composants et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de composants et leur état.

Cf. *Aide de Kaspersky Security Center* pour plus de détails sur la création et l'utilisation de sélections.

Pour consulter l'état des composant dans les paramètres de l'application :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique** → **Périphériques administrés**.
2. Cliquez sur le nom de l'appareil protégé.
3. Sous l'onglet **Général**, sélectionnez la section **Composants**.
4. Consultez le tableau d'état.

   Les informations sur l'état du composant Protection contre les exploits ne sont pas disponibles dans ce tableau.

Pour consulter un rapport standard Kaspersky Security Center Web Console :

1. Sélectionnez **Surveillance et rapports** → **Rapports**.
2. Sélectionnez l'option **Rapport sur l'état des composants de l'application**, puis cliquez sur le bouton **Afficher le rapport**.

   Un rapport est généré.
3. Consultez les détails de rapport suivants :
   - Diagramme graphique.
   - Tableau récapitulatif des composants et nombres totaux d'appareils de réseau où chacun des composants est installé et groupes auxquels ils appartiennent.
   - Tableau détaillé spécifiant l'état des composants, la version, l' et le groupe.

Rapports sur les applications interdites dans les modes actifs et d'essai

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications, deux types de rapports peuvent être générés : un rapport sur les applications interdites (si la tâche est démarrée en mode Actif) et un rapport sur les applications interdites en mode test (si la tâche est démarrée en mode Statistiques seulement). Ces rapports affichent des informations sur les applications interdites sur les appareils protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky installées sur les périphériques protégés.

Pour afficher un rapport sur les applications interdites en mode Statistiques seulement :

1. Démarrez la tâche Contrôle du lancement des applications en mode Statistiques seulement.

2. Sélectionnez **Surveillance et rapports → Rapports**.

3. Sélectionnez le **Rapport sur les applications interdites en mode test** et cliquez sur le bouton **Afficher le rapport**.

   Un rapport est généré.

4. Consultez les détails de rapport suivants :

   - Diagramme graphique qui affiche les dix applications avec le plus grand nombre de démarrages bloqués.
   - Tableau récapitulatif des interdictions d'applications spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
   - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

Pour afficher un rapport sur les applications interdites en mode Actif :

1. Lancez la tâche Contrôle du lancement des applications en mode Actif.

2. Sélectionnez **Surveillance et rapports → Rapports**.

3. Sélectionnez le **Rapport sur les applications interdites en mode test** et cliquez sur le bouton **Afficher le rapport**.

   Un rapport est généré.

Ce rapport comprend les mêmes données au sujet des blocs que le rapport sur les applications interdites en mode test.

Interface de diagnostic compacte

Cette section explique comment utiliser l'interface de diagnostic compacte pour réviser l'état de l'appareil protégé ou l'activité en cours et comment configurer l'écriture de fichiers dump et de fichiers de trace.

A propos de l'interface de diagnostic compacte

Le composant Interface de diagnostic compacte (également appelé "CDI") est installé et désinstallé avec le composant Icône dans la barre d'état système indépendamment de la Console de l'application et peut être utilisé quand la Console de l'application n'est pas installée sur l'appareil protégé. Le composant CDI est lancé depuis l'icône de la barre d'état système ou via l'exécution du fichier kavfsmui.exe depuis le dossier de l'application sur l'appareil protégé.

La fenêtre de la CDI permet de réaliser les opérations suivantes :

- Réviser les informations sur l'état général de l'application.
- Révisez les incidents de sécurité qui se sont produits.
- Réviser l'activité en cours sur le périphérique protégé.
- Lancer ou arrêter l'écriture des fichiers dump et de trace.
- Ouvrez la Console de l'application.
- Ouvrez la fenêtre **A propos de l'application** qui reprend la liste des mises à jour et des correctifs disponibles.

Le CDI est disponible même si l'accès à la fonction de Kaspersky Embedded Systems Security est protégés par un mot de passe. Aucun mot de passe requis.

Le composant CDI ne peut pas être configuré via Kaspersky Security Center.

Révision de l'état de Kaspersky Embedded Systems Security via l'interface de diagnostic compacte

Pour ouvrir la fenêtre Interface de diagnostic compacte, procédez comme suit :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.

   La fenêtre **Interface de diagnostic compacte** s'affiche.

Consultez l'état actuel de la clé, des tâches Protection en temps réel de l'ordinateur et des tâches de mise à jour sous l'onglet **État de la protection**. Différentes couleurs sont utilisées pour avertir l'utilisateur sur l'état de la protection (cf. tableau ci-dessous).

État de protection de l'interface de diagnostic compacte

Section	État

État de la Protection en temps réel	Le panneau est *vert* pour les scénarios suivants (si n'importe laquelle des conditions est remplie) :
	• Configuration recommandée :
	  • La tâche Protection des fichiers en temps réel est démarrée selon les paramètres par défaut.
	  • La tâche Contrôle du lancement des applications est démarrée en mode **Actif** avec les paramètres par défaut.
	• Configuration acceptable :
	  • La tâche Protection des fichiers en temps réel est configurée par l'utilisateur.
	  • Les paramètres de la tâche Contrôle du lancement des applications sont modifiés.

	Le panneau est *jaune* si une ou plusieurs des conditions suivantes sont remplies : • La tâche Protection des fichiers en temps réel est suspendue (par l'utilisateur ou selon une programmation). • La tâche Contrôle du lancement des applications est démarrée en mode **Statistiques seulement**. • Protection contre les exploits et Contrôle du lancement des applications sont démarrés en mode **Statistiques seulement**.
	Le panneau est *rouge* si une ou plusieurs des conditions suivantes sont remplies : • Le composant Protection des fichiers en temps réel n'est pas installé ou la tâche est arrêtée ou suspendue. • Le composant Contrôle du lancement des applications n'est pas installé ou la tâche Contrôle du lancement des applications est démarrée en mode **Statistiques seulement**.
Licence	Le panneau est *vert* si la licence en cours est valide.
	Un panneau *jaune* indique qu'un des événements suivants s'est produit : • *Vérification de l'état de la licence*. • *Il reste 14 jours avant l'expiration de la licence et aucune clé additionnelle ou code d'activation n'a été ajouté.* • *La clé ajoutée est inscrite sur la liste de refus et va bientôt être bloquée.*
	Un panneau *rouge* indique qu'un des événements suivants s'est produit : • *L'application n'a pas été activée* • *Licence expirée* • *Violation du Contrat de licence utilisateur final*

	• *Clé ajoutée à la liste de refus*
Mise à jour	Le panneau est *vert* lorsque les bases de l'application sont à jour.
	Le panneau est *jaune* lorsque les bases de l'application sont dépassées.
	Le panneau est *rouge* lorsque les bases de l'application sont fortement dépassées.

Révision des statistiques des événements de sécurité

L'onglet **Statistiques** affiche tous les événements de sécurité. Les statistiques de chaque tâche de protection s'affichent dans un bloc séparé, spécifiant le nombre d'incidents, ainsi que la date et l'heure de survenue du dernier incident. Lorsqu'un incident est enregistré, le bloc devient rouge.

Pour consulter les statistiques :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.

   La fenêtre **Interface de diagnostic compacte** s'affiche.
3. Ouvrez l'onglet **Statistiques**.
4. Révisez les incidents de sécurité pour les tâches de protection.

Révision de l'activité en cours de l'application

Cet onglet permet de consulter l'état des tâches et des processus en cours de l'application et d'obtenir des notifications rapides sur les événements critiques qui se produisent.

Différentes couleurs sont utilisées pour indiquer l'état de l'activité de l'application :

- Dans la section **Tâches** :
  - *Vert*. Il n'y a aucune condition qui pourrait nécessité le jaune ou le rouge.
  - *Jaune*. Analyse rapide non réalisée depuis longtemps.
  - *Rouge*. Au moins une des conditions suivantes est remplie :
    - Aucune tâche n'est lancée et la planification du lancement n'est défini pour aucune des tâches.
    - Les erreurs de lancement de l'application sont consignées en tant qu'événements critiques.
- Dans la section **Kaspersky Security Network** :
  - *Vert*. La tâche Utilisation du KSN est lancée.
  - *Jaune*. La Déclaration de KSN est acceptée, mais la tâche n'est pas lancée.

Pour consulter l'activité en cours de l'application sur l'appareil protégé :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.
2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.

   La fenêtre **Interface de diagnostic compacte** s'affiche.
3. Ouvrez l'onglet **Activité actuelle de l'application**.
4. Consultez les informations suivantes dans la section **Tâches** :
   - **Les zones critiques n'ont pas été analysées depuis longtemps**

     Ce champ est affiché uniquement si l'application renvoie un avertissement correspondants sur les analyses d'une zone critique.
   - **En cours d'exécution**
   - **Échec de l'exécution**
   - **Prochain lancement planifié**
5. Consultez les informations suivantes dans la section **Kaspersky Security Network** :
   - **KSN est activé. Les services concernant la réputation des fichiers sont activés** ou **La protection est désactivée**.
   - **KSN est activé. Les services concernant la réputation des fichiers sont activés, statistiques de l'application envoyées à KSN**.

     L'application envoie les données sur les détections d'applications malveillantes, y compris les logiciels frauduleux détectés pendant l'exécution des tâches de protection des fichiers en temps réel et d'analyse à la demande, ainsi que les informations de débogage relatives aux échecs survenus lors de l'analyse.

     Ce champ apparaît quand la case **Envoyer les statistiques de Kaspersky Security Network** est cochée dans les paramètres de la tâche Utilisation du KSN.
6. Consultez les informations suivantes dans la section **Intégration à Kaspersky Security Center** :
   - **Gestion locale autorisée**.
   - **La stratégie est appliquée :**<Nom du Serveur d'administration>.

Configuration de l'écriture de fichiers dump et de fichiers de trace

Vous pouvez configurer l'écriture de fichiers dump et de fichiers de trace via la CDI.

Vous pouvez également configurer les diagnostics des échecs via la Console de l'application.

Pour commencer à écrire les fichiers dump et de trace, réaliser les opérations suivantes :

1. Cliquez avec le bouton droit sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.

2. Sélectionnez l'option **Ouvrir l'interface de diagnostic compacte**.

   La fenêtre **Interface de diagnostic compacte** s'affiche.

3. Ouvrez l'onglet **Dépannage**.

4. Le cas échéant, configurez les paramètres suivants de la trace :

   a. Cochez la case **Activer le traçage**.

   b. Cliquez sur le bouton **Parcourir** afin de désigner le dossier où Kaspersky Embedded Systems Security enregistrera les fichiers de traçage.

      Le traçage sera activé pour tous les composants avec les paramètres par défaut avec le niveau de détail *Débogage* et la taille de journal maximale par défaut de 50 Mo.

5. Le cas échéant, configurez les paramètres suivants des fichiers dump :

   a. Cochez la case **Créez un fichier dump dans ce dossier en cas de dysfonctionnement**.

   b. Cliquez sur le bouton **Parcourir** afin de désigner le dossier où Kaspersky Embedded Systems Security enregistrera les fichiers dump.

6. Cliquez sur le bouton **Appliquer**.

   La nouvelle configuration est appliquée.

Mise à jour des bases de données et des modules de l'application Kaspersky Embedded Systems Security

Cette section présente les tâches de mises à jour des bases de données et des modules de l'application Kaspersky Embedded Systems Security, la copie des mises à jour de la base de données et le retour à l'état antérieur aux mises à jour. Elle explique également comment configurer les paramètres des tâches de mise à jour de la base de données et des modules de l'application.

A propos des tâches de mise à jour

Kaspersky Embedded Systems Security prévoit quatre tâches système pour la mise à jour : mise à jour des bases de l'application, mise à jour des modules de l'application, copie des mises à jour et annulation de la mise à jour des bases de l'application.

Par défaut Kaspersky Embedded Systems Security établit la connexion à la source des mises à jour (un des ordinateurs de mise à jour de Kaspersky) toutes les heures. Vous pouvez configurer tous les tâches de mise à jour, sauf la tâche Annulation de la mise à jour des bases de l'application. Une fois que les paramètres de la tâche ont été modifiés, Kaspersky Embedded Systems Security appliquera les nouvelles valeurs au prochain lancement de l'application.

Vous ne pouvez pas suspendre et reprendre une tâche de mise à jour.

Mise à jour des bases de l'application

Par défaut, Kaspersky Embedded Systems Security copie les bases depuis la source des mises à jour sur le périphérique protégé et les utilise directement dans la tâche Protection en temps réel de l'ordinateur en cours. Les tâches Analyse à la demande utiliseront les bases de l'application mises à jour à leur prochaine exécution.

Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des bases de l'application toutes les heures.

Mise à jour des modules de l'application

Par défaut, Kaspersky Embedded Systems Security vérifie la disponibilité des mises à jour des modules de l'application sur la source de mise à jour. L'utilisation des modules de l'application installés exige le redémarrage du périphérique protégé et/ou de Kaspersky Embedded Systems Security.

Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16:00 (l'heure dépend des paramètres régionaux du périphérique protégé). Pendant l'exécution de la tâche, l'application recherche la présence éventuelle de mises à jour prévues ou extraordinaires pour les modules de Kaspersky Embedded Systems Security, mais ne les distribue pas.

Copie des mises à jour

Par défaut, lors de l'exécution de la tâche, Kaspersky Embedded Systems Security télécharge les fichiers de mise à jour des bases de l'application et les enregistre dans le dossier de réseau ou dans le dossier local indiqué, sans les appliquer.

La Copie des mises à jour n'est pas exécutée par défaut.

Annulation de la mise à jour des bases de l'application

Au cours de cette tâche, Kaspersky Embedded Systems Security utilise à nouveau les bases de la mise à jour antérieure.

La tâche Annulation de la mise à jour des bases de l'application n'est pas exécutée par défaut.

A propos de la mise à jour des modules de l'application

Kaspersky peut diffuser des paquets de mise à jour pour les modules de Kaspersky Embedded Systems Security. Les mises à jour sont réparties entre les *mises à jour urgentes* (ou *critiques*) ou les mises à jour prévues. Les mises à jour urgentes suppriment des vulnérabilités et corrigent les erreurs tandis que les mises à jour prévues peuvent ajouter de nouvelles fonctions ou améliorer des fonctions existantes.

Les mises à jour urgentes (critiques) sont publiées sur les serveurs de mise à jour de Kaspersky. Vous pouvez configurer l'installation automatique grâce à la tâche Mise à jour des modules de l'application. Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16:00 (l'heure dépend des paramètres régionaux du périphérique protégé).

Kaspersky ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky. Vous pouvez obtenir des informations sur la diffusion des mises à jour prévues de Kaspersky Embedded Systems Security à l'aide la tâche Mise à jour des modules de l'application.

Vous pouvez récupérer les mises à jour critiques sur Internet et les appliquer à chaque appareil protégé ou choisir un appareil protégé en guise d'intermédiaire où vous copierez les mises à jour sans les installer avant de les diffuser sur les appareils protégés du réseau. Pour copier et enregistrer les mises à jour sans les installer, utilisez la tâche Copie des mises à jour.

Avant d'installer les mises à jour des modules, Kaspersky Embedded Systems Security crée une copie de sauvegarde des modules installés antérieurement. Si la mise à jour des modules de l'application est interrompue ou si elle se solde par un échec, Kaspersky Embedded Systems Security utilisera à nouveau automatiquement les modules installés précédemment. Vous pouvez aussi décider de revenir manuellement à l'état antérieur à la mise à jour des modules.

Lors de l'installation des mises à jour récupérées, le Service Kaspersky Security s'arrête puis redémarre automatiquement.

A propos de la mise à jour des bases de l’application

Les bases de Kaspersky Embedded Systems Security sur le périphérique protégé sont très vite dépassées. Les experts en virus de Kaspersky découvrent chaque jour des centaines de nouvelles menaces, créent les définitions qui permettent de les identifier et les intègrent aux mises à jour des bases de l'application. Une Mise à jour des bases de données est un fichier ou un ensemble de fichiers contenant les définitions capables d'identifier les menaces qui ont fait leur apparition depuis la diffusion de la mise à jour précédente. Pour réduire le risque d'infection de l'appareil au minium, il est conseillé de réaliser une mise à jour régulière des bases de données.

Par défaut, si les bases de données de Kaspersky Embedded Systems Security n'ont pas été mises à jour dans la semaine qui suit la création de la dernière mise à jour des bases de données installée, l'événement *Bases de l'application dépassées* est déclenché. Si les bases de données restent deux semaines sans mises à jour, l'événement *Bases de l'application fortement dépassées* est déclenché. Les informations relatives à l'état de mise à jour des bases de données sont affichées dans le volet résultats du nœud **Kaspersky Embedded Systems Security** de l'arborescence de la Console de l'application. Vous pouvez utiliser les paramètres généraux de Kaspersky Embedded Systems Security pour désigner une période différente (en jours) avant que ces événements ne se produisent. Vous pouvez configurer les notifications de l'administrateur au sujet de ces événements.

Kaspersky Embedded Systems Security télécharge les mises à jour des bases et des modules de l'application depuis des serveurs de mise à jour FTP ou HTTP de Kaspersky, depuis le Serveur d'administration de Kaspersky Security Center ou depuis d'autres sources de mises à jour.

Vous pouvez télécharger les mises à jour sur chaque appareil protégé ou choisir un appareil protégé en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les appareils protégés. Si vous utilisez Kaspersky Security Center pour l'administration centralisée de la protection des appareils de l'entreprise, vous pouvez utiliser le Serveur d'administration de Kaspersky Security Center en guise d'intermédiaire pour le téléchargement des mises à jour.

Les tâches de mise à jour des bases de l'application peuvent être lancées manuellement ou selon une planification. Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des bases de l'application toutes les heures.

Si le téléchargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des dernières mises à jour des bases de données installées. En cas d'endommagement des bases de données de Kaspersky Embedded Systems Security, il est possible de revenir manuellement aux mises à jour antérieures.

Schémas de mise à jour des bases et des modules des applications antivirus utilisées dans l'entreprise

La sélection d'une source de mises à jour dans les tâches de mise à jour dépend du schéma utilisé pour la mise à jour des bases et des modules de l'application dans l'entreprise.

Vous pouvez mettre à jour les bases et les modules de Kaspersky Embedded Systems Security sur les périphériques protégés selon les schémas suivants :

- Télécharger les mises à jour directement depuis Internet sur chaque appareil protégé (schéma 1).
- Télécharger les mises à jour depuis Internet sur un appareil intermédiaire et les diffuser sur les appareils protégés au départ de cet appareil.

  L'appareil intermédiaire peut être n'importe quel appareil sur lequel une des applications suivantes est installée :

  - Kaspersky Embedded Systems Security (schéma 2).
  - Serveur d'administration Kaspersky Security Center (schéma 3).

La mise à jour via un appareil intermédiaire non seulement réduit le trafic Internet, mais offre également une sécurité supplémentaire à l'appareil protégé réseau.

Les schémas de mise à jour sont décrits ci-après.

Schéma 1. Mises à jour des bases de données et des modules directement via Internet

Pour configurer les mises à jour de Kaspersky Embedded Systems Security directement via Internet :

dans les paramètres des tâches Mise à jour des bases de l'application et Mise à jour des modules de l'application de chaque périphérique protégé, désignez les ordinateurs de mise à jour de Kaspersky en tant que sources des mises à jour.

En guise de source des mises à jour, vous pouvez indiquer d'autres serveurs HTTP ou FTP qui contiennent un dossier de mise à jour.

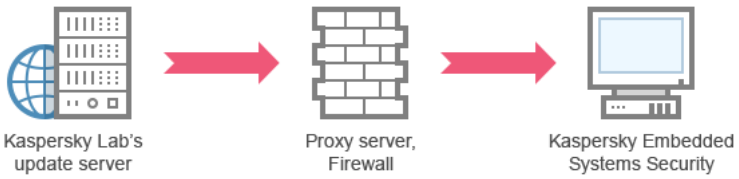

Figure 1 : Mises à jour des bases de données et des modules directement via Internet

Schéma 2. Mise à jour des bases de données et des modules via un des appareils protégés

Pour configurer la récupération des mises à jour de Kaspersky Embedded Systems Security via un des périphériques protégés, procédez comme suit :

1. Copiez les mises à jour sur l'appareil protégé sélectionné. Pour ce faire, procédez comme suit :
   - Sur l'appareil protégé sélectionné, configurez les paramètres de la tâche Copie des mises à jour :
     a. En guise de source des mises à jour, sélectionnez le serveur de mise à jour de Kaspersky.
     b. Désignez le dossier partagé en guise de dossier d'enregistrement des mises à jour.
2. Diffusez les mises à jour sur les autres appareils protégés. Pour ce faire, procédez comme suit :
   - Sur chaque périphérique protégé, configurez les paramètres de la tâche Mise à jour des bases de l'application (Mise à jour des modules de l'application) (cf. ill. ci-après) :
     a. En guise de source des mises à jour, saisissez le répertoire de l'appareil intermédiaire dans lequel vous avez copié les mises à jour.

Kaspersky Embedded Systems Security récupérera les mises à jour via un des périphériques protégés.

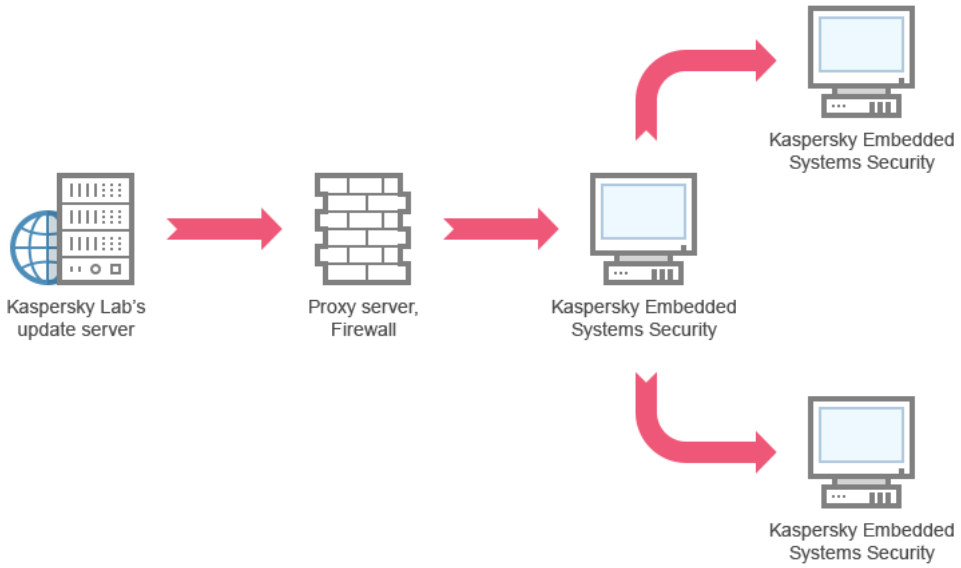

Figure 2 : Mise à jour des bases de données et des modules via un des périphériques protégés

Schéma 3. Mise à jour des bases de données et des modules via le Serveur d'administration Kaspersky Security Center

Si vous utilisez Kaspersky Security Center pour assurer l'administration centralisée de la protection du périphérique contre les virus, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Security Center (cf. ill. ci-après).

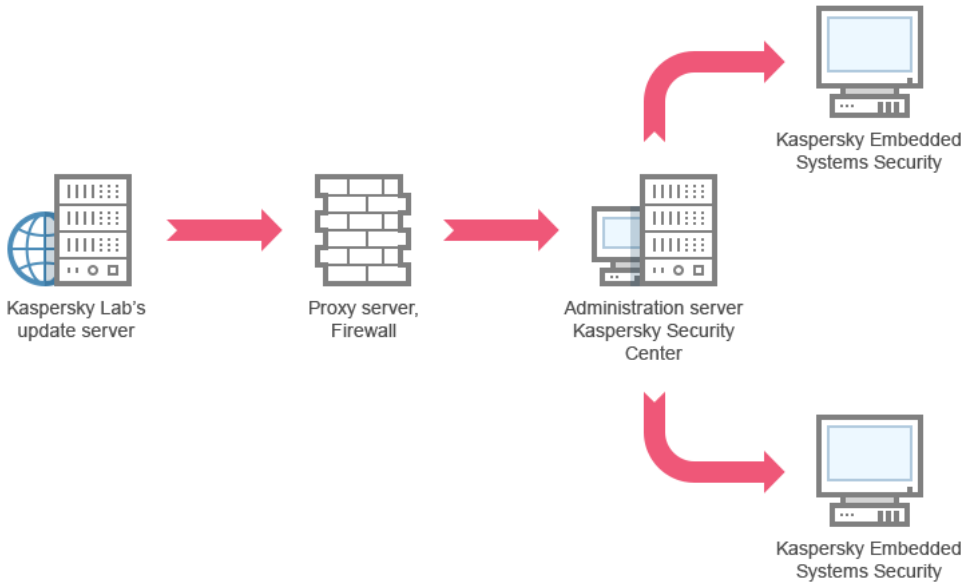

Figure 3 : Mise à jour des bases de données et des modules via le Serveur d'administration Kaspersky Security Center

Pour configurer la récupération des mises à jour de Kaspersky Embedded Systems Security via le Serveur d'administration Kaspersky Security Center, procédez comme suit.

1. Téléchargement des mises à jour depuis le serveur de mise à jour de Kaspersky vers le Serveur d'administration Kaspersky Security Center. Pour ce faire, procédez comme suit :

   - Configurez la tâche Réception des mises à jour par le Serveur d'administration pour une sélection d'appareils protégés indiquée :

     a. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky.

2. Diffusez les mises à jour sur les appareils protégés. Pour ce faire, réalisez une des opérations suivantes :

- Sur Kaspersky Security Center, configurez une tâche de groupe de mise à jour des bases antivirus (des modules de l'application) afin de diffuser les mises à jour aux appareils protégés :

  a. Dans la programmation de la tâche, choisissez la fréquence de démarrage **Après réception des mises à jour par le serveur d'administration**.

  Le Serveur d'administration exécutera la tâche chaque fois qu'il reçoit les mises à jour (cette méthode est la méthode recommandée).

  Vous ne pouvez pas spécifier la fréquence de démarrage **Après réception des mises à jour par le serveur d'administration** dans la console de l'application.

- Configurez sur chaque appareil protégé les tâches Mise à jour des bases de l'application et Mise à jour des modules de l'application :

  a. En guise de source des mises à jour, désignez le Serveur d'administration Kaspersky Security Center.

  b. Le cas échéant, planifiez l'exécution de la tâche.

  En cas de mises à jour peu fréquentes des bases antivirus de Kaspersky Embedded Systems Security (d'une fois par mois à une fois par an), la probabilité de détecter des menaces diminue tandis que la fréquence des faux positifs augmente dans les composants de l'application.

Kaspersky Embedded Systems Security récupérera les mises à jour via le Serveur d'administration Kaspersky Security Center.

Si vous avez l'intention d'utiliser le Serveur d'administration Kaspersky Security Center pour la diffusion des mises à jour, installez au préalable sur chaque appareil protégé le module logiciel Agent d'administration qui fait partie du kit de distribution de Kaspersky Security Center. Il assure l'interaction entre le Serveur d'administration et Kaspersky Embedded Systems Security sur le périphérique protégé. Pour obtenir de plus amples informations sur l'Agent d'administration et sa configuration à l'aide de l'application Kaspersky Security Center, consultez l'*aide de Kaspersky Security Center.*

Configuration des tâches de mise à jour

Cette section contient des instructions sur la configuration des tâches de mise à jour de Kaspersky Embedded Systems Security.

Configuration des paramètres d'utilisation des sources de mise à jour de Kaspersky Embedded Systems Security

Pour chaque tâche de mise à jour, à l'exception de la tâche Annulation de la mise à jour des bases de l'application, il est possible de définir une ou plusieurs sources de mise à jour, d'ajouter des sources de mise à jour définies par l'utilisateur et de configurer les paramètres de connexion aux sources indiquées.

En cas de modification des paramètres des tâches de mises à jour, sachez que les nouvelles valeurs ne sont pas appliquées immédiatement dans les tâches de mises à jour en cours d'exécution. Les nouveaux paramètres seront appliqués uniquement à la prochaine exécution de la tâche.

Pour déterminer le type de source des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le volet résultats du nœud sélectionné, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.
4. Dans la section **Source des mises à jour**, sélectionnez le type de source de mises à jour pour Kaspersky Embedded Systems Security :
   - **Serveur d'administration Kaspersky Security Center**
   - **Serveurs de mise à jour de Kaspersky**
   - **Serveurs HTTP, FTP ou dossiers réseau personnalisés**
5. Le cas échéant, configurez les paramètres complémentaires des sources de mise à jour définie par l'utilisateur :
   a. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.
      1. Dans la fenêtre **Serveurs de mise à jour** qui s'ouvre, cochez ou décochez les cases en regard des sources de mise à jour définies par l'utilisateur afin de commencer à les utiliser ou de suspendre leur utilisation.
      2. Cliquez sur le bouton **OK**.

   b. Dans la section **Source des mises à jour**, sous l'onglet **Général**, cochez ou décochez la case **Utiliser les serveurs de mise à jour de Kaspersky si les serveurs indiqués ne sont pas disponibles**.
6. Dans la fenêtre **Paramètres de la tâche**, choisissez l'onglet **Paramètres de connexion**, afin de configurer les paramètres de connexion à la source des mises à jour :
   - Cochez ou décochez la case **Utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky**.
   - Cochez ou décochez la case **Utiliser les paramètres du serveur proxy pour se connecter aux autres serveurs**.

   Pour des informations sur la configuration des paramètres facultatifs du serveur proxy et d'authentification pour l'accès au serveur proxy, cf. section Lancement et configuration de la tâche de mise à jour des bases de l'application de Kaspersky Embedded Systems Security.
7. Cliquez sur le bouton **OK**.

Les paramètres configurés de la source de mises à jour de Kaspersky Embedded Systems Security seront enregistrés et appliqués au prochain lancement de la tâche.

Vous pouvez gérer la liste des sources de mises à jour de Kaspersky Embedded Systems Security définies par l'utilisateur.

Pour modifier la liste des sources de mises à jour définies par l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le volet résultats du nœud sélectionné, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.
4. Cliquez sur le lien **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

   La fenêtre **Serveurs de mise à jour** s'ouvre.
5. Exécutez les actions suivantes :

   - Pour ajouter une nouvelle source définie par un utilisateur, cliquez sur **Ajouter**, puis saisissez dans le champ l'adresse du dossier contenant les fichiers de mise à jour sur le serveur FTP ou HTTP. Déterminer un dossier local ou réseau au format UNC (Universal Naming Convention). Appuyez sur la touche **ENTER**.

     Par défaut, le dossier ajouté est utilisé en guise de source de mises à jour.
   - Pour suspendre l'utilisation de la source définie par l'utilisateur, décochez la case en regard de la source dans la liste.
   - Pour activer l'utilisation de la source définie par l'utilisateur, cochez la case en regard de la source dans la liste.
   - Pour modifier l'ordre de sollicitation par Kaspersky Embedded Systems Security des sources de mise à jour définies par l'utilisateur, déplacez la source sélectionnée vers le haut ou vers le bas de la liste (si vous voulez l'utiliser plus tôt ou plus tard) à l'aide des boutons **Monter** et **Descendre**.
   - Pour modifier le chemin d'accès à une source définie par l'utilisateur, sélectionnez la source dans la liste et cliquez sur le bouton **Modifier**. Introduisez les modifications nécessaires dans le champ, puis appuyez sur la touche **RETOUR**.
   - Pour supprimer une source définie par l'utilisateur, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

     La liste doit toujours compter au moins une source.
6. Cliquez sur le bouton **OK**.

Les modifications introduites dans la liste des sources de mises à jour de l'application définies par l'utilisateur sont enregistrées.

Optimisation des entrées-sorties du disque lors de l'exécution de la tâche Mise à jour des bases de l'application

Dans le cadre de l'exécution de la tâche Mise à jour des bases de l'application, Kaspersky Embedded Systems Security place les fichiers de la mise à jour sur le disque local de l'appareil protégé. Vous pouvez réduire la charge sur le sous-système d'entrée/sortie du disque de l'appareil protégé en plaçant les fichiers des mises à jour sur un disque virtuel dans la mémoire vive lors de l'exécution de la mise à jour.

Cette fonction est disponible sous les systèmes d'exploitation Windows Server 7 et les versions plus récentes.

Si vous utilisez cette fonction lors de l'exécution de la tâche Mise à jour des bases de l'application, un disque logique supplémentaire peut apparaître dans le système d'exploitation. Ce disque logique disparaît du système d'exploitation quand la tâche est terminée.

Pour réduire la charge sur le sous-système disque du périphérique protégé lors de l'exécution de la tâche Mise à jour des bases de l'application :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant **Mise à jour des bases de l'application**.
3. Dans le volet résultats du nœud **Mise à jour des bases de l'application**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.
4. Configurez les paramètres suivants dans la section **Optimisation de l'utilisation des I/O du disque** :

   - Cochez ou décochez la case **Réduire la charge sur les I/O du disque**.
   - Définissez le volume de mémoire vive en méga-octets dans le champ **Volume de mémoire vive utilisé pour l'optimisation (en Mo)**. Le système d'exploitation affecte temporairement ce volume de mémoire vive à l'hébergement des fichiers des mises à jour pendant l'exécution de la tâche. Le volume de mémoire vive défini par défaut est de 512 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

     Lors de l'exécution de la tâche de Mise à jour des bases de l'application avec la fonction d'optimisation du sous-système de disque activée, l'une des situations suivantes peut se produire, selon la quantité de RAM allouée à la fonction :

     - Si la valeur est trop petite, la quantité de RAM allouée peut être insuffisante pour terminer la tâche de mise à jour des bases de l'application (par exemple, lors de la première mise à jour), ce qui entraînera la fin de la tâche avec une erreur.

       Dans ce cas, il est recommandé d'allouer plus de RAM pour la fonction d'optimisation du sous-système de disque.

     - Si la valeur est trop grande, au démarrage de la tâche de mise à jour des bases de l'application, il peut être impossible de créer un lecteur virtuel d'une taille sélectionnée en mémoire vive. Par conséquent, la fonctionnalité d'optimisation du sous-système de disque est automatiquement désactivée et la tâche de mise à jour des bases de l'application est exécutée sans la fonctionnalité d'optimisation.

       Dans ce cas, il est recommandé d'allouer moins de RAM pour la fonction d'optimisation du sous-système de disque.
5. Cliquez sur le bouton **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Configuration des paramètres de la tâche Copie des mises à jour

Pour configurer les paramètres de la tâche Copie des mises à jour, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.

2. Sélectionnez le nœud enfant **Copie des mises à jour**.
3. Dans le volet résultats du nœud **Copie des mises à jour**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous les onglets **Général** et **Paramètres de connexion**, configurez les paramètres d'utilisation des sources de mise à jour.
5. Dans la section **Paramètres de copie des mises à jour** de l'onglet **Général**, procédez comme suit :
   - Définissez les conditions de copie des mises à jour :
     - **Copier les mises à jour des bases de l'application**
     - **Copier les mises à jour critiques des modules de l'application**
     - **Copier les mises à jour des bases de l'application et les mises à jour critiques des modules de l'application**
   - Indiquez le répertoire local ou de réseau dans lequel Kaspersky Embedded Systems Security copiera les mises à jour reçues.
6. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche.
7. Sous l'onglet **Exécuter en tant que**, configurez le lancement de la tâche sous les autorisations d'un compte utilisateur spécifique.
8. Cliquez sur le bouton **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Configuration des paramètres de la tâche Mise à jour des modules de l'application

Pour configurer les paramètres de la tâche Mise à jour des modules de l'application, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant **Mise à jour des modules de l'application**.
3. Dans le volet résultats du nœud **Mise à jour des modules de l'application**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous les onglets **Général** et **Paramètres de connexion**, configurez les paramètres d'utilisation des sources de mise à jour.
5. Dans la section **Paramètres de la mise à jour** du groupe **Général**, configurez les paramètres de la mise à jour des modules de l'application :
   - **Rechercher uniquement la présence de mises à jour critiques des modules de l'application**
   - **Copier et installer les mises à jour critiques des modules de l'application**
   - **Autoriser le redémarrage du système d'exploitation**

- Recevoir des informations sur les mises à jour des modules de l'application prévues

6. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche. Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16:00 (l'heure dépend des paramètres régionaux du périphérique protégé).

7. Sous l'onglet **Exécuter en tant que**, configurez le lancement de la tâche sous les autorisations d'un compte utilisateur spécifique.

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

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Kaspersky ne publie pas les mises à jour prévues sur les serveurs de mise à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky. Vous pouvez configurer les notifications pour l'administrateur pour l'événement *Des mises à jour critiques et prévues sont disponibles* ; celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées.

Annulation des mises à jour des bases de l'application Kaspersky Embedded Systems Security

Avant d'exécuter la mise à jour des bases de données, Kaspersky Embedded Systems Security crée une copie de sauvegarde des bases utilisées antérieurement. Si la mise à jour est interrompue ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des bases de données installées antérieurement.

Si vous rencontrez des problèmes après la mise à jour des bases de données, vous pouvez revenir à l'état antérieur des bases grâce à la tâche Annulation de la mise à jour des bases de l'application.

Pour lancer la tâche Annulation de la mise à jour des bases de l'application,

Dans le panneau des résultats du nœud **Annulation de la mise à jour des bases de l'application**, cliquez sur le lien **Démarrer**.

Remise à l'état antérieur à la mise à jour des modules de l'application

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Avant d'appliquer la mise à jour des modules de l'application, Kaspersky Embedded Systems Security crée une copie de sauvegarde des modules utilisés actuellement. Si le processus de mise à jour des modules est interrompu ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des derniers modules actualisés installés.

Pour annuler la mise à jour des modules de l'application, exploitez la fonction **Installer et supprimer des applications** dans Microsoft Windows.

Statistiques sur les tâches de mise à jour

Pendant l'exécution de la tâche de mise à jour, les informations en temps réel sur le volume de données téléchargé depuis le lancement de la tâche ainsi que d'autres statistiques liées à l'exécution de la tâche, s'affichent.

Ces informations sont disponibles dans le journal d'exécution de la tâche quand la tâche est terminée ou arrêtée.

Pour afficher les statistiques des tâches de mise à jour :

1. Dans l'arborescence de la console de l'application, développez le nœud **Mise à jour**.
2. Sélectionnez le nœud enfant qui correspond à la tâche dont vous souhaitez consulter les statistiques.

   Le volet résultats du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Si vous consultez la tâche Mise à jour des bases de l'application ou la tâche Copie des mises à jour, la section **Statistiques** affiche le volume de données téléchargées par Kaspersky Embedded Systems Security à ce moment (**Données reçues**).

Le tableau suivant reprend les détails pour la tâche Mise à jour des modules de l'application.

Informations sur la tâche Mise à jour des modules de l'application

Champ	Description
Données reçues	Volume total de données téléchargées
Mises à jour critiques disponibles	Nombre de mises à jour critiques prêtes pour l'installation.
Mises à jour prévues disponibles	Nombre de mises à jour prévues disponibles pour l'installation.
Erreur d'application des mises à jour	Si la valeur de ce champ est différente de zéro, la mise à jour n'a pas été appliquée. Le nom de la mise à jour qui a provoqué une erreur est repris dans le journal d'exécution de la tâche.

Isolement des objets et copie des sauvegardes

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur le placement en quarantaine des fichiers probablement infectés.

Isolement des objets probablement infectés. Quarantaine

Cette section aborde l'isolement des objets probablement infectés, c.-à-d. le placement de ces objets en quarantaine, et la configuration du stockage de la quarantaine.

A propos du placement en quarantaine des objets probablement infectés

Kaspersky Embedded Systems Security place les objets considérés comme probablement infectés en quarantaine. Autrement dit, il les déplace de leur emplacement d'origine vers le dossier *Quarantaine*. Pour des raisons de sécurité, les objets dans le dossier de quarantaine sont conservés sous forme chiffrée.

Consultation des objets en quarantaine

Vous pouvez consulter les objets en quarantaine dans le nœud **Quarantaine** de la Console de l'application.

Pour consulter les objets en quarantaine :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.

   Les informations relatives aux objets placés en quarantaine apparaissent dans le volet résultats du nœud sélectionné.

Pour trouver l'objet requis dans la liste des objets en quarantaine,

triez les objets ou filtrez-les.

Tri des objets en quarantaine

Par défaut, les objets dans la liste des objets en quarantaine sont triés par date de placement dans l'ordre chronologique inverse. Pour trouver l'objet requis, vous pouvez trier les objets selon les colonnes contenant les informations relatives aux objets. Les résultats du tri sont préservés si vous fermez et ouvrez à nouveau le nœud **Quarantaine**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau.

Pour trier les objets :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.

2. Sélectionnez le nœud enfant **Quarantaine**.

3. Dans le volet résultats du nœud **Quarantaine**, sélectionnez l'en-tête de la colonne selon lequel vous souhaitez trier les objets de la liste.

Les objets de la liste seront triés selon le paramètre sélectionné.

Filtrage des objets en quarantaine

Pour trouver l'objet requis en quarantaine, vous pouvez filtrer les objets de la liste, par exemple afficher uniquement ceux qui répondent aux critères de filtrage que vous avez définis. Les résultats du filtrage sont préservés si vous quittez et ouvrez à nouveau le nœud **Quarantaine**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau à partir de ce fichier.

Pour désigner un ou plusieurs filtres :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.

2. Sélectionnez le nœud enfant **Quarantaine**.

3. Dans le menu contextuel du nom du nœud, sélectionnez l'option **Filtrer**.

   La fenêtre **Paramètres du filtre** s'ouvre.

4. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira de critère de filtrage.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans la liste **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez les étapes de a à d pour chaque filtre que vous ajoutez. Utilisez les recommandations ci-après lorsque vous travaillez avec des filtres :

   - Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.

   - Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.

   - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

   - Pour modifier un filtre, sélectionnez-le dans la liste de la fenêtre **Paramètres du filtre**. Changez ensuite les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer**.

5. Une fois que tous les filtres auront été ajoutés, cliquez sur le bouton **Appliquer**.

Les filtres créés sont enregistrés.

Pour afficher à nouveau tous les objets en quarantaine :

sélectionnez l'option **Supprimer le filtre** dans le menu contextuel du nœud **Quarantaine**.

Analyse de la quarantaine

Par défaut, Kaspersky Embedded Systems Security exécute la tâche locale du système Analyse de la quarantaine après chaque mise à jour des bases de l'application. Les paramètres de la tâche sont présentés dans le tableau suivant. Vous ne pouvez pas modifier les paramètres de la tâche Analyse de la quarantaine.

Vous pouvez configurer la planification du lancement de la tâche, la lancer manuellement et modifier les autorisations du compte utilisé pour lancer la tâche.

Suite à l'analyse des objets en quarantaine après la mise à jour des bases de l'application, Kaspersky Embedded Systems Security peut décider que certains de ces objets sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés, auquel cas Kaspersky Embedded Systems Security exécutera les actions définies dans les paramètres de la tâche Analyse de la quarantaine : désinfecter, supprimer si la désinfection est impossible.

Paramètres de la tâche Analyse de la quarantaine

Paramètres de la tâche Analyse de la quarantaine	Valeur
Zone d'analyse	Dossier de quarantaine
Paramètres de sécurité	Identiques pour toute la zone d'analyse ; les valeurs possibles sont reprises au tableau suivant

Paramètres de sécurité de la tâche Analyse de la quarantaine

Paramètre de sécurité	Valeur
Analyser les objets	Tous les objets de la zone d'analyse
Optimisation	Désactivée
Actions à exécuter sur les objets infectés et autres	Désinfecter, supprimer si la désinfection est impossible
Actions à exécuter sur les objets probablement infectés	Rapport uniquement
Exclure les fichiers	non
Ne pas détecter	non
Arrêter si l'analyse dure plus de (s.)	Non configuré
Ne pas analyser les objets de plus de (Mo)	Non configuré
Analyser les flux NTFS alternatifs	Activée
Analyser les secteurs d'amorçage et la partition MBR	Désactivée
Utiliser la technologie iChecker	Désactivée
Utiliser la technologie iSwift	Désactivée
Analyser les objets composés	• **Archives*** • **Archives SFX***

	• **Objets compactés*** • **Objets OLE intégrés*** * La fonction **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est désactivée.
Vérifier la signature Microsoft des fichiers	Non exécutée
Utiliser l'analyse heuristique	Appliqué au niveau d'analyse **Minutieuse**
Zone de confiance	Pas appliqué

Restauration du contenu de la quarantaine

Kaspersky Embedded Systems Security place les objets probablement infectés sous une forme chiffrée dans le dossier Quarantaine afin de protéger le périphérique protégé contre une éventuelle action malveillante.

Vous pouvez restaurer n'importe quel objet de la quarantaine. La restauration d'un objet peut s'imposer dans les situations suivantes :

- Après l'analyse de la quarantaine à l'aide des bases actualisées, l'état d'un objet devient **Fausse alerte** ou **Désinfecté**.
- Vous estimez que l'objet ne présente aucun danger pour l'appareil protégé et vous souhaitez l'utiliser. Afin que Kaspersky Embedded Systems Security n'isole plus cet objet lors des analyses ultérieures, il faut l'exclure du traitement dans la tâche Protection des fichiers en temps réel et des tâches d'analyse à la demande. Pour ce faire, désignez l'objet dans le paramètre de sécurité **Exclure les fichiers**(selon le nom du fichier) ou **Ne pas détecter** dans ces tâches ou ajoutez-le à la Zone de confiance.

Lors de la restauration des objets, vous pouvez sélectionner l'endroit où sera enregistré l'objet : dans l'emplacement d'origine (par défaut), dans un dossier spécial pour objets restaurés sur l'appareil protégé ou dans un dossier personnalisé de l'appareil protégé où est installé la console de l'application, ou sur un autre ordinateur du réseau.

Vous pouvez préciser le dossier utilisé pour stocker les objets restaurés sur le périphérique protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce répertoire est défini par les paramètres de la quarantaine.

La restauration d'objets de la Quarantaine peut entraîner l'infection de l'appareil protégé.

Vous pouvez restaurer l'objet en conservant une copie dans le répertoire Quarantaine afin de pouvoir l'utiliser ultérieurement, par exemple afin de pouvoir analyser une nouvelle fois l'objet après la mise à jour des bases de données.

Si l'objet placé en quarantaine faisait partie d'un objet composé (une archive par exemple), Kaspersky Embedded Systems Security ne l'inclut pas à nouveau dans cet objet lors de la restauration mais l'enregistre séparément dans le dossier indiqué.

Vous pouvez restaurer un ou plusieurs objets.

Pour restaurer des objets de la quarantaine, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Dans le volet résultats du nœud **Quarantaine**, exécutez une des actions suivantes :

   - Pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer.
   - Pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur un des objets sélectionnés et sélectionnez la commande Restaurer dans le menu contextuel.

   La fenêtre **Restauration de l'objet** s'ouvre.
4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chacun des objets sélectionnés le dossier dans lequel l'objet à restaurer va être enregistré.

   Le nom de l'objet apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous aviez choisi plusieurs objets, le nom du premier objet de la liste des objets sélectionnés s'affiche.
5. Exécutez une des actions suivantes :

   - Pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine**.
   - Pour restaurer un objet dans le dossier que vous avez défini en tant qu'emplacement de restauration des objets dans les paramètres, sélectionnez **Restaurer dans le dossier par défaut**.
   - Pour restaurer l'objet dans un autre dossier du périphérique protégé où vous avez installé la console de l'application ou dans un dossier partagé, sélectionnez **Restaurer dans le dossier de l'ordinateur local**, puis sélectionnez le dossier souhaité ou saisissez le chemin d'accès à celui-ci.
6. Si vous souhaitez conserver une copie de l'objet dans le dossier *Quarantaine* après leur restauration, décochez la case **Supprimer les objets des stockages après leur restauration**.
7. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les objets sélectionnés sont restaurés et enregistrés à l'emplacement indiqué. Si vous avez choisi **Restaurer dans le dossier d'origine**, chacun de ces objets sera enregistré dans son emplacement d'origine ; si vous aviez choisi **Restaurer dans le dossier par défaut** ou **Restaurer dans le dossier de l'ordinateur local**, tous les objets seront enregistrés dans le dossier indiqué.
8. Cliquez sur le bouton **OK**.

   Kaspersky Embedded Systems Security commence par restaurer le premier des objets que vous avez sélectionnés.
9. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

   a. Sélectionnez une des actions suivantes de Kaspersky Embedded Systems Security :

      - **Remplacer**, pour remplacer l'objet existant par l'objet restaurer.

- **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet restauré et son chemin d'accès dans le champ.

- **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

b. Si vous sélectionnez plusieurs objets en vue de la restauration, cochez la case **Appliquer à tous les objets sélectionnés** pour appliquer l'action (**Remplacer** ou **Renommer**) au reste de la sélection d'objets. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).

c. Cliquez sur le bouton **OK**.

L'objet sera restauré. Les informations relatives à la restauration sont consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, la fenêtre **Restauration de l'objet** peut s'ouvrir à nouveau. Vous pouvez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 4 des présentes instructions).

Mise en quarantaine d'objets

Vous pouvez mettre manuellement des fichiers en quarantaine.

Pour mettre un fichier en quarantaine :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Quarantaine**.
2. Choisissez l'option **Ajouter**.
3. Dans la fenêtre **Ouvrir**, sélectionnez le fichier que vous souhaitez placer en quarantaine.
4. Cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security place le fichier sélectionné en quarantaine.

Suppression d'objets de la quarantaine

Sur la base des paramètres de la tâche Analyse de la quarantaine, Kaspersky Embedded Systems Security supprime automatiquement du dossier Quarantaine les objets dont l'état est devenu *Infecté* suite à l'analyse de la quarantaine à l'aide des bases actualisées et si Kaspersky Embedded Systems Security n'avait pas réussi à les désinfecter. Kaspersky Embedded Systems Security ne supprime pas les autres objets de la Quarantaine.

Vous pouvez supprimer un ou plusieurs objets de la quarantaine.

Pour supprimer un ou plusieurs objets de la quarantaine :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Quarantaine**.
3. Exécutez une des actions suivantes :

- Pour supprimer un objet, choisissez l'option **Supprimer** dans le menu contextuel du nom de l'objet.

- Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez l'option **Supprimer**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

Les objets sélectionnés seront supprimés de la Quarantaine.

Envoi des objets probablement infectés à Kaspersky pour examen

Si le comportement d'un fichier indique selon vous la présence éventuelle d'une menace et que Kaspersky Embedded Systems Security le considère comme un fichier sain, il se peut que vous soyez en présence d'une menace inconnue dont la signature n'a pas encore été ajoutée aux bases de données. Vous pouvez envoyer ce fichier à Kaspersky pour examen. Les experts antivirus de Kaspersky analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de réparation aux bases. Quand vous analysez à nouveau l'objet après la mise à jour des bases de l'application, il est probable que Kaspersky Embedded Systems Security détermine que l'objet est infecté et qu'il le désinfecte. Vous pourrez alors non seulement conserver l'objet mais également éviter une épidémie virale.

Seuls les fichiers de la quarantaine peuvent être envoyés pour examen. Les fichiers en quarantaine sont conservés sous forme cryptée et lors de leur transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

Une fois que la licence a expiré, il est impossible d'envoyer un objet en quarantaine à Kaspersky pour examen.

Pour envoyer un fichier à Kaspersky pour examen :

1. Si le fichier ne se trouve pas déjà en quarantaine, placez-le à titre préventif en **Quarantaine**.

2. Dans le nœud **Quarantaine**, dans la liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous souhaitez envoyer à Kaspersky pour examen et sélectionnez l'option **Envoyer l'objet pour analyse**.

3. Dans la fenêtre de confirmation de l'opération, cliquez sur **Oui** si vous voulez vraiment envoyer l'objet sélectionné pour le soumettre à un examen.

4. Si un client de messagerie est configuré sur l'appareil protégé où la Console de l'application est installée, un nouveau message électronique est créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

   Le champ **Destinataire** du message contient l'adresse email de Kaspersky newvirus@kaspersky.com. Le champ Sujet contient le texte "Objet de la quarantaine".

   Le corps du message contient le texte "Le fichier sera envoyé à Kaspersky pour examen". Vous pouvez reprendre dans le corps du message n'importe quelle information complémentaire sur le fichier : raisons pour lesquelles il vous semble probablement infecté ou dangereux, son comportement et ses effets sur le système.

   Le message est accompagné de l'archive <nom de l'objet>.cab. L'archive contient un fichier <uuid>.klq avec l'objet chiffré, un fichier <uuid>.txt avec les informations relatives à l'objet extraites par Kaspersky Embedded Systems Security et un fichier Sysinfo.txt qui contient les informations suivantes relatives à Kaspersky Embedded Systems Security et au système d'exploitation de l'appareil protégé :

   - Nom et version du système d'exploitation.
   - Nom et version de Kaspersky Embedded Systems Security.
   - Date de publication des dernières mises à jour des bases de l'application installées.
   - Clé active.

Ces informations sont indispensables aux experts antivirus de Kaspersky afin de pouvoir analyser le fichier le plus vite et le plus efficacement possible. Toutefois, si vous ne souhaitez pas les transmettre, vous pouvez supprimer le fichier Sysinfo.txt de l'archive.

Si aucun client de messagerie n'est installé sur l'appareil protégé où se trouve la Console de l'application, l'application vous demande d'enregistrer l'objet chiffré sélectionné dans un fichier. Ce fichier peut être envoyé seul à Kaspersky.

Pour enregistrer un objet chiffré dans un fichier :

1. Dans la fenêtre qui vous invite à enregistrer l'objet, cliquez sur le bouton **OK**.
2. Sélectionnez le répertoire sur le disque de l'appareil protégé ou le répertoire de réseau dans lequel vous souhaitez enregistrer le fichier avec l'objet.

L'objet sera enregistré dans un fichier au format CAB.

Configuration des paramètres de la quarantaine

Vous pouvez configurer les paramètres de la Quarantaine. Les nouveaux paramètres de la quarantaine sont appliqués immédiatement après l'enregistrement.

Pour configurer les paramètres de la quarantaine :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Quarantaine**.
3. Choisissez l'option **Propriétés**.
4. Dans la fenêtre **Quarantaine de la quarantaine**, configurez les paramètres requis de la Quarantaine en fonction de vos besoins :
   - Dans la section **Paramètres de quarantaine** :
     - **Dossier de quarantaine**
     - **Taille maximale de la quarantaine (Mo)**
     - **Seuil d'espace disponible (Mo)**

     Si le volume des objets en quarantaine dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Embedded Systems Security vous le signale sans arrêter de placer les objets en quarantaine.
   - Dans la section **Paramètres de restauration** :
     - **Dossier cible pour la restauration des objets**
5. Cliquez sur le bouton **OK**.

Les nouveaux paramètres de la Quarantaine seront enregistrés.

Statistiques de quarantaine

Vous pouvez consulter les informations relatives au nombre d'objets en quarantaine ; il s'agit des statistiques de la quarantaine.

Pour consulter les statistiques de la Quarantaine,

choisissez l'option **Statistiques** dans le menu contextuel du nœud **Quarantaine** de l'arborescence de la console de l'application.

La fenêtre **Statistiques de quarantaine** reprend les informations sur le nombre d'objets en quarantaine à l'heure actuelle (cf. tableau ci-dessous).

Champ	Description
Objets probablement infectés	Nombre d'objets découverts par Kaspersky Embedded Systems Security et considérés comme probablement infectés.
Espace de quarantaine utilisé	Volume général de données dans le dossier Quarantaine.
Fausses alertes	Nombre d'objets qui ont reçu l'état *Fausse alerte* car l'Analyse de la quarantaine à l'aide des bases mises à jour a indiqué que ces objets étaient non infectés.
Objets désinfectés	Nombre d'objets qui ont reçu l'état *Désinfecté* après l'Analyse de la quarantaine.
Nombre total d'objets	Nombre total d'objets en quarantaine.

Sauvegarde des objets. Sauvegarde

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur la configuration des paramètres de la Sauvegarde.

A propos de la Sauvegarde des objets avant la désinfection ou la suppression

Kaspersky Embedded Systems Security enregistre une copie chiffrée des objets dont le statut est *Infecté* dans la *Sauvegarde* avant de les désinfecter ou de les supprimer.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Embedded Systems Security enregistre cet objet composé complet dans la Sauvegarde. Par exemple, si Kaspersky Embedded Systems Security considère un des objets de la base de messagerie comme étant infecté, il place l'ensemble de la base de messagerie dans la sauvegarde.

Si la taille de l'objet que Kaspersky Embedded Systems Security copie dans la sauvegarde est importante, le système peut ralentir et l'espace disponible sur le disque dur peut diminuer.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur l'appareil protégé ou sur un autre appareil du réseau local. Il est possible de restaurer un fichier depuis la sauvegarde, par exemple si un fichier infecté contient des informations importantes et que Kaspersky Embedded Systems Security ne parvient pas à le désinfecter sans endommager son intégrité et perdre les informations.

La restauration de fichiers de la sauvegarde peut provoquer l'infection de l'appareil protégé.

Consultation des objets dans la sauvegarde

Vous pouvez consulter les objets du dossier Sauvegarde uniquement via la console de l'application sous le nœud **Sauvegarde**. Vous ne pouvez pas les consulter à l'aide des gestionnaires de fichiers de Microsoft Windows.

Pour consulter les objets de la Sauvegarde,

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Sauvegarde**.

   Les informations relatives aux objets placés dans la Sauvegarde apparaissent dans le volet résultats du nœud sélectionné.

Pour trouver l'objet requis dans la liste des objets de la Sauvegarde,

triez les objets ou filtrez-les.

Tri des fichiers de la Sauvegarde

Par défaut, les fichiers de la Sauvegarde sont classés par date de sauvegarde dans l'ordre chronologique inversé. Pour trouver le fichier requis, vous pouvez trier les fichiers selon le contenu de n'importe quelle colonne dans le volet résultats.

Les résultats du filtrage sont préservés si vous quittez et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau à partir de ce fichier.

Pour trier les fichiers de la Sauvegarde :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Sauvegarde**.
3. Dans la liste des fichiers de la **Sauvegarde**, sélectionnez l'en-tête de la colonne selon laquelle vous souhaitez trier les objets.

Les fichiers de la Sauvegarde seront triés en fonction du critère sélectionné.

Filtrage des fichiers de la Sauvegarde

Pour trouver le fichier requis dans la Sauvegarde, vous pouvez filtrer les fichiers, c.-à-d. afficher dans le nœud **Sauvegarde** uniquement les fichiers qui répondent aux conditions de filtrage que vous avez définies (les filtres).

Les résultats du tri sont préservés si vous fermez et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de l'application, enregistrez le fichier msc et si vous l'ouvrez à nouveau.

Pour filtrer les fichiers dans la Sauvegarde :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Sauvegarde** et choisissez l'option **Filtrer**.

   La fenêtre **Paramètres du filtre** s'ouvre.

2. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez le champ qui servira de critère de filtrage.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage de la liste peuvent varier en fonction de la valeur sélectionnée dans le champ **Nom du champ**.

   c. Dans le champ **Valeur du champ**, saisissez la valeur du filtre ou sélectionnez-la dans la liste.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**. Répétez ces étapes pour chaque filtre que vous ajoutez. Les recommandations ci-après peuvent être utilisées lorsque vous travaillez avec des filtres :

   - Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
   - Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.
   - Pour modifier un filtre, sélectionnez-le dans la liste des filtres de la fenêtre **Paramètres du filtre**, modifiez les valeurs requises dans les champs **Nom du champ**, **Opérateur** ou **Valeur du champ**, puis cliquez sur le bouton **Remplacer**.

   Une fois que tous les filtres ont été ajoutés, cliquez sur le bouton **Appliquer**. La liste affichera uniquement les fichiers qui répondent aux conditions des filtres.

Pour afficher tous les fichiers dans la liste des fichiers dans la sauvegarde,

sélectionnez l'option **Supprimer le filtre** dans le menu contextuel du nœud **Sauvegarde**.

Restauration des fichiers depuis la Sauvegarde

Kaspersky Embedded Systems Security place les fichiers dans la Sauvegarde sous forme chiffrée afin de protéger le périphérique contre une éventuelle action malveillante.

Vous pouvez restaurer les fichiers de la Sauvegarde.

La restauration d'un fichier peut s'imposer dans les situations suivantes :

- Si le fichier original infecté contenait des informations importantes et que Kaspersky Embedded Systems Security n'a pas pu préserver son intégrité et que les informations qu'il contenait sont devenues inaccessibles.
- Vous estimez que le fichier ne présente aucun danger pour l'appareil protégé et vous souhaitez l'utiliser. Afin que Kaspersky Embedded Systems Security ne considère plus ce fichier comme un fichier infecté ou probablement infecté lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche Protection des fichiers en temps réel et dans les tâches Analyse à la demande. Pour ce faire, désignez le fichier dans le paramètre **Exclure les fichiers** ou le paramètre **Ne pas détecter** dans les tâches correspondantes.

  La restauration de fichiers de la sauvegarde peut provoquer l'infection de l'appareil protégé.

Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où il sera enregistré : l'emplacement d'origine (par défaut), un dossier spécial pour objets restaurés sur l'appareil protégé ou un dossier personnalisé sur l'appareil protégé où la console de l'application est installée ou sur un autre appareil du réseau.

Vous pouvez préciser le dossier pour stocker les objets restaurés sur le périphérique protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès à ce répertoire est défini par les paramètres de la Sauvegarde.

Par défaut, quand Kaspersky Embedded Systems Security restaure un fichier, il enregistre une copie dans la Sauvegarde. Vous pouvez supprimer la copie du fichier de la Sauvegarde après la restauration.

Pour restaurer les fichiers depuis la Sauvegarde :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Sélectionnez le nœud enfant **Sauvegarde**.
3. Dans le volet résultats du nœud **Sauvegarde**, exécutez une des actions suivantes :
   - Pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer.
   - Pour restaurer plusieurs objets, sélectionnez les objets souhaités à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur un des objets sélectionnés et sélectionnez la commande Restaurer dans le menu contextuel.

   La fenêtre **Restauration de l'objet** s'ouvre.
4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chacun des objets sélectionnés le dossier dans lequel l'objet à restaurer va être enregistré.

   Le nom de l'objet apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous aviez choisi plusieurs objets, le nom du premier objet de la liste des objets sélectionnés s'affiche.
5. Exécutez une des actions suivantes :
   - Pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine**.

- Pour restaurer un objet dans le dossier que vous avez défini en tant qu'emplacement de restauration des objets dans les paramètres, sélectionnez **Restaurer dans le dossier par défaut**.

- Pour restaurer l'objet dans un autre dossier du périphérique protégé où vous avez installé la console de l'application ou dans un dossier partagé, sélectionnez **Restaurer dans le dossier de l'ordinateur local**, puis sélectionnez le dossier souhaité ou saisissez le chemin d'accès à celui-ci.

6. Si vous ne souhaitez pas conserver une copie du fichier dans la sauvegarde après la restauration, cochez la case **Supprimer les objets des stockages après leur restauration** (case décochée par défaut).

7. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les objets sélectionnés sont restaurés et enregistrés à l'emplacement indiqué. Si vous avez choisi **Restaurer dans le dossier d'origine**, chacun de ces objets sera enregistré dans son emplacement d'origine ; si vous aviez choisi **Restaurer dans le dossier par défaut** ou **Restaurer dans le dossier de l'ordinateur local**, tous les objets seront enregistrés dans le dossier indiqué.

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

   Kaspersky Embedded Systems Security commence par restaurer le premier des objets que vous avez sélectionnés.

9. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

   a. Sélectionnez une des actions suivantes de Kaspersky Embedded Systems Security :

      - **Remplacer**, pour remplacer l'objet existant par l'objet restaurer.

      - **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet restauré et son chemin d'accès dans le champ.

      - **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

   b. Si vous sélectionnez plusieurs objets en vue de la restauration, cochez la case **Appliquer à tous les objets sélectionnés** pour appliquer l'action (**Remplacer** ou **Renommer**) au reste de la sélection d'objets. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).

   c. Cliquez sur le bouton **OK**.

   L'objet sera restauré. Les informations relatives à la restauration sont consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, la fenêtre **Restauration de l'objet** peut s'ouvrir à nouveau. Vous pouvez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant (cf. étape 4 des présentes instructions).

Suppression des fichiers de la Sauvegarde

Pour supprimer un ou plusieurs fichiers de la Sauvegarde :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.

2. Sélectionnez le nœud enfant **Sauvegarde**.

3. Exécutez une des actions suivantes :

   - Pour supprimer un objet, choisissez l'option **Supprimer** dans le menu contextuel du nom de l'objet.
   - Pour supprimer plusieurs objets, sélectionnez les objets dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez l'option **Supprimer**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Oui**, afin de confirmer l'opération.

Les fichiers sélectionnés seront supprimés de la Sauvegarde.

Configuration des paramètres de la Sauvegarde

Pour configurer les paramètres de la Sauvegarde :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Sauvegarde**.
3. Choisissez l'option **Propriétés**.
4. Dans fenêtre **Sauvegarde de la sauvegarde**, configurez les paramètres requis de la Sauvegarde en fonction de vos besoins :

   Dans la section **Paramètres de la Sauvegarde** :

   - Dossier de sauvegarde
   - Taille maximale de sauvegarde (Mo)
   - Seuil d'espace disponible (Mo)

     > Si le volume des objets de la Sauvegarde dépasse la valeur de la taille maximale ou du seuil d'espace disponible, Kaspersky Embedded Systems Security vous le signale sans arrêter de placer les objets dans la Sauvegarde.

   Dans la section **Paramètres de restauration** :

   - Dossier cible pour la restauration des objets

5. Cliquez sur le bouton **OK**.

Les paramètres configurés de la Sauvegarde seront enregistrés.

Statistiques de sauvegarde

Vous pouvez consulter les informations relatives à l'état de la Sauvegarde en ce moment ; il s'agit des statistiques de la Sauvegarde.

Pour consulter les statistiques de la Sauvegarde,

dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Sauvegarde** et sélectionnez **Statistiques**. La fenêtre **Statistiques de sauvegarde** s'ouvre.

La fenêtre **Statistiques de sauvegarde** reprend les informations relatives à l'état de la Sauvegarde à l'heure actuelle (cf. tableau ci-dessous).

Informations sur l'état actuel de la Sauvegarde

Champ	Description
Taille actuelle de la sauvegarde	Volume de données dans le dossier Sauvegarde ; tient compte de la taille des fichiers chiffrés
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde

Interdire l'accès aux ressources réseau. Sessions réseau bloquées

Cette section décrit comment bloquer les appareils distants et configurer les paramètres pour la Liste des sessions réseau bloquées.

À propos de la liste des sessions réseau bloquées

Par défaut, la Liste des sessions réseau bloquées peut être utilisée si l'un des composants suivants est installé : Protection des fichiers en temps réel, Protection contre les menaces réseau. Ces composants détectent les tentatives à distance de chiffrement, d'ouverture ou d'exécution des objets sur l'appareil protégé ou dans les dossiers partagés du périphérique de stockage NAS conformément à la liste des sessions réseau bloquées. Les informations relatives aux sessions réseau bloquées de tous les appareils protégés sont envoyées au Kaspersky Security Center. Kaspersky Embedded Systems Security bloque la session en cours et, en termes de session en cours, rend les dossiers partagés ou les dossiers de périphériques de stockage NAS inaccessibles.

La liste des sessions réseau bloquées est remplie quand au moins une des tâches suivantes est lancée en mode actif et (quand les conditions indiquées sont remplies) :

- Pour la tâche Protection des fichiers en temps réel : détection d'une activité malveillante émanant d'un périphérique qui tente d'accéder aux ressources de fichier réseau et dans les paramètres de la tâche Protection des fichiers en temps réel, la case **Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante** a été cochée.

- Pour la tâche Protection contre les menaces réseau : une activité typique des attaques réseau est détectée.

Après la détection d'une activité malveillante ou d'une tentative de chiffrement, la tâche envoie des informations sur la session réseau attaquante à la Liste des sessions réseau bloquées et l'application crée un événement de type *Attention* pour la session en cours de l'hôte attaquant. Toute tentative de cette session pour accéder au dossier réseau partagé protégés sera bloquée.

Si l'identifiant local unique (LUID) d'un hôte à l'origine de la session réseau attaquante est ajouté à la liste des sessions réseau bloquées, Kaspersky Embedded Systems Security détermine l'adresse IP de cet hôte et l'ajoute au lieu du LUID de l'hôte attaquant à la liste des sessions réseau bloquées.

Par défaut, Kaspersky Embedded Systems Security supprime les sessions réseau bloquées de la liste 30 minutes après leur ajout. L'accès aux ressources de fichier réseau est rétabli automatiquement après la suppression des sessions réseau de la liste des sessions réseau bloquées. Vous pouvez indiquer la durée au terme de laquelle les sessions réseau bloquées sont automatiquement débloquées.

Sachez que lorsque vous limitez l'accès à la gestion des stockages pour n'importe quel compte utilisateur, la liste des sessions réseau bloquées reste disponible. Les paramètres pour les sessions réseau bloquées ne sont pas modifiables, sauf si le compte utilisateur sélectionné possède les **Modifier les autorisations** pour l'administration de Kaspersky Embedded Systems Security.

Gestion de la liste des sessions réseau bloquées via le plug-in d'administration

Cette section explique comment configurer les paramètres de la Liste des sessions réseau bloquées via l'interface du Plug-in d'administration.

Activation du blocage des hôtes douteux

Pour ajouter des sessions réseau qui affichent une activité malveillante ou de chiffrement malveillant quelconque à la Liste des **sessions réseau bloquées** et bloquer l'accès aux ressources de fichier réseau pour ces hôtes, au moins une des tâches suivantes doit être exécutée en mode actif :

- Protection des fichiers en temps réel
- Protection contre les menaces réseau

Configuration de la tâche Protection des fichiers en temps réel :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.
2. Sélectionnez l'onglet **Stratégies** et ouvrez **<Nom de la stratégie>** > **Protection en temps réel de l'ordinateur** > **Paramètres** dans le groupe **Protection des fichiers en temps réel**.

   La fenêtre **Protection en temps réel de l'ordinateur** s'ouvre.
3. Dans la section **Intégration aux autres composants**, cochez la case **Ajouter les hôtes à l'origine d'une activité malveillante à la liste des ordinateurs douteux** si vous souhaitez que Kaspersky Embedded Systems Security bloque l'accès aux ressources de fichier réseau pour les hôtes sur lesquels une activité malveillante a été détectée pendant l'exécution de la tâche Protection des fichiers en temps réel.
4. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la planification**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
5. Dans la fenêtre **Protection en temps réel de l'ordinateur**, cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Configurez la tâche Protection contre les menaces réseau :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section.
6. Cliquez sur **Configuration** dans la sous-section **Protection contre les menaces réseau**.

   La fenêtre **Protection contre les menaces réseau** s'ouvre.
7. Ouvrez l'onglet **Général**.
8. Dans la section **Mode de traitement**, sélectionnez le mode de traitement **Bloquer les connexions quand une attaque est détectée**.

   La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

   Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

   Le mode est sélectionné par défaut.

   Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

   Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.
9. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la planification**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
10. Dans la fenêtre, cliquez sur **OK**.
11. Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres de la Liste des sessions réseau bloquées

Pour configurer la Liste des sessions réseau bloquées :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

- Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

  En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans la sous-section **Stockages**.

   La fenêtre **Paramètres des stockages** s'affiche.

5. Dans la section **Conditions du blocage des sessions réseau** de l'onglet **Sessions réseau bloquées**, indiquez le nombre de jours, d'heures et de minutes à décompter à partir du moment du blocage de la session réseau et au terme desquels les sessions réseau bloquées ont de nouveau accès aux ressources de fichier réseau.

6. Cliquez sur le bouton **OK**.

Gestion de la liste des sessions réseau bloquées via la Console de l'application

Cette section explique comment configurer les paramètres de la Liste des sessions réseau bloquées via l'interface de la Console de l'application

Activation du blocage des hôtes douteux

Pour ajouter des sessions réseau qui affichent une activité malveillante ou de chiffrement malveillant quelconque à la **Liste des sessions réseau bloquées** et bloquer l'accès aux ressources de fichier réseau pour ces hôtes, au moins une des tâches suivantes doit être exécutée en mode actif :

- Protection des fichiers en temps réel
- Protection contre les menaces réseau

Configuration de la tâche Protection des fichiers en temps réel :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.

3. Dans le volet résultats, cliquez sur le lien **Propriétés**.

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

4. Dans la section **Minutieuse**, cochez la case **Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante** si vous souhaitez que Kaspersky Embedded Systems Security bloque les hôtes sur lesquels une activité malveillante a été détectée pendant l'exécution de la tâche Protection des fichiers en temps réel.

5. Si la tâche n'a pas été lancée, ouvrez l'onglet **Planification** :

a. Cochez la case **Exécuté selon la planification**.

b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.

6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Configurez la tâche Protection contre les menaces réseau :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les menaces réseau**.
3. Dans le panneau de détails du nœud **Protection contre les menaces réseau**, cliquez sur le lien **Propriétés**.
4. La fenêtre **Paramètres de la tâche** s'ouvre.
5. Ouvrez l'onglet **Général**.
6. Dans la section **Mode de traitement**, sélectionnez le mode de traitement **Bloquer les connexions quand une attaque est détectée**.

   La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

   Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

   Le mode est sélectionné par défaut.

   Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

   Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.

7. Cochez ou décochez la case **Ne pas arrêter l'analyse du trafic quand la tâche n'est pas en cours d'exécution**.

   Si cette case est cochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security recherche dans le trafic réseau entrant toute activité typique des attaques réseau et bloque l'activité réseau de l'ordinateur attaquant en fonction du mode de traitement sélectionné.

   Si cette case est décochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security ne recherche pas dans le trafic réseau entrant les activités typiques des attaques réseau et ne bloque pas l'activité réseau de l'ordinateur attaquant.

   Cette case est décochée par défaut.

8. Si la tâche n'a pas été lancée, ouvrez l'onglet **Planification** :

   a. Cochez la case **Exécuté selon la planification**.

   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.

9. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres de la Liste des sessions réseau bloquées

Pour configurer la Liste des sessions réseau bloquées :

1. Dans l'arborescence de la console de l'application, développez le nœud **Stockages**.
2. Ouvrez le menu contextuel du nœud enfant **Sessions réseau bloquées**.
3. Sélectionnez l'option de menu **Propriétés**.

   La fenêtre **Paramètres de la liste des sessions réseau bloquées** s'affiche.
4. Dans la section **Condition de blocage des sessions réseau**, indiquez le nombre de jours, d'heures et de minutes au terme desquels les sessions réseau bloquées sont de nouveau autorisés à accéder aux ressources de fichier réseau.
5. Cliquez sur le bouton **OK**.
6. Pour restaurer l'accès à toutes les sessions réseau bloquées :
   a. Ouvrez le menu contextuel du nœud enfant **Sessions réseau bloquées**.
   b. Sélectionnez l'option **Débloquer tout**.

      Toutes les sessions réseaux bloquées seront supprimées de la liste et débloqués.
7. Pour supprimer plusieurs sessions de la liste des sessions réseau bloquées :
   a. Dans la liste des sessions réseau bloquées, qui s'affiche dans le volet résultats, sélectionnez un ou plusieurs sessions.
   b. Ouvrez le menu contextuel du nœud enfant **Sessions réseau bloquées**.
   c. Sélectionnez l'option **Débloquer la sélection**.

      Les sessions réseau sélectionnées sont débloquées.

Gestion de la liste des sessions réseau bloquées via le plug-in Web

Cette section explique comment configurer les paramètres de la Liste des sessions réseau bloquées via l'interface du plug-in Web.

Activation du blocage des sessions réseau

Pour ajouter des hôtes qui affichent une activité malveillante ou de chiffrement malveillant quelconque à la **Sessions réseau bloquées** et bloquer l'accès aux ressources de fichier réseau pour ces sessions, au moins une des tâches suivantes doit être exécutée en mode actif :

- Protection des fichiers en temps réel
- Protection contre les menaces réseau

Configuration de la tâche Protection des fichiers en temps réel :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection des fichiers en temps réel**.
6. Dans la section **Intégration aux autres composants**, cochez la **Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante** si vous souhaitez que Kaspersky Embedded Systems Security bloque la session en cours et rende les ressources réseau partagées indisponibles pour les sessions réseau pour lesquelles une activité malveillante a été détecté.
7. Si la tâche n'a pas été lancée, ouvrez l'onglet **Administration des tâches** :
   a. Cochez la case **Exécuté selon la planification**.
   b. Choisissez la fréquence **Au lancement de l'application** dans la liste déroulante.
8. Cliquez sur **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres de la Liste des sessions réseau bloquées

Pour configurer la Liste des sessions réseau bloquées :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Complémentaire**.
5. Cliquez sur **Configuration** dans la sous-section **Stockages**.
6. Dans la section **Complémentaire**, cliquez sur le bouton **Configuration** dans la sous-section **Stockages**.
   La fenêtre **Stockages** s'affiche.
7. Dans la section **Condition de blocage des sessions réseau** de l'onglet **Sessions réseau bloquées**, indiquez le nombre de jours, d'heures et de minutes à décompter à partir du moment du blocage de la session réseau et au terme desquels les sessions réseau bloquées ont de nouveau accès aux ressources de fichier réseau.
8. Cliquez sur le bouton **OK**.

Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security

Cette section fournit des informations sur l'utilisation des journaux de Kaspersky Embedded Systems Security.

Méthodes d'enregistrement des événements de Kaspersky Embedded Systems Security

Les événements de Kaspersky Embedded Systems Security sont scindés en deux groupes :

- événements liés au traitement des objets dans les tâches de Kaspersky Embedded Systems Security ;
- événements liés à l'administration de Kaspersky Embedded Systems Security, par exemple lancement de l'application, création ou suppression de tâches, modification des paramètres d'une tâche.

Kaspersky Embedded Systems Security enregistre les événements dans le journal à l'aide des méthodes suivantes :

- **Journaux d'exécution de la tâche**. Le journal d'exécution de la tâche contient des informations sur l'état actuel de paramètres de la tâche ou sur les événements survenus pendant l'exécution de la tâche.
- **Journal d'audit système**. Le journal d'audit système contient les informations relatives aux événements en rapport avec l'administration de Kaspersky Embedded Systems Security.
- **Journal des événements**. Le journal des événements contient les informations relatives aux événements nécessaires au diagnostic des échecs de fonctionnement de Kaspersky Embedded Systems Security. Ce journal est accessible dans la console Observateur d'événements de Microsoft Windows.
- **Journaux de sécurité**. Les Journaux de sécurité contiennent les informations relatives aux événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur l'appareil protégé.

Si un problème survient durant l'utilisation de Kaspersky Embedded Systems Security (par exemple, Kaspersky Embedded Systems Security ou une tâche particulière s'arrête suite à une erreur ou ne démarre pas) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un fichier de trace et un fichier dump des processus de Kaspersky Embedded Systems Security et envoyer ces fichiers avec ces informations au Support Technique de Kaspersky afin de diagnostiquer le problème rencontré.

Kaspersky Embedded Systems Security n'envoie pas de fichiers de trace ou dump automatiquement. Les données de diagnostics peuvent être envoyées uniquement par un utilisateur doté des autorisations adéquates.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump en clair. Le dossier où les fichiers sont enregistrés est sélectionné par l'utilisateur et géré par la configuration du système d'exploitation et les paramètres de Kaspersky Embedded Systems Security. Vous pouvez configurer les autorisations d'accès et permettre l'accès aux journaux, aux fichiers de trace et aux fichiers dump uniquement pour les utilisateurs qui en ont besoin.

Les fichiers téléchargeables via les liens suivants contiennent des tableaux qui reprennent la liste complète des événements de Kaspersky Embedded Systems Security des catégories suivantes :

- Événements enregistrés par Kaspersky Embedded Systems Security dans le journal des événements.

TÉLÉCHARGER KESS-WEL-EVENTS.ZIP

- Événements que Kaspersky Embedded Systems Security envoie au Serveur d'administration.

  TÉLÉCHARGER KESS-KSC-EVENTS.ZIP

Journal d'audit système

Kaspersky Embedded Systems Security réalise un audit système des événements liés à l'administration de Kaspersky Embedded Systems Security. L'application enregistre les informations relatives au lancement de l'application, au lancement et à l'arrêt de tâches de Kaspersky Embedded Systems Security, aux modifications des paramètres des tâches, à la création et à la suppression de tâches Analyse à la demande. Les enregistrements de l'ensemble de ces événements apparaissent dans le volet résultats lorsque vous sélectionnez le nœud **Journal d'audit système** dans la console de l'application.

Par défaut, Kaspersky Embedded Systems Security conserve les entrées du journal d'audit système pendant une durée illimitée. Vous pouvez spécifier la période de stockage des enregistrements dans le journal d'audit système.

Vous pouvez désigner un dossier dans lequel Kaspersky Embedded Systems Security va stocker les fichiers du journal d'audit système, différent du dossier choisi par défaut.

Tri des événements dans le journal d'audit système

Par défaut, les événements sont classés dans le nœud du journal d'audit système par ordre chronologique inverse.

Vous pouvez les trier selon le contenu de n'importe quelle colonne, à l'exception de la colonne **Événement**.

Pour trier les événements dans le journal d'audit système, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez le nœud enfant **Journal d'audit système**.
3. Dans le volet résultats, sélectionnez l'en-tête de la colonne que vous souhaitez utiliser pour trier les événements de la liste.

Les résultats triés sont enregistrés pour la prochaine session d'affichage du journal d'audit système.

Filtrage des événements dans le journal d'audit système

Vous pouvez configurer le journal d'audit système pour afficher uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage (filtres) que vous définissez.

Pour filtrer les événements dans le journal d'audit système :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez l'option **Filtrer**.

La fenêtre **Paramètres du filtre** s'ouvre.

3. Pour ajouter un filtre, procédez comme suit :

   a. Dans **Nom du champ**, sélectionnez une colonne pour filtrer les événements.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.

   c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.

   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.

4. Le cas échéant, réalisez une des opérations suivantes :

   - Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.

5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements du journal d'audit système.

   La liste des événements du journal d'audit système affiche uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est enregistré jusqu'à prochaine session d'affichage du journal d'audit système.

Pour désactiver le filtre, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.

2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez **Supprimer le filtre**.

   La liste des événements du journal d'audit système affiche alors tous les événements.

Suppression des événements du journal d'audit système

Par défaut, Kaspersky Embedded Systems Security conserve les entrées du journal d'audit système pendant une durée illimitée. Vous pouvez spécifier la période de stockage des enregistrements dans le journal d'audit système.

Vous pouvez supprimer manuellement tous les événements du journal d'audit système.

Pour supprimer des événements du journal d'audit système, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.

2. Ouvrez le menu contextuel du nœud enfant **Journal d'audit système** et choisissez **Effacer**.

3. Exécutez une des actions suivantes :

   - Si vous souhaitez exporter le contenu du journal d'audit système dans un fichier au format CSV ou TXT avant de supprimer les événements, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de la

suppression. Indiquez le nom et l'emplacement du fichier dans la fenêtre qui s'ouvre.

- Si vous ne souhaitez pas exporter le contenu du journal dans un fichier, cliquez sur le bouton **Non** dans la fenêtre de confirmation de la suppression.

Le contenu du journal d'audit système est effacé.

Journaux d'exécution des tâches

Cette section contient des informations relatives aux journaux d'exécution des tâches de Kaspersky Embedded Systems Security et des instructions sur leur administration.

A propos des journaux d'exécution des tâches

Les informations relatives à l'exécution des tâches de Kaspersky Embedded Systems Security apparaissent dans le panneau des résultats quand vous sélectionnez le nœud **Journaux d'exécution de la tâche** dans la Console de l'application.

Le journal d'exécution de chaque tâche permet de voir les statistiques de l'exécution de la tâche, les informations relatives à chaque objet traité par l'application depuis le lancement de la tâche ainsi que les paramètres de la tâche.

Par défaut, Kaspersky Embedded Systems Security conserve les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez désigner un dossier différent du dossier par défaut dans lequel Kaspersky Embedded Systems Security va enregistrer les fichiers des journaux d'exécution de la tâche. Vous pouvez également sélectionner les événements qui seront consignés dans les journaux d'exécution de la tâche par Kaspersky Embedded Systems Security.

Consultation de la liste des événements dans les journaux d'exécution de la tâche

Pour filtrer les journaux d'exécution de la tâche :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.

   La liste des événements consignés dans les journaux d'exécution de la tâche de Kaspersky Embedded Systems Security apparaît dans le volet résultats.

Vous pouvez les trier selon le contenu de n'importe quelle colonne ou appliquer un filtre.

Tri des journaux d'exécution des tâches

Par défaut, les journaux d'exécution des tâches s'affichent par ordre chronologique inverse. Vous pouvez les trier selon le contenu de n'importe quelle colonne.

Pour trier les journaux d'exécution des tâches :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le panneau des résultats, sélectionnez l'en-tête de la colonne que vous souhaitez utiliser pour trier les journaux d'exécution de la tâche de Kaspersky Embedded Systems Security.

Le résultat du tri est conservé jusqu'à la prochaine consultation des journaux d'exécution des tâches.

Filtrage des journaux d'exécution des tâches

Si vous le souhaitez, vous pouvez afficher dans la liste des événements des journaux d'exécution des tâches uniquement les journaux d'exécution des tâches qui répondent aux conditions de filtrage que vous définissez (filtres).

Pour filtrer les journaux d'exécution des tâches :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez **Filtrer**.
   La fenêtre **Paramètres du filtre** s'ouvre.
3. Pour ajouter un filtre, procédez comme suit :
   a. Dans **Nom du champ**, sélectionnez une colonne pour filtrer les journaux d'exécution des tâches.
   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.
   c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.
   d. Cliquez sur **Ajouter**.

   Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.
4. Le cas échéant, réalisez une des opérations suivantes :
   - Afin de réunir quelques filtres selon le « ET » logique, sélectionnez l'option **Quand toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres selon le « OU » logique, sélectionnez l'option **Quand n'importe quelle condition est remplie**.
5. Cliquez sur le bouton **Appliquer** pour enregistrer les critères de filtrage des événements dans la liste des événements des journaux d'exécution des tâches.

La liste des journaux d'exécution des tâches affiche alors uniquement les journaux d'exécution des tâches qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusqu'à la prochaine consultation des journaux d'exécution de la tâche.

Pour désactiver le filtre, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez l'option **Supprimer le filtre**.

La liste des journaux d'exécution des tâches reprend tous les journaux d'exécution des tâches.

Consultation des statistiques et des informations relatives à une tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution de la tâche

Les journaux d'exécution des tâches reprennent des informations détaillées sur tous les événements survenus dans ces tâches depuis leur lancement ainsi que les statistiques d'exécution des tâches et leurs paramètres.

Pour consulter les statistiques et les informations relatives à une tâche de Kaspersky Embedded Systems Security, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le volet résultats, ouvrez la fenêtre **Journaux** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le journal d'exécution de la tâche que vous souhaitez consulter.
   - Ouvrez le menu contextuel du journal d'exécution de la tâche que vous souhaitez consulter et choisissez l'option **Voir le journal**.
4. La fenêtre qui s'ouvre affiche les informations suivantes :
   - L'onglet **Statistiques** indique l'heure de lancement et de fin de la tâche et ses statistiques.
   - L'onglet **Événements** affiche une liste des événements consignés lors de l'exécution de la tâche.
   - L'onglet **Options** reprend les paramètres de la tâche.
5. Le cas échéant, cliquez sur le bouton **Filtrer** pour filtrer les événements dans le journal d'exécution de la tâche.
6. Le cas échéant, cliquez sur le bouton **Exporter** pour exporter les données du journal d'exécution de la tâche dans un fichier au format CSV ou TXT.
7. Cliquez sur le bouton **Fermer**.

La fenêtre **Journaux** se ferme.

Exportation des informations depuis le journal d'exécution de la tâche

Vous pouvez exporter les données contenues dans le journal d'exécution de la tâche dans un fichier au format CSV ou TXT.

Pour exporter les données du journal d'exécution de la tâche, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Dans le volet résultats, ouvrez la fenêtre **Journaux** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le journal d'exécution de la tâche que vous souhaitez consulter.
   - Ouvrez le menu contextuel du journal d'exécution de la tâche que vous souhaitez consulter et choisissez l'option **Voir le journal**.
4. Dans la partie inférieure de la fenêtre **Journaux**, cliquez sur le bouton **Exporter**.

   La fenêtre **Enregistrer sous** s'ouvre.
5. Indiquez le nom, l'emplacement et le type d'encodage dans lequel vous souhaitez exporter les informations du journal d'exécution de la tâche.
6. Cliquez sur le bouton **Enregistrer**.

Les paramètres définis seront enregistrés.

Suppression des journaux d'exécution des tâches

Par défaut, Kaspersky Embedded Systems Security conserve les enregistrements dans les journaux d'exécution des tâches pendant 30 jours à partir de la fin de la tâche. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches.

Vous pouvez supprimer manuellement les journaux d'exécution des tâches déjà terminées.

> Les événements des journaux des tâches en cours d'exécution et les journaux utilisés par d'autres utilisateurs ne seront pas supprimés.

Pour supprimer les journaux d'exécution des tâches :

1. Dans l'arborescence de la console de l'application, développez le nœud **Journaux et notifications**.
2. Choisissez l'entrée secondaire **Journaux d'exécution de la tâche**.
3. Exécutez une des actions suivantes :
   - Si vous souhaitez supprimer les journaux de toutes les tâches déjà terminées, ouvrez le menu contextuel du nœud enfant **Journaux d'exécution de la tâche** et choisissez l'option **Effacer**.
   - Si vous souhaitez effacer le journal d'une tâche distincte, ouvrez, dans le volet résultats, le menu contextuel du journal d'exécution de la tâche que vous souhaitez effacer, et choisissez **Supprimer**.
   - Si vous souhaitez effacer le contenu des journaux de plusieurs tâches, procédez comme suit :
     a. Dans le volet résultats, utilisez la touche **Ctrl** ou **Maj** pour sélectionner les journaux d'exécution des tâches que vous souhaitez supprimer.
     b. Ouvrez le menu contextuel de n'importe lequel des journaux d'exécution de la tâche sélectionnés et choisissez l'option **Supprimer**.

4. Dans la fenêtre de confirmation de la suppression, cliquez sur **Oui** afin de confirmer la suppression de la clé.

Les journaux d'exécution de la tâche sélectionnés seront effacés. La suppression des journaux d'exécution des tâches sera enregistrée dans le journal d'audit système.

Journaux de sécurité

Kaspersky Embedded Systems Security tient un journal des événement liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le périphérique protégé. Ce journal enregistre les événements suivants :

- Événements de Protection contre les exploits.
- Les événements critiques du composant Inspection des journaux.
- Les événements critiques qui indiquent une tentative de violation de la sécurité (pour les tâches Protection en temps réel de l'ordinateur, Analyse à la demande, Moniteur d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez effacer le contenu du journal de sécurité. De plus, Kaspersky Embedded Systems Security consigne un événement d'audit système quand les journaux de sécurité sont effacés.

Consultation du journal des événements de Kaspersky Embedded Systems Security dans l'observateur d'événements

Le composant logiciel enfichable Observateur d'événements pour Microsoft Management Console permet de consulter le journal des événements de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security y consigne les événements nécessaires au diagnostic des échecs de fonctionnement de l'application.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements selon les critères suivants :

- **selon le type d'événement**.
- **Selon le niveau de détail**. Le niveau de détail correspond au niveau d'importance des événements enregistrés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est le niveau Informatif qui enregistre tous les événements. Le niveau le moins détaillé est le niveau Critique qui enregistre uniquement les événements critiques.

Pour consulter les informations reprises dans le journal des événements de Kaspersky Embedded Systems Security.

1. Cliquez sur le bouton **Démarrer**, saisissez la commande `mmc` dans la barre de recherche, puis appuyez sur la touche **ENTER**.

   Microsoft Management Console s'ouvre.

2. Choisissez **Fichier** > **Ajouter ou supprimer un composant logiciel enfichable**.

   La fenêtre **Ajout et suppression de composants logiciels enfichables** s'ouvre.

3. Dans la liste des composants logiciels enfichables disponibles, sélectionnez **Observateur d'événements** et cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection d'ordinateur** s'ouvre.

4. Indiquez dans la fenêtre **Sélection d'ordinateur** le périphérique protégé sur lequel Kaspersky Embedded Systems Security est installé, puis cliquez sur le bouton **OK**.

5. Dans la fenêtre **Ajout et suppression de composants logiciels enfichables**, cliquez sur le bouton **OK**.

   Le nœud **Observateur d'événements** apparaît dans l'arborescence de Microsoft Management Console.

6. Développez le nœud **Observateur d'événements** et sélectionnez le nœud enfant **Journaux des applications et des services** > **Kaspersky Embedded Systems Security**.

Le journal des événements de Kaspersky Embedded Systems Security s'ouvre.

Configuration des paramètres des journaux via la Console de l'application

Vous pouvez modifier les paramètres suivants pour les journaux de Kaspersky Embedded Systems Security :

- Durée de la conservation des événements dans les journaux d'exécution des tâches et du journal d'audit système.
- Emplacement du dossier dans lequel Kaspersky Embedded Systems Security enregistre les fichiers des journaux d'exécution de la tâche et du journal d'audit système.
- Seuils de déclenchement des événements *Bases de l'application dépassées*, *Bases de l'application fortement dépassées* et *Analyse rapide non réalisée depuis longtemps*.
- Événements consignés par Kaspersky Embedded Systems Security dans les journaux d'exécution de la tâche, dans le journal d'audit système et dans le journal des événements de Kaspersky Embedded Systems Security dans la console Observateur d'événements.
- Paramètres de la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le serveur syslog.

Pour configurer les journaux de Kaspersky Embedded Systems Security, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications** et choisissez l'option **Propriétés**.

   La fenêtre **Paramètres des journaux et des notifications** s'ouvre.

2. Dans la fenêtre **Paramètres des journaux et des notifications**, configurez les journaux en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, sélectionnez, le cas échéant, les événements consignés par Kaspersky Embedded Systems Security dans les journaux d'exécution de la tâche, dans le journal d'audit système et dans le journal des événements de Kaspersky Embedded Systems Security dans la console Observateur d'événements. Pour ce faire, procédez comme suit :

     - Dans la liste **Composant**, sélectionnez le composant de Kaspersky Embedded Systems Security pour lequel vous souhaitez indiquer le niveau de détails.

Il est possible d'enregistrer les événements via les journaux d'exécution de la tâche et le journal des événements pour les composants Protection des fichiers en temps réel, Analyse à la demande et Mise à jour. Pour ces composants, le tableau de la liste des événements contient les colonnes **Journal d'exécution de la tâche** et **Journal des événements Windows**. Pour les composants Quarantaine et Sauvegarde, les événements sont enregistrés dans le journal d'audit système et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Audit** et **Journal des événements Windows**.

- La liste **Niveau d'importance** permet de sélectionner le niveau de détail des événements dans les journaux d'exécution des tâches, dans le journal d'audit système et dans le journal des événements pour le composant fonctionnel sélectionné.

  Le tableau de la liste des événements en dessous reprend des cases cochées en regard des événements consignés dans les journaux d'exécution de la tâche, le journal d'audit système et le journal des événements en fonction du niveau de détail sélectionné.

- Si vous souhaitez activer manuellement l'enregistrement d'événements distincts pour le module fonctionnel sélectionné, procédez comme suit :

a. Dans la liste **Niveau d'importance**, choisissez **Personnalisé**.

b. Dans le tableau de la liste des événements, cochez les cases en regard des événements dont vous souhaitez activer l'enregistrement dans les journaux d'exécution des tâches, le journal d'audit système et le journal des événements.

- Sous l'onglet **Avancé**, configurez les paramètres de stockage des journaux et les seuils de création des événements sur l'état de la protection du périphérique :
  - Dans la section **Stockage des journaux** :
    - **Dossier des journaux**
    - **Supprimer les journaux d'exécution de la tâche de plus de (jours)**
    - **Supprimer les événements du journal d'audit système de plus de (jours)**
  - Dans la section **Seuils de déclenchement des événements** :
    - Nombre de jours à l'issue desquels les événements *Bases de l'application dépassées*, *Bases de l'application fortement dépassées* et *Analyse rapide non réalisée depuis longtemps* sont déclenchés.
- Sous l'onglet **Intégration à SIEM**, configurez les paramètres de publication des événements d'audit et de performance des tâches sur le serveur syslog.

3. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

A propos de l'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des tailles des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il stocke et analyse les événements reçu et exécute d'autres actions de gestion de journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : dans ce mode, tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'appareil protégé même après avoir été envoyés au serveur SIEM.

  Nous conseillons l'utilisation de ce mode pour réduire autant que possible la charge sur l'appareil protégé.

- Supprimer les copies locales des événements : dans ce mode, tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans le serveur SIEM soient supprimés de l'appareil protégé.

  L'application ne supprime jamais les versions locales des Journaux de sécurité.

Kaspersky Embedded Systems Security peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus par le serveur SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Il est recommandé de choisir le format des événements d'après la configuration du serveur SIEM utilisé.

Paramètres de fiabilité

Vous pouvez réduire le risque d'erreur d'envoi des événements au serveur SIEM en indiquant les paramètres de connexion au serveur syslog de miroir.

Le serveur syslog de miroir est un serveur syslog complémentaire vers lequel l'application passe automatiquement si la connexion au serveur principal syslog ou son utilisation sont impossibles.

Kaspersky Embedded Systems Security utilise également les événements de l'audit système pour vous signaler les tentatives ratées de connexion au serveur SIEM ainsi que les erreurs survenues lors de l'envoi des événements au serveur SIEM.

Configuration des paramètres d'intégration à SIEM

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres pertinents (cf. tableau ci-dessous).

Paramètres d'intégration à SIEM

Paramètre	Valeur par défaut	Description
Envoyer les événements à un serveur syslog externe via le protocole syslog	Pas appliqué	Vous pouvez activer et désactiver l'intégration à SIEM en cochant ou décochant la case.
Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi au serveur SIEM en cochant ou décochant la case.
Format des événements	Données structurées	Vous pouvez choisir un de deux formats sous lesquels l'application convertit les événements avant de les envoyer

		au serveur syslog pour mieux les reconnaître au niveau du serveur SIEM.
Protocole de connexion	TCP	Vous pouvez configurer la connexion aux serveurs syslog principal et complémentaire via les protocoles UDP ou TCP à l'aide de la liste déroulante.
Paramètres de connexion au serveur syslog principal	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.
Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible	Pas appliqué	Vous pouvez activer et désactiver l'application du serveur syslog de miroir à l'aide de la case.
Paramètres de connexion au serveur syslog complémentaire	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog complémentaire à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.

Pour configurer les paramètres d'intégration à SIEM, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres des journaux et des notifications** s'ouvre.
3. Sélectionnez l'onglet **Intégration à SIEM**.
4. Dans la section **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.
5. Si besoin, dans la section **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe**.

   L'état de la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe** n'influence pas les paramètres de conservation des événements des Journaux de sécurité : l'application ne supprime jamais automatiquement les événement des Journaux de sécurité.
6. Dans la section **Format des événements**, indiquez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi au serveur SIEM.

   Par défaut, l'application exécute la conversion dans un format de données structurées.
7. Dans la section **Paramètres de connexion**, procédez comme suit :

   - Indiquez le protocole de connexion à SIEM.
   - Indiquez les paramètres de connexion au serveur syslog principal.

     Vous pouvez uniquement indiquer l'adresse IP au format IPv4.

- Cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si vous voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n'est pas possible.

  Définissez les paramètres suivants de connexion au serveur syslog de miroir : **Adresse** et **Port**.

  Les champs **Adresse** et **Port** pour le serveur syslog de miroir ne peuvent pas être modifiés si la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible** est décochée.

  Vous pouvez uniquement indiquer l'adresse IP au format IPv4.

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

   Les paramètres d'intégration à SIEM configurés seront appliqués.

Configuration des paramètres des journaux et des notifications via le plug-in d'administration

La Console d'administration de Kaspersky Security Center permet de configurer les notifications adressées à l'administrateur et aux utilisateurs relatives aux événements suivants liés à l'utilisation de Kaspersky Embedded Systems Security et à l'état de la protection antivirus du périphérique protégé :

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent le périphérique protégé et les utilisateurs de terminaux du périphérique protégé peuvent obtenir des informations sur les événements de type *Objet détecté*.

Vous pouvez configurer les notifications relatives aux événements de Kaspersky Embedded Systems Security pour un périphérique protégé dans la fenêtre **Propriétés :<nom du périphérique protégé>** ou pour un groupe de périphériques protégés dans la fenêtre **Propriétés : <nom de la stratégie>** du groupe d'administration sélectionné.

L'onglet **Notifications sur les événements** ou la fenêtre **Configuration des notifications** permettent de configurer les types de notification suivants :

- L'onglet **Notifications sur les événements** (onglet standard de Kaspersky Security Center) permet de configurer les notifications adressées à l'administrateur sur les événements de certains types. Pour en savoir plus sur les modes de notification, consultez *l'aide de Kaspersky Security Center*.
- La fenêtre **Configuration des notifications** permet de configurer les notifications pour l'administrateur et pour les utilisateurs.

Les notifications relatives aux événements de certains types peuvent être configurées uniquement sous l'onglet ou dans la fenêtre tandis que les notifications relatives à d'autres événements peuvent être configurées dans les deux.

Si vous configurez les notifications sur les événements d'un même type via une méthode identique sous l'onglet **Notifications sur les événements** et dans la fenêtre **Configuration des notifications**, l'administrateur système recevra les notifications relatives à ces événements via la méthode indiquée deux fois.

Configuration des paramètres des journaux d'exécution de la tâche

Pour configurer les journaux de Kaspersky Embedded Systems Security, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans la sous-section **Journaux d'exécution de la tâche**.
5. Dans la fenêtre **Paramètres des journaux**, configurez les paramètres suivants de Kaspersky Embedded Systems Security conformément à vos exigences :
   - Configurez le niveau de détail des événements dans les journaux. Pour ce faire, procédez comme suit :
     a. Dans la liste **Composant**, sélectionnez le composant de Kaspersky Embedded Systems Security pour lequel vous souhaitez indiquer le niveau de détails.
     b. Pour définir le niveau de détails dans les journaux d'exécution de la tâche et dans le journal d'audit système du composant sélectionné, choisissez le niveau dans la liste **Niveau d'importance**.
   - Pour modifier l'emplacement par défaut des journaux, indiquez le chemin d'accès complet au dossier ou cliquez sur le bouton **Parcourir**.
   - Indiquez la durée de conservation en jour des journaux d'exécution des tâches.
   - Indiquez le nombre de jours pendant lesquels les informations reprises dans le nœud **Journal d'audit système** seront conservées.
6. Cliquez sur le bouton **OK**.

Les paramètres des journaux configurés sont conservés.

Journaux de sécurité

Kaspersky Embedded Systems Security tient un journal des événement liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur le périphérique protégé. Ce journal enregistre les événements suivants :

- Événements de Protection contre les exploits.
- Les événements critiques du composant Inspection des journaux.
- Les événements critiques qui indiquent une tentative de violation de la sécurité (pour les tâches Protection en temps réel de l'ordinateur, Analyse à la demande, Moniteur d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez effacer le contenu du journal de sécurité. De plus, Kaspersky Embedded Systems Security consigne un événement d'audit système quand les journaux de sécurité sont effacés.

Configuration des paramètres d'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des tailles des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il stocke et analyse les événements reçu et exécute d'autres actions de gestion de journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : dans ce mode, tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'appareil protégé même après avoir été envoyés au serveur SIEM.

  Nous conseillons l'utilisation de ce mode pour réduire autant que possible la charge sur l'appareil protégé.

- Supprimer les copies locales des événements : dans ce mode, tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans le serveur SIEM soient supprimés de l'appareil protégé.

  L'application ne supprime jamais les versions locales des Journaux de sécurité.

Kaspersky Embedded Systems Security peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus par le serveur SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Pour réduire le risque d'un échec de la transmission des événements au serveur SIEM, vous pouvez définir les paramètres pour la connexion à un serveur syslog miroir.

Le serveur syslog de miroir est un serveur syslog complémentaire vers lequel l'application passe automatiquement si la connexion au serveur principal syslog ou son utilisation sont impossibles.

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres pertinents (cf. tableau ci-dessous).

Paramètres d'intégration à SIEM

Paramètre	Valeur par défaut	Description
Envoyer les événements à un serveur syslog externe via le protocole syslog	Pas appliqué	Vous pouvez activer et désactiver l'intégration à SIEM en cochant ou décochant la case.
Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi au serveur SIEM en cochant ou décochant la case.
Format des événements	Données structurées	Vous pouvez choisir un de deux formats sous lesquels l'application convertit les événements avant de les envoyer au serveur syslog pour mieux les reconnaître au niveau du serveur SIEM.
Protocole de connexion	TCP	Vous pouvez utiliser la liste déroulante pour configurer la

		connexion au serveur syslog principal via les protocoles UDP ou TCP et au serveur syslog miroir via le protocole TCP.
Paramètres de connexion au serveur syslog principal	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog principal à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.
Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible	Pas appliqué	Vous pouvez activer et désactiver l'application du serveur syslog de miroir à l'aide de la case.
Paramètres de connexion au serveur syslog complémentaire	Adresse IP : 127.0.0.1 Port : 514	Vous pouvez configurer les valeurs de l'adresse IP et du port de connexion au serveur syslog complémentaire à l'aide des champs correspondants. Vous pouvez indiquer la valeur de l'adresse IP uniquement au format IPv4.

Pour configurer les paramètres d'intégration à SIEM, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans la sous-section **Journaux d'exécution de la tâche**.

   La fenêtre **Paramètres des journaux et des notifications** s'ouvre.
5. Sélectionnez l'onglet **Intégration à SIEM**.
6. Dans la section **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.
7. Si besoin, dans la section **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe**.

   L'état de la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog externe** n'influence pas les paramètres de conservation des événements des Journaux de sécurité : l'application ne supprime jamais automatiquement les événement des Journaux de sécurité.

8. Dans la section **Format des événements**, indiquez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi au serveur SIEM.

   Par défaut, l'application exécute la conversion dans un format de données structurées.

9. Dans la section **Paramètres de connexion**, procédez comme suit :

   - Indiquez le protocole de connexion à SIEM.
   - Indiquez les paramètres de connexion au serveur syslog principal.

     Vous pouvez uniquement indiquer l'adresse IP au format IPv4.
   - Cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si vous voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n'est pas possible.

     Définissez les paramètres suivants de connexion au serveur syslog de miroir : **Adresse** et **Port**.

     Les champs **Adresse** et **Port** pour le serveur syslog de miroir ne peuvent pas être modifiés si la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible** est décochée.

     Vous pouvez uniquement indiquer l'adresse IP au format IPv4.

10. Cliquez sur le bouton **OK**.

Les paramètres d'intégration à SIEM configurés seront appliqués.

Configuration des paramètres des notifications

Pour configurer les notifications de Kaspersky Embedded Systems Security, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configuration** dans la sous-section **Notifications sur les événements**.
5. Dans la fenêtre **Configuration des notifications**, configurez les paramètres suivants de Kaspersky Embedded Systems Security conformément à vos exigences :

- Sélectionnez le type de notification dont vous souhaitez configurer les paramètres dans la liste **Configuration des notifications**.
- Configurez le mode de notification de l'utilisateur dans la section **Informer les utilisateurs**. Le cas échéant, rédigez le texte de la notification.
- Configurez le mode de notification de l'administration dans la section **Informer les administrateurs**. Le cas échéant, rédigez le texte de la notification. Le cas échéant, cliquez sur **Configuration** pour configurer les paramètres supplémentaires des notifications.
- Définissez dans la section **Seuils de déclenchement des événements** les intervalles à l'issue desquels Kaspersky Embedded Systems Security enregistre les événements *Bases de l'application dépassées*, *Bases de l'application fortement dépassées* et *Analyse rapide non réalisée depuis longtemps*.
  - **Les bases de l'application sont dépassées (jours)**
  - **Les bases de l'application sont fortement dépassées (jours)**
  - **Analyse rapide non réalisée depuis longtemps (jours)**

6. Cliquez sur le bouton **OK**.

Les paramètres de la notification définis seront enregistrés.

Configuration de l'interaction avec le Serveur d'administration

Pour sélectionner les types des objets au sujet desquels Kaspersky Embedded Systems Security va envoyer des informations au serveur d'administration de Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Cliquez sur le bouton **Configuration** dans le bloc **Interaction avec le serveur d'administration** de la section **Journaux et notifications**.

   La fenêtre **Listes réseau du Serveur d'administration** s'ouvre.

5. Dans la fenêtre **Listes réseau du Serveur d'administration**, choisissez les types d'objets au sujet desquels Kaspersky Embedded Systems Security va transmettre des informations au serveur d'administration de Kaspersky Security Center :

- Objets en quarantaine.
- Objets sauvegardés.

6. Cliquez sur le bouton **OK**.

   Kaspersky Embedded Systems Security transmet les informations relatives aux types d'objets choisis au Serveur d'administration.

Configuration des notifications

Cette section contient des informations sur les différentes méthodes de notification des utilisateurs et des administrateurs de Kaspersky Embedded Systems Security sur les événements de l'application et l'état de la protection du périphérique, ainsi que les instructions relatives à la configuration des notifications.

Moyens de notification de l'administrateur et des utilisateurs

Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent au périphérique sur les événements suivants liés au fonctionnement de Kaspersky Embedded Systems Security et à l'état de la protection antivirus du périphérique.

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent le périphérique protégé et les utilisateurs de terminaux du périphérique peuvent obtenir des informations sur les événements de type *Objet détecté* qui surviennent pendant la tâche Protection des fichiers en temps réel.

Dans la console de l'application, vous pouvez activer les notifications de l'administrateur ou des utilisateurs de plusieurs manières :

- Moyens de notification des utilisateurs :
  a. Outils des services des terminaux.

     Vous pouvez utiliser cette méthode pour la notification des utilisateurs de l'appareil protégé de terminal si l'appareil protégé est utilisé comme un terminal.

  b. Outils du service Windows Messenger.

     Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger.

- Moyens de notification des administrateurs :
  a. Outils du service Windows Messenger.

     Vous pouvez utiliser cette méthode pour la notification via le service Windows Messenger.

  b. Lancement du fichier exécutable.

     Cette méthode lance un fichier exécutable stocké sur le disque local de l'appareil protégé quand un événement se produit.

  c. Envoi par email.

     Ce mode permet l'envoi d'emails.

Vous pouvez rédiger le texte du message pour les types d'événement individuels. Ce texte peut contenir des champs avec les informations sur l'événement. Un message standard est utilisé par défaut pour les notifications des utilisateurs.

Configuration des notifications de l'administrateur et des utilisateurs

La configuration des notifications sur les événements porte sur le mode de notification et sur la composition du texte du message.

Pour configurer les paramètres de notification d'événements :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications** et choisissez l'option **Propriétés**.

   La fenêtre **Paramètres des journaux et des notifications** s'ouvre.

2. Sous l'onglet **Notifications**, indiquez les modes de notification :

   a. Dans la liste **Type d'événement**, sélectionnez les types d'événements.

   b. Dans le groupe de paramètres **Informer les administrateurs** ou **Informer les utilisateurs**, cochez la case en regard des modes de notification que vous souhaitez configurer.

   > Vous pouvez uniquement configurer les notifications des utilisateurs pour les événements : **Objet détecté**, **Périphérique externe douteux détecté et restreint** et **Session réseau ajoutée à la liste des sessions douteuses**.

3. Si vous souhaitez modifier le texte de la notification, procédez comme suit :

   a. Cliquez sur le bouton **Texte du message**.

   b. Dans la fenêtre qui s'ouvre, saisissez le texte qui sera affiché dans le message relatif à l'événement.

   > Vous pouvez créer le même message pour différents types d'événements : après voir choisi une méthode de notification pour un type d'événement, utiliser la touche **Ctrl** ou Maj pour sélectionner les autres types d'événements pour lesquels vous souhaitez utiliser le même message, puis cliquez sur le bouton Texte du message.

   a. Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Macro** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.

   b. Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Par défaut**.

4. Si vous souhaitez configurer les modes de notification de l'administrateur pour l'événement sélectionné, ouvrez l'onglet **Notifications**, cliquez sur le bouton **Configuration** dans la section **Informer les administrateurs** et procédez à la configuration des modes sélectionnés dans la fenêtre **Paramètres avancés**. Pour ce faire, procédez comme suit :

   a. Pour les notifications via email, ouvrez l'onglet **Email** et saisissez les adresses email des destinataires (séparez les adresses par un point-virgule), le nom ou l'adresse de réseau du serveur SMTP, ainsi que son port, dans les champs prévus à cet effet. Si nécessaire, indiquez le texte qui figurera dans les champs **Objet** et **De**. Le texte du champ **Objet** peut contenir des variables de champs d'informations (cf. tableau ci-dessous).

      Si vous souhaitez utiliser la vérification de l'authenticité selon le compte utilisateur lors de la connexion au serveur SMTP, il faudra dans ce cas cocher la case **Utiliser l'authentification SMTP** dans le groupe **Paramètres d'authentification** et saisir le nom et le mot de passe de l'utilisateur dont l'authenticité sera vérifiée.

   b. Pour les notifications via Service Windows Messenger, sous l'onglet **Service Windows Messenger**, composez la liste des périphériques protégés des destinataires des messages : pour chaque périphérique protégé que vous souhaitez ajouter, cliquez sur le bouton **Ajouter** et dans le champ, saisissez son nom de réseau.

c. Pour le lancement d'un fichier exécutable, sélectionnez le fichier sur le disque local du périphérique protégé qui sera exécuté sur le périphérique protégé lorsque l'événement se produira ou saisissez son chemin d'accès complet sous l'onglet **Fichier exécutable**. Saisissez le nom et le mot de passe de l'utilisateur sous le compte duquel le fichier sera exécuté.

En indiquant le chemin d'accès au fichier exécutable, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Si vous souhaitez limiter le nombre de messages de notification en fonction d'événements d'un même type par unité de temps, cochez la case **Ne pas envoyer la même notification plus de** sous l'onglet **Avancé** et indiquez le nombre de fois et un intervalle de temps.

5. Cliquez sur le bouton **OK**.

Les paramètres de la notification définis seront enregistrés.

Champs d'information sur les événements

Variable	Description
%EVENT_TYPE%	Type d'événements.
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%EVENT_SEVERITY%	Niveau d'importance de l'événement.
%OBJECT%	Nom de l'objet (dans les tâches Protection en temps réel de l'ordinateur et Analyse à la demande). Dans la tâche de mise à jour des modules de l'application, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.
%VIRUS_NAME%	Nom de l'objet détecté selon la classification de l'Encyclopédie des virus. Ce nom figure dans le nom complet de l'objet détecté que Kaspersky Embedded Systems Security renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
%VIRUS_TYPE%	Type de l'objet détecté selon la classification de Kaspersky, par exemple "virus" ou "cheval de Troie". Figure dans le nom complet de l'objet détecté renvoyé par Kaspersky Embedded Systems Security lorsque celui-ci considère l'objet comme infecté ou probablement infecté. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
%USER_COMPUTER%	Dans les tâches Protection des fichiers en temps réel, désigne le nom du périphérique protégé de l'utilisateur qui a accédé à l'objet sur le périphérique.
%USER_NAME%	Dans la tâche Protection des fichiers en temps réel, désigne le nom de l'utilisateur qui a sollicité l'objet sur le périphérique.
%FROM_COMPUTER%	Nom de l'appareil protégé d'où provient la notification
%EVENT_REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements).
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement "erreur interne de la tâche").
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)

Lancement et arrêt de Kaspersky Embedded Systems Security

Cette section fournit des informations sur le lancement de la console de l'application, ainsi que sur le lancement et l'arrêt du service Kaspersky Security.

Lancement et arrêt du plug-in Kaspersky Embedded Systems Security

Aucune action supplémentaire n'est requise pour lancer le plug-in Kaspersky Embedded Systems Security dans Kaspersky Security Center. Après l'installation du plug-in sur l'appareil protégé de l'administrateur, le lancement s'opère en même temps que le lancement de Kaspersky Security Center. Vous trouverez toutes les informations détaillées sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center.*

Lancement de la console de Kaspersky Embedded Systems Security depuis le menu Démarrer

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

*Pour démarrer la console de l'application depuis le menu **Démarrer** :*

1. Dans le menu **Démarrer**, sélectionnez **Programmes** > **Kaspersky Embedded Systems Security** > **Outils d'administration** > **Console de Kaspersky Embedded Systems Security**.

Pour ajouter d'autres composants logiciels enfichables à la console de l'application, lancez-la en mode auteur.

Pour démarrer la Console de l'application en mode auteur :

1. Dans le menu **Démarrer**, sélectionnez **Programmes** > **Kaspersky Embedded Systems Security** > **Outils d'administration**.
2. Dans le menu contextuel de la console de l'application, choisissez la commande **Auteur**.

   La console de l'application est lancée en mode auteur.

Si vous avez lancé la console de l'application sur l'appareil protégé, la fenêtre de la console de l'application s'ouvre.

Si vous avez lancé la console de l'application sur un appareil non protégé, connectez-la à l'appareil protégé.

Pour vous connecter à l'appareil protégé, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Sélectionnez la commande **Se connecter à un autre ordinateur**.

   La fenêtre **Sélection de l'appareil protégé** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez **Autre appareil**.
4. Dans le champ de saisie de droite, indiquez le nom réseau de l'appareil protégé.

5. Cliquez sur le bouton **OK**.

La console de l'application est connectée à l'appareil protégé.

Si le compte utilisateur employé pour accéder à Microsoft Windows ne dispose pas des privilèges d'accès au service Kaspersky Security Management sur l'appareil protégé, cochez la case **Se connecter sous le compte utilisateur** et indiquez un autre compte utilisateur qui dispose de tels privilèges.

Lancement et arrêt du service Kaspersky Security

Le Service Kaspersky Security est lancé automatiquement par défaut immédiatement après le démarrage du système d'exploitation. Le service Kaspersky Security gère les processus de travail chargés des tâches Protection en temps réel de l'ordinateur, Contrôle de l'ordinateur, Analyse à la demande et de la mise à jour.

Le lancement de Kaspersky Embedded Systems Security marque par défaut le lancement des tâches Protection des fichiers en temps réel et Analyse au démarrage du système d'exploitation ainsi que d'autres tâches dont la fréquence d'exécution est **Au lancement de l'application**.

Si vous arrêtez le Service Kaspersky Security, l'ensemble des tâches en cours d'exécution sera interrompu. Après que vous avez relancé le service Kaspersky Security, l'application lance automatiquement uniquement les tâches dont la planification correspond à **Au lancement de l'application**, les autres tâches doivent être lancées manuellement.

Vous pouvez lancer et arrêter le service Kaspersky Security à l'aide du menu contextuel du nœud **Kaspersky Embedded Systems Security** ou via le composant logiciel enfichable Microsoft Windows Services.

Vous pouvez lancer et arrêter Kaspersky Embedded Systems Security uniquement si vous faites partie du groupe d'administrateurs sur le périphérique protégé.

Pour arrêter ou lancer l'application via la console de l'application :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Choisissez une des commandes suivantes :
   - **Arrêter le service**.
   - **Démarrer le service**.

Le Service Kaspersky Security sera lancé ou arrêté.

Lancement des composants Kaspersky Embedded Systems Security en mode sans échec du système d'exploitation

Cette section fournit des informations sur l'utilisation de Kaspersky Embedded Systems Security en mode sans échec.

A propos du fonctionnement de Kaspersky Embedded Systems Security en mode sans échec

Les composants de Kaspersky Embedded Systems Security peuvent être lancés quand le système d'exploitation démarre en mode sans échec. Outre le service Kaspersky Security (kavfs.exe), le pilote klam.sys est chargé. Il permet d'enregistrer le service Kaspersky Security en tant que service protégé lors du lancement du système d'exploitation. Pour en savoir plus, cf. section Enregistrement du Service Kaspersky Security comme service protégé.

Kaspersky Embedded Systems Security peut être lancé dans les modes sans échec suivants du système d'exploitation :

- Mode sans échec minimal – ce mode est lancé lorsque l'option standard du mode sans échec du système d'exploitation est sélectionnée. Dans ce cas, Kaspersky Embedded Systems Security peut démarrer les composants suivants :
  - Protection des fichiers en temps réel.
  - Analyse à la demande.
  - Contrôle du lancement des applications et Génération des règles du Contrôle du lancement des applications.
  - Inspection des journaux.
  - Moniteur d'intégrité des fichiers.
  - Surveillance de l'intégrité des fichiers.
  - Vérification de l'intégrité de l'application.

Réseau mode sans échec : ce mode est lancé lorsque le système d'exploitation est chargé en mode sans échec avec les pilotes réseau. Outre les composants chargés en mode sans échec minime, Kaspersky Embedded Systems Security peut lancer les composants suivants dans ce mode :

- Mise à jour des bases de l'application.
- Mise à jour des modules de l'application.

Lancement de Kaspersky Embedded Systems Security en mode sans échec

Par défaut, Kaspersky Embedded Systems Security n'est pas lancé quand le système d'exploitation démarre en mode sans échec.

Pour lancer Kaspersky Embedded Systems Security en mode sans échec :

1. Démarrez l'éditeur de registre Windows (C:\Windows\regedit.exe).
2. Ouvrez la clé du registre du système [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].

3. Ouvrez le paramètre LoadInSafeMode.

4. Attribuez la valeur `1`.

5. Cliquez sur le bouton **OK**.

Pour annuler le démarrage de Kaspersky Embedded Systems Security en mode sans échec du système d'exploitation :

1. Démarrez l'éditeur de registre Windows (C:\Windows\regedit.exe).

2. Ouvrez la clé du registre du système [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].

3. Ouvrez le paramètre LoadInSafeMode.

4. Attribuez la valeur `0`.

5. Cliquez sur le bouton **OK**.

Auto-défense de Kaspersky Embedded Systems Security

Cette section contient des informations sur les mécanismes d'auto-défense de Kaspersky Embedded Systems Security.

A propos de l'auto-défense de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security inclut des mécanismes d'auto-défense qui protègent l'application contre la modification ou la suppression de ses dossiers, des processus de mémoire et des entrées du registre du système.

Protection contre les modifications des dossiers contenant les composants de Kaspersky Embedded Systems Security installés

Kaspersky Embedded Systems Security bloque le renommage et la suppression des dossiers contenant les composants de l'application installés pour n'importe quel compte utilisateur. Par défaut, les chemins d'accès aux dossiers d'installation de l'application sont les suivants :

- Sur la version 32 bits de Microsoft Windows : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Sur la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Protection contre les modifications des clés de registre de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security limite l'accès aux branches et clés de registre qui permettent le chargement des pilotes et des services de l'application :

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\CrashDump]

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2] (sur la version 64 bits de Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\Trace]

Les droits de modification de ces branches et clés de registre sont accordés uniquement au compte Local System (SYSTEM). Les comptes Utilisateur et Administrateur se voient accorder des droits de lecture seule.

Protection contre les modifications de la mémoire des parties service de l'application

Pour protéger les parties service du programme contre les processus tiers, les pilotes de Kaspersky Embedded Systems Security restreignent l'accès aux fichiers exécutables suivants :

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

Par défaut, l'accès à la mémoire des composants de Kaspersky Embedded Systems Security est limité pour les processus tiers.

Vous pouvez activer les fonctions d'autodéfense dans les propriétés de la stratégie de la Console de Kaspersky Embedded Systems Security et du plug-in Kaspersky Embedded Systems Security.

Enregistrement du service Kaspersky Security

La technologie *Protected Process Light* (également appelée "PPL") fait en sorte que le système d'exploitation charge uniquement les services et les processus de confiance. Pour qu'un service puisse fonctionner comme un périphérique protégé, un pilote *à lancement anticipé anti-application malveillante* doit être installé sur le périphérique protégé.

Un pilote *à lancement anticipé anti-application malveillante* (également appelé "ELAM") fournit une protection aux périphériques de votre réseau lors de leur démarrage et avant l'initialisation des pilotes tiers.

Le pilote ELAM est automatiquement installé lors de l'installation de Kaspersky Embedded Systems Security et sert à enregistrer le service Kaspersky Security comme PPL lors du démarrage du système d'exploitation. Lorsque le service Kaspersky Security (KAVFS) est démarré en tant que processus protégé par le système, d'autres processus non protégés sur le système ne peuvent pas injecter de threads, écrire dans la mémoire virtuelle du processus protégé ou arrêter le service.

Quand un processus est lancé en tant que PPL, l'utilisateur ne peut pas l'administrer en ignorant les autorisations qu'il lui ont été attribuées. L'enregistrement du Service Kaspersky Security comme PPL avec le pilote ELAM est prise en charge sur les systèmes d'exploitation Microsoft Windows 10 et plus. Si vous installez Kaspersky Embedded Systems Security sur un serveur tournant sous un système d'exploitation compatible avec PPL, l'administration des autorisations pour le service Kaspersky Security (KAVFS) ne sera pas disponible.

Pour installer Kaspersky Embedded Systems Security en tant que PPL, exécutez la commande suivante :

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Gestion des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Embedded Systems Security et des services d'exploitation enregistrés par l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

A propos des autorisations d'administration de Kaspersky Embedded Systems Security

Par défaut, l'accès à toutes les fonctions de Kaspersky Embedded Systems Security est octroyé aux utilisateurs du groupe Administrateurs sur le périphérique protégé et aux utilisateurs du groupe Administrateurs ESS créé sur le périphérique protégé lors de l'installation de Kaspersky Embedded Systems Security et aussi au groupe SYSTEM.

Les utilisateurs qui ont accès à la fonction Modifier les privilèges de Kaspersky Embedded Systems Security peuvent offrir l'accès aux fonctions de Kaspersky Embedded Systems Security aux autres utilisateurs enregistrés sur le périphérique protégé ou repris dans le domaine.

Si l'utilisateur ne figure pas dans la liste des utilisateurs de Kaspersky Embedded Systems Security, il ne pourra pas ouvrir la Console de l'application.

Vous pouvez attribuer à l'utilisateur ou au groupe d'utilisateurs un des niveaux prédéfinis d'accès suivants :

- **Contrôle complet** : accès à toutes les fonctions de l'application : consultation et modification des paramètres généraux de Kaspersky Embedded Systems Security, des paramètres des composants et des autorisations des utilisateurs de Kaspersky Embedded Systems Security ainsi que la consultation des statistiques de Kaspersky Embedded Systems Security.
- **Modifier** : accès à l'ensemble des fonctions de l'application, sauf la modification des autorisations des utilisateurs : possibilité de consulter et de modifier les paramètres généraux et les paramètres des modules Kaspersky Embedded Systems Security.
- **Lire** : consultation des paramètres généraux de Kaspersky Embedded Systems Security, des paramètres des composants de Kaspersky Embedded Systems Security, des statistiques de Kaspersky Embedded Systems Security et des autorisations d'utilisateur de Kaspersky Embedded Systems Security.

Vous pouvez également configurer les autorisations d'accès avancées : autoriser ou interdire l'accès aux fonctions spécifiques de Kaspersky Embedded Systems Security.

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

A propos des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security

Autorisations d'accès	Description
Administration des tâches	Lancement/arrêt/suspension/reprise d'une tâche de Kaspersky Embedded Systems Security.
Création et suppression des tâches Analyse à la demande	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilités :

	• Importation des paramètres de Kaspersky Embedded Systems Security depuis un fichier de configuration. • Modifiez les paramètres de l'application.
Lire les paramètres	Possibilités : • Consultation des paramètres généraux de Kaspersky Embedded Systems Security et des paramètres des tâches. • Exportation des paramètres de Kaspersky Embedded Systems Security vers un fichier de configuration. • Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Gérer les référentiels	Possibilités : • Placement d'objets en quarantaine ; • Suppression d'objets de la quarantaine et de la Sauvegarde ; • Restauration d'objets de la quarantaine et de la Sauvegarde.
Administration des journaux	Suppression des journaux d'exécution des tâches et purge du journal d'audit système.
Lecture des journaux	Possibilité de consulter les événements dans les journaux d'exécution des tâches et le journal d'audit système.
Consultation des statistiques	Consultation des statistiques de chacune des tâches de Kaspersky Embedded Systems Security.
Licence de l'application	Fonction d'activation de Kaspersky Embedded Systems Security.
Suppression de l'application	Fonction de désinstallation de Kaspersky Embedded Systems Security.
Lecture des privilèges	Possibilité de consulter la liste des utilisateurs de Kaspersky Embedded Systems Security et des privilèges d'accès de ceux-ci.
Modification des privilèges	Possibilités : • Modifier la liste des utilisateurs qui ont accès à l'administration de l'application ; • Modification des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security.

A propos des autorisations d'administration des services enregistrés

Lors de l'installation, Kaspersky Embedded Systems Security enregistre sous Windows le service Kaspersky Security (KAVFS) et le service Kaspersky Security Management (KAVFSGT), ainsi que la protection contre les exploits de Kaspersky Security (KAVFSSLP).

L'enregistrement du service Kaspersky Security comme Protected Process Light (PPL) avec le pilote ELAM est pris en charge sur les systèmes d'exploitation Microsoft Windows 10 et suivants. Quand un processus est lancé en tant que PPL, l'utilisateur ne peut pas l'administrer, quelles que soient les autorisations qu'il possède. Si vous installez Kaspersky Embedded Systems Security sur un périphérique protégé doté d'un système d'exploitation qui prend en charge PPL, l'administration des autorisations ne sera pas disponible pour le service Kaspersky Security (KAVFS).

Service Kaspersky Security Service

Par défaut, l'accès à l'administration du Service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe "Administrateurs" de l'appareil protégé, ainsi qu'aux groupes système SERVICE et INTERACTIVE avec autorisation de lecture et au groupe système SYSTEM avec autorisation de lecture et d'exécution.

Les utilisateurs qui disposent d'un accès aux fonctions du niveau Modifier les privilèges peuvent octroyer l'accès à l'administration du Service Kaspersky Security à d'autres utilisateurs enregistrés sur l'ordinateur protégé ou appartenant au domaine.

Service Kaspersky Security Management

Pour administrer l'application via la Console de l'application installée sur un autre serveur, il faut que le compte sous les autorisations duquel la connexion à Kaspersky Embedded Systems Security s'opère possède un accès complet au service Kaspersky Security Management sur le périphérique protégé.

Par défaut, l'accès au service Kaspersky Security Management est octroyé aux utilisateurs du groupe Administrateurs sur le périphérique protégé et aux utilisateurs du groupe Administrateurs ESS créé sur le périphérique protégé lors de l'installation de Kaspersky Embedded Systems Security.

Vous pouvez administrer le Service Kaspersky Security Management uniquement via le composant logiciel enfichable Services de Microsoft Windows.

Protection contre les exploits de Kaspersky Security

Par défaut, l'accès à l'administration du service Kaspersky Security Exploit Prevention est octroyé aux utilisateurs qui appartiennent au groupe Administrateurs de l'appareil protégé, ainsi qu'au groupe SYSTEM avec autorisation de lecture et d'exécution.

A propos des autorisations d'accès au Service Kaspersky Security Management

Vous pouvez passer en revue la liste des services de Kaspersky Embedded Systems Security.

Lors de l'installation, Kaspersky Embedded Systems Security enregistre le Service Kaspersky Security Management (KAVFSGT). Pour administrer l'application via la Console de l'application installée sur un autre périphérique protégé, le compte utilisé pour la connexion à Kaspersky Embedded Systems Security doit posséder un accès complet au service Kaspersky Security Management sur le périphérique protégé.

Par défaut, l'accès au service Kaspersky Security Management est octroyé aux utilisateurs du groupe Administrateurs sur le périphérique protégé et aux utilisateurs du groupe Administrateurs ESS créé sur le périphérique protégé lors de l'installation de Kaspersky Embedded Systems Security.

Vous pouvez administrer le Service Kaspersky Security Management uniquement via le composant logiciel enfichable Services de Microsoft Windows.

Il est impossible d'autoriser ou d'interdire l'accès de l'utilisateur au Service Kaspersky Security Management en configurant Kaspersky Embedded Systems Security.

Vous pouvez vous connecter à Kaspersky Embedded Systems Security sous un compte utilisateur local si un compte utilisateur avec le même nom d'utilisateur et le même mot de passe est enregistré sur le périphérique protégé.

A propos des autorisations d'administration du Service Kaspersky Security

Lors de l'installation, Kaspersky Embedded Systems Security enregistre le Service Kaspersky Security (KAVFS) dans Windows et autorise en interne les composants fonctionnels démarrés au lancement du système d'exploitation. Pour réduire le risque d'accès d'un tiers aux fonctions de l'application et aux paramètres de sécurité sur un périphérique protégé via l'administration du Service Kaspersky Security, vous pouvez limiter les autorisations d'administration du service Kaspersky Security depuis la console de l'application ou depuis le plug-in d'administration.

Par défaut, l'accès à l'administration du Service Kaspersky Security est octroyé aux utilisateurs qui appartiennent au groupe Administrateurs du périphérique protégé. L'accès en lecture est octroyé aux groupes SERVICE et INTERACTIVE ; l'accès en lecture et en exécution est octroyé au groupe SYSTEM.

Il est impossible de supprimer le compte utilisateur SYSTEM ou de modifier les autorisations de ce compte. Si les autorisations du compte SYSTEM sont modifiées, les autorisations maximales sont rétablies pour ce compte lors de l'enregistrement des modifications.

Les utilisateurs qui disposent d'un accès aux fonctions qui requièrent Modifier les privilèges peuvent octroyer l'accès à l'administration du Service Kaspersky Security à d'autres utilisateurs enregistrés sur le périphérique protégé ou appartenant au domaine.

Vous pouvez attribuer à l'utilisateur ou à un groupe d'utilisateurs de Kaspersky Embedded Systems Security un des niveaux prédéfinis d'autorisation pour administrer le Service Kaspersky Security :

- **Contrôle complet** : consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs, ainsi lancement et arrêt du Service Kaspersky Security.
- **Lire** : consultation des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
- **Modifier** : consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
- **Exécution** : lancement et arrêt du fonctionnement du service Kaspersky Security.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès : autoriser ou interdire l'accès à des fonctions particulières de Kaspersky Embedded Systems Security (voir tableau ci-dessous).

Si vous avez configuré manuellement les autorisations d'accès pour l'utilisateur ou le groupe, cet utilisateur ou ce groupe bénéficiera du niveau d'accès **Autorisations spéciales**.

Autorisations d'accès aux fonctions du Service Kaspersky Security

Fonction	Description
Affichage des paramètres du service	Possibilité d'afficher les paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
Solliciter l'état du service auprès du Gestionnaire de contrôle des services	Interrogation sur l'état d'exécution du Service Kaspersky Security dans le gestionnaire de services de Microsoft Windows.
Interrogation du service sur son état	Interrogation du Service Kaspersky Security sur l'état de l'exécution du service.
Lire la liste des services dépendants	Possibilité d'afficher la liste des services dont dépend le Service Kaspersky Security ainsi et qui dépendent du Service Kaspersky Security.
Modification des paramètres du service	Consultation et modification des paramètres généraux de fonctionnement du Service Kaspersky Security et des autorisations des utilisateurs.
Lancer le service	Exécution du service Kaspersky Security.
Arrêter le service	Arrêt du service Kaspersky Security.
Suspension/reprise du service	Suspension et reprise de l'exécution du service Kaspersky Security.
Lecture des privilèges	Consultation de la liste des utilisateurs du service Kaspersky Security et des privilèges d'accès de chacun d'entre eux.
Modification des privilèges	Possibilités : • Ajout et suppression d'utilisateurs du Service Kaspersky Security ; • Modification des autorisations d'accès des utilisateurs au service Kaspersky Security.
Suppression du service	Annulation de l'enregistrement du Service Kaspersky Security dans le Gestionnaire de service de Microsoft Windows.
Interrogations personnalisées adressées au service	Création et envoi d'interrogations personnalisées adressées au service Kaspersky Security.

Administration des autorisations d'accès via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres d'accès pour un seul ou pour l'ensemble des appareils protégés du réseau.

Configuration des autorisations d'accès à Kaspersky Embedded Systems Security et au service Kaspersky Security

Vous pouvez modifier la liste d'utilisateurs et de groupes d'utilisateurs autorisés à accéder aux fonctions de Kaspersky Embedded Systems Security et à administrer le Service Kaspersky Security. Vous pouvez également modifier les autorisations d'accès de ces utilisateurs et groupes d'utilisateurs.

Pour ajouter un utilisateur ou un groupe à la liste ou pour l'en supprimer, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Complémentaire**, exécutez une des étapes suivantes :
   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs autorisés à l'administrer les fonctions de Kaspersky Embedded Systems Security.
   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du Service Kaspersky Security.

     La fenêtre de groupe **Autorisations pourKaspersky Embedded Systems Security 3.2** s'ouvre.
5. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Pour ajouter un utilisateur ou un groupe à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez accorder des privilèges.
   - Pour supprimer un utilisateur ou un groupe de la liste, sélectionnez l'utilisateur ou le groupe dont vous souhaitez restreindre l'accès et cliquez sur le bouton **Supprimer**.
6. Cliquez sur le bouton **Appliquer**.

Les utilisateurs (ou groupes) sélectionnés seront ajoutés ou supprimés.

Pour modifier les autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security par un utilisateur ou un groupe d'utilisateurs, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Complémentaire**, exécutez une des étapes suivantes :

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs autorisés à l'administrer les fonctions de Kaspersky Embedded Systems Security.

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du Service Kaspersky Security.

     La fenêtre de groupe **Autorisations pour Kaspersky Embedded Systems Security** s'ouvre.

5. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste **Groupes ou noms d'utilisateurs** l'utilisateur ou le groupe d'utilisateurs pour lequel vous souhaitez modifier les autorisations.

6. Dans la section **Autorisation pour <Utilisateur (Groupe)>**, cochez les cases **Autoriser** ou **Interdire** pour les niveaux d'accès suivants :

   - **Contrôle complet** : sélection complète des autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security.

   - **Lire** :

     - Autorisations suivantes sur l'administration de Kaspersky Embedded Systems Security : **Récupérer les statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lire les autorisations**.

     - Les autorisations d'administration suivantes pour le service Kaspersky Security : **Lire les paramètres du service**, **Solliciter l'état auprès du Gestionnaire de contrôle des services**, **Solliciter le statut auprès du service**, **Lire la liste des services dépendants**, **Lire les autorisations**.

   - **Modifier** :

     - Toutes les autorisations d'administration de Kaspersky Embedded Systems Security, à l'exception de **Modifier les autorisations**.

     - Les autorisations d'administration suivantes pour le service Kaspersky Security : **Modifier les paramètres du service**, **Lire les autorisations**.

   - **Autorisations spéciales** : les autorisations suivantes pour administrer le service Kaspersky Security : **Lancement du service**, **Arrêter le service**, **Suspension/reprise du service**, **Lire les autorisations** ,

Requêtes de l'utilisateur au service.

7. Si vous souhaitez réaliser une configuration étendue des autorisations pour un utilisateur ou un groupe d'utilisateurs (**Autorisations spéciales**), cliquez sur le bouton **Avancé**.

   a. Dans la fenêtre **Paramètres de sécurité avancésKaspersky Embedded Systems Security** qui s'ouvre, sélectionnez l'utilisateur ou le groupe souhaité.

   b. Cliquez sur le bouton **Modifier**.

   c. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).

   d. Cochez les cases en regard des fonctions pour lesquelles vous souhaitez octroyer ou non un accès à un utilisateur ou un groupe d'utilisateurs sélectionnés.

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

   f. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Embedded Systems Security** cliquez sur **OK**.

8. Dans la fenêtre de groupe **Autorisations pour Kaspersky Embedded Systems Security**, cliquez sur le bouton **Appliquer**.

Les autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security configurées sont enregistrées.

Accès protégé par mot de passe aux fonctions de Kaspersky Embedded Systems Security

Vous pouvez limiter l'accès à l'administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs. Vous pouvez renforcer la protection des opérations critiques grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security requiert alors la saisie du mot de passe lors des tentatives d'accès aux fonctions suivantes de l'application :

- connexion à la Console de l'application ;
- désinstallation de Kaspersky Embedded Systems Security ;
- modification des composants de Kaspersky Embedded Systems Security ;
- exécution des commandes de la ligne de commande.

L'interface de Kaspersky Embedded Systems Security masque le mot de passe désigné à l'écran. Kaspersky Embedded Systems Security conserve le mot de passe spécifié sous la forme d'une somme de contrôle calculée à la saisie du mot de passe.

Kaspersky Embedded Systems Security ne vérifie pas la sécurité du mot de passe et ne bloque pas la saisie du mot de passe après plusieurs tentatives infructueuses.

Lors de la création d'un mot de passe, il est recommandé de respecter les conditions suivantes :

- Le mot de passe ne contient pas le nom du compte ou le nom de l'ordinateur.
- Le mot de passe comporte au moins 8 caractères.
- Le mot de passe contient des caractères appartenant à au moins trois des catégories suivantes :
  - lettres latines majuscules (A à Z) ;
  - lettres latines minuscules (a à z) ;
  - chiffres (0 à 9) ;
  - symboles du point d'exclamation (!), du signe dollar ($), du signe dièse (#) et du signe de pourcentage (%).

Vous pouvez exporter et importer les paramètres d'une application protégée par un mot de passe. Un fichier de configuration obtenu après l'exportation des paramètres de l'application protégée contient la valeur de la somme de contrôle du mot de passe et la valeur du modificateur utilisé pour l'extension de la ligne du mot de passe.

Ne modifiez pas la valeur de la somme de contrôle ou du modificateur dans le fichier de configuration. L'importation d'une configuration protégée par mot de passe qui a été modifiée manuellement peut entraîner le blocage complet de l'accès à l'application.

Pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security :

1. Dans l'arborescence de la console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**. Sélectionnez le groupe d'administration reprenant les appareils protégés pour lesquels vous souhaitez configurer les paramètres de l'application.
2. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de stratégie pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégie** et ouvrez les propriétés de **<Nom de la stratégie>** via le menu contextuel.
   - Si vous souhaitez configurer les paramètres de l'application pour un seul appareil protégé, ouvrez les paramètres requis dans la fenêtre **Paramètres de l'application** de Kaspersky Security Center.
3. Dans la section **Sécurité et fiabilité** de l'onglet **Paramètres de l'application**, cliquez sur le bouton **Configuration**.

   La fenêtre **Paramètres de sécurité** s'ouvre.
4. Dans la section **Paramètres de protection par mot de passe**, cochez la case **Utiliser la protection par mot de passe**.

   Les champs **Mot de passe** et **Confirmer mot de passe** deviennent actifs.
5. Saisissez dans le champ **Mot de passe** le mot de passe que vous voulez utiliser pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security.
6. Dans le champ **Confirmer mot de passe**, saisissez à nouveau le mot de passe.
7. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés. Kaspersky Embedded Systems Security demandera le mot de passe défini pour octroyer l'accès aux fonctions protégées.

Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pourrez plus contrôler l'application. Il devient également impossible de désinstaller l'application depuis l'appareil protégé.

Il est possible de réinitialiser le mot de passe à tout moment. Pour ce faire, décochez la case **Utiliser la protection par mot de passe** et enregistrez les modifications. La protection par mot de passe est désactivée et la somme de contrôle de l'ancien mot de passe est supprimée. Répétez le processus de création du mot de passe avec un nouveau mot de passe.

Administration des autorisations d'accès via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration autorisations d'accès sur un appareil protégé.

Configuration des autorisations d'accès à l'administration de Kaspersky Embedded Systems Security et au Service Kaspersky Security

Vous pouvez modifier la liste d'utilisateurs et de groupes d'utilisateurs autorisés à accéder aux fonctions de Kaspersky Embedded Systems Security et à administrer le Service Kaspersky Security. Vous pouvez également modifier les autorisations d'accès de ces utilisateurs et groupes d'utilisateurs.

Pour ajouter un utilisateur ou un groupe à la liste ou pour l'en supprimer, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Complémentaire**, exécutez une des étapes suivantes :
   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs autorisés à l'administrer les fonctions de Kaspersky Embedded Systems Security.
   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration de l'application à l'aide du Service Kaspersky Security.

     La fenêtre de groupe **Autorisations pourKaspersky Embedded Systems Security 3.2** s'ouvre.

5. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

   - Pour ajouter un utilisateur ou un groupe à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez accorder des privilèges.

   - Pour supprimer un utilisateur ou un groupe de la liste, sélectionnez l'utilisateur ou le groupe dont vous souhaitez restreindre l'accès et cliquez sur le bouton **Supprimer**.

6. Cliquez sur le bouton **Appliquer**.

Les utilisateurs (ou groupes) sélectionnés seront ajoutés ou supprimés.

Pour modifier les autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security pour un utilisateur ou un groupe :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Complémentaire**, exécutez une des étapes suivantes :

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs autorisés à l'administrer les fonctions de Kaspersky Embedded Systems Security.

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du Service Kaspersky Security.

     La fenêtre de groupe **Autorisations pour Kaspersky Embedded Systems Security** s'ouvre.

5. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste **Groupes ou noms d'utilisateurs** l'utilisateur ou le groupe d'utilisateurs pour lequel vous souhaitez modifier les autorisations.

6. Dans la section **Autorisation pour <Utilisateur (Groupe)>**, cochez les cases **Autoriser** ou **Interdire** pour les niveaux d'accès suivants :

   - **Contrôle complet** : sélection complète des autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security.

   - **Lire** :

     - Autorisations suivantes sur l'administration de Kaspersky Embedded Systems Security : **Récupérer les statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lire les autorisations**.

- Les autorisations d'administration suivantes pour le service Kaspersky Security : **Lire les paramètres du service**, **Solliciter l'état auprès du Gestionnaire de contrôle des services**, **Solliciter le statut auprès du service**, **Lire la liste des services dépendants**, **Lire les autorisations**.

- **Modifier** :

  - Toutes les autorisations d'administration de Kaspersky Embedded Systems Security, à l'exception de **Modifier les autorisations**.

  - Les autorisations d'administration suivantes pour le service Kaspersky Security : **Modifier les paramètres du service**, **Lire les autorisations**.

- **Autorisations spéciales** : les autorisations suivantes pour administrer le service Kaspersky Security : **Lancement du service**, **Arrêter le service**, **Suspension/reprise du service**, **Lire les autorisations** , **Requêtes de l'utilisateur au service**.

7. Si vous souhaitez réaliser une configuration étendue des autorisations pour un utilisateur ou un groupe d'utilisateurs (**Autorisations spéciales**), cliquez sur le bouton **Avancé**.

   a. Dans la fenêtre **Paramètres de sécurité avancésKaspersky Embedded Systems Security** qui s'ouvre, sélectionnez l'utilisateur ou le groupe souhaité.

   b. Cliquez sur le bouton **Modifier**.

   c. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).

   d. Cochez les cases en regard des fonctions pour lesquelles vous souhaitez octroyer ou non un accès à un utilisateur ou un groupe d'utilisateurs sélectionnés.

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

   f. Dans la fenêtre **Paramètres de sécurité avancés pour Kaspersky Embedded Systems Security** cliquez sur **OK**.

8. Dans la fenêtre de groupe **Autorisations pour Kaspersky Embedded Systems Security**, cliquez sur le bouton **Appliquer**.

9. Les autorisations d'administration de Kaspersky Embedded Systems Security ou du Service Kaspersky Security configurées sont enregistrées.

Accès protégé par mot de passe aux fonctions de Kaspersky Embedded Systems Security

Vous pouvez limiter l'accès à l'administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs. Vous pouvez renforcer la protection des opérations critiques grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security requiert alors la saisie du mot de passe lors des tentatives d'accès aux fonctions suivantes de l'application :

- connexion à la Console de l'application ;

- désinstallation de Kaspersky Embedded Systems Security ;

- modification des composants de Kaspersky Embedded Systems Security ;
- exécution des commandes de la ligne de commande.

L'interface de Kaspersky Embedded Systems Security masque le mot de passe désigné à l'écran. Kaspersky Embedded Systems Security conserve le mot de passe spécifié sous la forme d'une somme de contrôle calculée à la saisie du mot de passe.

Kaspersky Embedded Systems Security ne vérifie pas la sécurité du mot de passe et ne bloque pas la saisie du mot de passe après plusieurs tentatives infructueuses.

Lors de la création d'un mot de passe, il est recommandé de respecter les conditions suivantes :

- Le mot de passe ne contient pas le nom du compte ou le nom de l'ordinateur.
- Le mot de passe comporte au moins 8 caractères.
- Le mot de passe contient des caractères appartenant à au moins trois des catégories suivantes :
  - lettres latines majuscules (A à Z) ;
  - lettres latines minuscules (a à z) ;
  - chiffres (0 à 9) ;
  - symboles du point d'exclamation (!), du signe dollar ($), du signe dièse (#) et du signe de pourcentage (%).

Vous pouvez exporter et importer les paramètres d'une application protégée par un mot de passe. Un fichier de configuration obtenu après l'exportation des paramètres de l'application protégée contient la valeur de la somme de contrôle du mot de passe et la valeur du modificateur utilisé pour l'extension de la ligne du mot de passe.

Ne modifiez pas la valeur de la somme de contrôle ou du modificateur dans le fichier de configuration. L'importation d'une configuration protégée par mot de passe qui a été modifiée manuellement peut entraîner le blocage complet de l'accès à l'application.

Pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security :

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et réalisez l'une des actions suivantes :
   - Dans le volet résultats du nœud, suivez le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application** s'ouvre.
2. Sous l'onglet **Sécurité et fiabilité** de la section **Paramètres de protection par mot de passe**, cochez la case **Utiliser la protection par mot de passe**.

   Les champs **Mot de passe** et **Confirmer mot de passe** deviennent actifs.
3. Saisissez dans le champ **Mot de passe** le mot de passe que vous voulez utiliser pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security.

4. Dans le champ **Confirmer mot de passe**, saisissez à nouveau le mot de passe.

5. Cliquez sur le bouton **OK**.

Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pouvez plus contrôler l'application. Il devient également impossible de désinstaller l'application depuis l'appareil protégé.

Il est possible de réinitialiser le mot de passe à tout moment. Pour ce faire, décochez la case **Utiliser la protection par mot de passe** et enregistrez les modifications. La protection par mot de passe est désactivée et la somme de contrôle de l'ancien mot de passe est supprimée. Répétez le processus de création du mot de passe avec un nouveau mot de passe.

Administration des autorisations d'accès via le Plug-in Web

Cette section présente la navigation dans l'interface du Plug-in Web et la configuration des paramètres d'accès pour un seul ou pour l'ensemble des périphériques protégés du réseau.

Configuration des autorisations d'accès à Kaspersky Embedded Systems Security et au service Kaspersky Security

Pour configurer les autorisations d'accès pour un utilisateur ou un groupe, vous devez spécifier la chaîne de descripteur de sécurité à l'aide de la syntaxe SDDL. Pour en savoir plus sur la chaîne de descripteur de sécurité, consultez le site Web de Microsoft.

Pour configurer les autorisations d'accès pour un utilisateur ou un groupe :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.

2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Complémentaire**.

5. Exécutez une des actions suivantes :

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs autorisés à l'administrer les fonctions de Kaspersky Embedded Systems Security.

   - Cliquez sur **Configuration** dans la sous-section **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration du Service Kaspersky Security.

6. Ajoutez un utilisateur ou un groupe en définissant la chaîne de descripteur de sécurité dans la fenêtre **Autorisations d'accès de l'utilisateur pour l'administration de l'application** ou **Autorisations d'accès de l'utilisateur pour l'administration du service Kaspersky Security**.

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

Accès protégé par mot de passe aux fonctions de Kaspersky Embedded Systems Security

Vous pouvez limiter l'accès à l'administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs. Vous pouvez renforcer la protection des opérations critiques grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security requiert alors la saisie du mot de passe lors des tentatives d'accès aux fonctions suivantes de l'application :

- connexion à la Console de l'application ;
- désinstallation de Kaspersky Embedded Systems Security ;
- modification des composants de Kaspersky Embedded Systems Security ;
- exécution des commandes de la ligne de commande.

L'interface de Kaspersky Embedded Systems Security masque le mot de passe désigné à l'écran. Kaspersky Embedded Systems Security conserve le mot de passe spécifié sous la forme d'une somme de contrôle calculée à la saisie du mot de passe.

Kaspersky Embedded Systems Security ne vérifie pas la sécurité du mot de passe et ne bloque pas la saisie du mot de passe après plusieurs tentatives infructueuses.

Lors de la création d'un mot de passe, il est recommandé de respecter les conditions suivantes :

- Le mot de passe ne contient pas le nom du compte ou le nom de l'ordinateur.
- Le mot de passe comporte au moins 8 caractères.
- Le mot de passe contient des caractères appartenant à au moins trois des catégories suivantes :
  - lettres latines majuscules (A à Z) ;
  - lettres latines minuscules (a à z) ;
  - chiffres (0 à 9) ;
  - symboles du point d'exclamation (!), du signe dollar ($), du signe dièse (#) et du signe de pourcentage (%).

Vous pouvez exporter et importer les paramètres d'une application protégée par un mot de passe. Un fichier de configuration obtenu après l'exportation des paramètres de l'application protégée contient la valeur de la somme de contrôle du mot de passe et la valeur du modificateur utilisé pour l'extension de la ligne du mot de passe.

Ne modifiez pas la valeur de la somme de contrôle ou du modificateur dans le fichier de configuration. L'importation d'une configuration protégée par mot de passe qui a été modifiée manuellement peut entraîner le blocage complet de l'accès à l'application.

Pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Dans la section **Sécurité et fiabilité**, cliquez sur le bouton **Configuration**.
6. Dans la section **Paramètres de protection par mot de passe**, cochez la case **Utiliser la protection par mot de passe**.
7. Saisissez dans le champ **Mot de passe** le mot de passe que vous voulez utiliser pour protéger l'accès aux fonctions de Kaspersky Embedded Systems Security.
8. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés. Kaspersky Embedded Systems Security demandera le mot de passe défini pour octroyer l'accès aux fonctions protégées.

Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pourrez plus contrôler l'application. Il devient également impossible de désinstaller l'application depuis l'appareil protégé.

Il est possible de réinitialiser le mot de passe à tout moment. Pour ce faire, décochez la case **Utiliser la protection par mot de passe** et enregistrez les modifications. La protection par mot de passe est désactivée et la somme de contrôle de l'ancien mot de passe est supprimée. Répétez le processus de création du mot de passe avec un nouveau mot de passe.

Protection des fichiers en temps réel

Cette section contient des informations sur la tâche Protection des fichiers en temps réel et les instructions sur la configuration de cette tâche.

A propos de la tâche Protection des fichiers en temps réel

Au cours de l'exécution de la tâche Protection des fichiers en temps réel, Kaspersky Embedded Systems Security analyse les objets du périphérique protégé suivants lorsqu'ils sont sollicités :

- Les fichiers.
- Flux de données alternatifs NTFS.
- Les enregistrements de démarrage principaux et les secteurs d'amorçage des disques durs locaux ou des périphériques externes.

Lorsqu'une application quelconque enregistre un fichier sur le périphérique protégé ou le lit, Kaspersky Embedded Systems Security intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace, il exécute les actions que vous avez définies dans les paramètres de la tâche ou les actions par défaut : il tente de désinfecter le fichier, le place en quarantaine ou il le supprime. Avant la désinfection ou la suppression, Kaspersky Embedded Systems Security enregistre une copie chiffrée du fichier source dans le dossier Sauvegarde.

Kaspersky Embedded Systems Security détecte également les applications malveillantes pour les processus exécutés dans le sous-système Windows pour Linux®. Pour ces processus, la tâche Protection des fichiers en temps réel applique l'action définie par la configuration actuelle.

A propos de la zone de protection de la tâche et des paramètres de sécurité

Par défaut, la tâche Protection des fichiers en temps réel protège tous les objets du système de fichiers de l'appareil. Si la sécurité n'exige pas de protéger tous les objets du système de fichiers ou vous voulez exclure expressément certains objets de la zone d'action de la tâche de protection en temps réel, vous pouvez limiter la zone de protection.

Dans la Console de l'application, la zone de protection se présente sous la forme d'une arborescence ou d'une liste de ressources fichiers du périphérique que Kaspersky Embedded Systems Security peut surveiller. Par défaut les ressources de fichier réseau de l'appareil s'affichent sous la forme d'une liste.

Seul l'affichage sous forme de liste est disponible dans le plug-in d'administration.

Pour activer l'affichage des ressources de fichier réseau sous la forme d'une arborescence dans la Console de l'application,

dans la liste déroulante de la section du coin supérieur gauche de la fenêtre **Configuration de la zone de protection**, choisissez l'option **Afficher sous forme d'arborescence**.

Selon l'affichage des ressources de fichier du périphérique protégé en tant que liste ou d'arborescence, les icônes des nœuds prennent les significations suivantes :

☑ Nœud inclus dans la zone de protection.

☐ Nœud exclu de la zone de protection.

Au moins un des nœuds enfants intégrés à ce nœud est exclu de la zone de protection ou les paramètres de protection de ces nœuds diffèrent des paramètres de protection du nœud de niveau supérieur (pour l'arborescence uniquement).

L'icône s'affiche si tous les nœuds enfants ont été sélectionnés, mais pas le nœud parent. Dans ce cas, les modifications du contenu des fichiers et dossiers du nœud parent sont automatiquement ignorées lors de la constitution de la zone de protection du nœud enfant sélectionné.

La console de l'application permet également d'ajouter des disques virtuels à la zone de protection. Le nom des entrées virtuelles apparaît en bleu.

Paramètres de sécurité

Les paramètres de sécurité de la tâche peuvent être configurés globalement pour l'ensemble des nœuds ou des éléments repris dans la zone de protection ou individuellement pour chaque nœud ou élément dans l'arborescence ou la liste des ressources de fichier de l'appareil.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Vous pouvez configurer les paramètres de la zone de protection sélectionnée de l'une des manières suivantes :

- Sélection d'un des niveaux de sécurité prédéfinis.
- Configuration manuelle des paramètres de sécurité pour les nœuds ou les éléments sélectionnés dans l'arborescence ou la liste des ressources de fichier (le niveau de sécurité devient **Personnalisé**).

Vous pouvez enregistrer un ensemble de paramètres pour un nœud ou un élément dans un modèle afin de pouvoir l'appliquer à d'autres nœuds.

A propos des zones de protection virtuelles

Kaspersky Embedded Systems Security peut analyser non seulement les fichiers et les dossiers existants sur les disques durs et les disques amovibles mais également ceux qui sont créés dynamiquement sur le périphérique protégé par divers applications et services.

Si vous avez inclus tous les objets de l'appareil dans la zone de protection, ces entrées dynamiques seront automatiquement reprises dans la zone de protection. Toutefois, si vous souhaitez attribuer des valeurs particulières aux paramètres de sécurité de ces entrées dynamiques ou si vous avez sélectionné uniquement une partie de l'appareil pour la protection, pour pouvoir inclure les disques, les fichiers ou les dossiers virtuels dans la zone de protection, vous devrez d'abord les créer dans la Console de l'application ; c'est ce que l'on appelle la spécification d'une zone de protection virtuelle. Les disques, les fichiers ou les dossiers que vous créez existent uniquement dans la Console de l'application et non pas dans la structure du système de fichiers de l'appareil protégé.

Si au moment de composer la zone de protection, vous sélectionnez tous les fichiers ou les répertoires inclus sans choisir le répertoire parent, les répertoires ou les fichiers virtuels qui s'y trouvent ne seront pas repris automatiquement dans la zone de protection. Vous devez créer des "copies virtuelles" dans la console de l'application et les ajouter à la zone de protection.

Zones de protection prédéfinies

L'arborescence ou la liste des ressources fichiers affiche les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security couvre les zones de protection définies suivantes :

- **Disques durs locaux**. Kaspersky Embedded Systems Security protège les fichiers sur les disques durs du périphérique.
- **Disques amovibles**. Kaspersky Embedded Systems Security protège les fichiers sur les périphériques externes tels que les disques compacts ou amovibles. Vous pouvez inclure ou exclure de la zone de protection tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Réseau**. Kaspersky Embedded Systems Security protège les fichiers qui sont enregistrés dans les dossiers réseau ou qui y sont lus par les applications exécutées sur le périphérique. Kaspersky Embedded Systems Security ne protège pas les fichiers dans les répertoires réseau lorsqu'ils sont sollicités par des applications depuis d'autres périphériques protégés.
- **Disques virtuels**. Vous pouvez inclure dans la zone de protection les dossiers et les fichiers virtuels ainsi que les disques qui sont connectés temporairement à l'appareil, par exemple les disques partagés d'un cluster.

Par défaut, vous pouvez afficher et configurer des zones de protection prédéfinies dans la liste de zones ; vous pouvez également ajouter des zones prédéfinies à la liste au moment de sa création dans les paramètres de la zone de protection.

La zone de protection inclut par défaut tous les secteurs prédéfinis, à l'exception des disques virtuels.

Les disques virtuels créés à l'aide de la commande SUBST ne figurent pas dans l'arborescence des ressources fichier de l'appareil protégé dans la console de l'application. Pour inclure les objets d'un disque virtuel dans la zone de protection, il faut inclure le répertoire de l'appareil associé à ce disque virtuel dans la zone de protection.

Les disques réseau connectés ne sont pas non plus affichés dans la liste des ressources fichier de l'appareil protégé. Pour inclure les objets d'un disque réseau dans la zone de protection, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

A propos des niveaux de sécurité prédéfinis

Pour les entrées sélectionnées dans l'arborescence ou la liste des ressources de fichiers de l'appareil protégé, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si votre réseau a adopté des mesures de sécurité pour le périphérique protégé additionnelles comme des pare-feu ou des stratégies de sécurité existantes, en plus de l'installation de Kaspersky Embedded Systems Security sur les périphériques protégés et les postes de travail.

Recommandé

Le niveau de sécurité **Recommandé** offre le meilleur équilibre entre la protection et l'impact sur les performances des appareils protégés. Les experts de Kaspersky recommandent ce niveau pour protéger les périphériques sur la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité élevé pour les périphériques.

Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Options	Niveau de sécurité		
	Performance maximale	**Recommandé**	**Protection maximale**
Protection des objets	Selon l'extension	En fonction du format	En fonction du format
Protection uniquement des nouveaux fichiers et des fichiers modifiés	Activée	Activée	Désactivée
Actions à exécuter sur les objets infectés et autres	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible	Informer uniquement	Interdire l'accès et désinfecter. Supprimer si la désinfection est impossible
Actions à exécuter sur les objets probablement infectés	Interdire l'accès et placer en quarantaine	Informer uniquement	Interdire l'accès et placer en quarantaine
Exclure les fichiers	non	non	non
Ne pas détecter	non	non	non
Arrêter si l'analyse dure plus de (s.)	60 s	60 s	60 s
Ne pas analyser les objets composés de plus de (Mo)	8 Mo	8 Mo	Non configuré
Analyser les flux NTFS alternatifs	Oui	Oui	Oui
Analyser les secteurs d'amorçage et la partition MBR	Oui	Oui	Oui
Protection des objets composés	• Objets compactés* *Uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés*	• Archives SFX* • Objets compactés* • Objets OLE intégrés*

		• Objets OLE intégrés* *Uniquement les objets nouveaux et modifiés	*Tous les objets
Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré	non	non	Oui

Les paramètres **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift** et **Utiliser l'analyse heuristique** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si, après avoir choisi un des niveaux de sécurité prédéfinis, vous modifiez les paramètres de sécurité **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique**, le niveau de sécurité que vous aviez choisi ne change pas.

Extensions de fichiers analysés par défaut dans la tâche Protection des fichiers en temps réel

Kaspersky Embedded Systems Security analyse par défaut les fichiers possédant les extensions suivantes :

- *386*
- *acm*
- *ade, adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*
- *chm*
- *cla, clas**
- *cmd*
- *com*
- *cpl*

- *crt*
- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*
- *efi*
- *emf*
- *eml*
- *exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm, html**
- *htt*
- *ico*
- *inf*
- *ini*
- *ins*
- *isp*
- *jpg, jpe*
- *js, jse*
- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*

- *msp*
- *mst*
- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*
- *pht*
- *phtm**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*
- *shb*
- *shs*
- *sht*
- *shtm**
- *swf*

- *sys*
- *the*
- *them**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*
- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

Paramètres par défaut de la tâche Protection des fichiers en temps réel

Par défaut, la tâche Protection des fichiers en temps réel utilise les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres par défaut de la tâche Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
Zone de protection	L'ensemble de l'appareil protégé, à	Utilisez cette option pour modifier la zone de protection.

	l'exception des disques virtuels.	
Paramètres de sécurité	Identique pour toute la zone de protection ; correspond au niveau de sécurité **Recommandé**.	Pour les nœuds sélectionnées dans l'arborescence ou dans la liste des ressources de fichiers de l'appareil protégé, vous pouvez exécuter les actions suivantes : • Sélectionner un autre niveau de sécurité prédéfini ; • Modifier manuellement les paramètres de sécurité. Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à un autre nœud.
Mode de protection d'objets	**Mode intelligent**	Cette option permet de sélectionner le mode de protection, c'est-à-dire de définir le type de tentative d'accès pour lesquels Kaspersky Embedded Systems Security va analyser les objets.
Analyse heuristique	Le niveau de sécurité **Moyenne** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Appliquer la zone de confiance	Appliquée.	Liste d'exclusions générale que vous pouvez appliquer dans les tâches sélectionnées.
Utiliser KSN pour la protection	Appliquée.	Choisissez cette option pour améliorer l'efficacité de la protection de l'appareil en utilisant l'infrastructure de services cloud du Kaspersky Security Network (disponible si la Déclaration KSN a été acceptée).
Planification du lancement de la tâche	Au lancement de l'application.	Choisissez cette option pour configurer le lancement de la tâche planifiée.
Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante	Pas appliqué.	Choisissez cette option pour bloquer la session en cours et pour ajouter l'adresse IP de l'hôte ou le LUID de l'hôte pour lequel une activité malveillante a été détectée dans la section Stockage des ordinateurs bloqués.
Lancer une analyse rapide quand une infection active est détectée	Appliquée.	Kaspersky Embedded Systems Security crée et lance une tâche temporaire d'analyse rapide quand une infection active est détectée.

Administration de la tâche Protection des fichiers en temps réel via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des appareils protégés du réseau.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la stratégie pour la tâche Protection des fichiers en temps réel

Pour accéder aux paramètres de la tâche Protection des fichiers en temps réel via une stratégie de Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel de l'ordinateur**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Protection des fichiers en temps réel**.

   La fenêtre **Protection des fichiers en temps réel** s'ouvre.

Si l'appareil protégé est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés via la Console de l'application.

Accès aux propriétés de la tâche Protection des fichiers en temps réel

Pour ouvrir la fenêtre de configuration de la tâche Protection des fichiers en temps réel pour un seul appareil du réseau, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <Nom du périphérique>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - Sélectionnez l'option **Propriétés** dans le menu contextuel du périphérique protégé.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
5. Dans la section **Tâches**, sélectionnez la tâche **Protection des fichiers en temps réel**.
6. Cliquez sur le bouton **Propriétés**.

   La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.

Configuration de la tâche Protection des fichiers en temps réel

Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel**.
2. Configurez les paramètres de la tâche suivants :
   - Sous l'onglet **Général** :
     - **Paramètres d'interception**
     - **Analyse heuristique**
     - **Intégration aux autres composants**
   - Sous l'onglet **Administration des tâches** :
     - Paramètres de lancement de la tâche planifiée.
3. Sélectionnez l'onglet **Zone de protection**, puis réalisez les opérations suivantes :
   - Cliquez sur le bouton **Ajouter** ou **Modifier** pour modifier la zone de protection.
     - Dans la fenêtre qui s'ouvre, sélectionnez les éléments que vous souhaitez inclure dans la zone de protection de la tâche :
       - **Zone prédéfinie**
       - **Disque, dossier ou objet réseau**
       - **Fichier**
     - Sélectionnez un des niveaux de sécurité prédéfinis ou configurez manuellement les paramètres de protection.
4. Cliquez sur le bouton **OK** dans la fenêtre **Protection des fichiers en temps réel**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres à la tâche en cours d'exécution. La date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Sélection du mode de protection

La tâche Protection des fichiers en temps réel permet de sélectionner le mode de protection. La section **Mode de protection d'objets** permet de définir le type de tentative d'accès pour lesquels Kaspersky Embedded Systems Security analyse les objets.

La valeur du paramètre **Mode de protection d'objets** s'applique à toute la zone de protection définie dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les entrées particulières de la zone de protection.

Pour sélectionner le mode de protection :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection que vous souhaitez définir :
   - **Mode intelligent**
   - **À l'accès et à la modification**
   - **À l'accès**
   - **À l'exécution**
   - **Analyse plus profonde du lancement de processus (le lancement de processus est bloqué jusqu'à la fin de l'analyse)**
3. Cliquez sur le bouton **OK**.

Le mode de protection des objets sélectionné sera adopté.

Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Pour configurer l'analyse heuristique et l'intégration aux autres composants, procédez comme suit :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel**.
2. Sous l'onglet **Général**, cochez ou décochez la case **Utiliser l'analyse heuristique**.
3. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.
4. Configurez les paramètres suivants dans la section **Intégration aux autres composants** :
   - Cochez ou décochez la case **Appliquer la zone de confiance**.
   - Cochez ou décochez la case **Utiliser KSN pour la protection**.

     La case **Envoyer des données sur les fichiers analysés** doit être cochée dans les paramètres de la tâche Utilisation du KSN.
   - Cochez ou décochez la case **Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante**.
   - Cochez ou décochez la case **Lancer une analyse rapide quand une infection active est détectée**.
5. Cliquez sur le bouton **OK**.

Les paramètres configurés de la tâche seront appliqués immédiatement à une tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Planification des tâches

La Console de l'application permet de configurer la planification du lancement des tâches locales du système et des tâches définies par l'utilisateur. L'administration des tâches de groupe via la Console de l'application est impossible.

Pour planifier des tâches de groupe à l'aide du plug-in d'administration :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés**.
2. Sélectionnez le groupe auquel appartient l'appareil protégé.
3. Dans le volet résultats, choisissez l'onglet **Tâches**.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche.
   - Ouvrez le menu contextuel du nom de la tâche et sélectionnez l'option Propriétés.
5. Sélectionnez la section **Planification**.
6. Dans le groupe **Paramètres de planification**, cochez la case **Exécuté selon la planification**.

   Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée de ces tâches est interdite par une stratégie de Kaspersky Security Center.

7. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit :
   a. Choisissez une des options suivantes dans la liste **Fréquence** :
      - **Toutes les heures** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Chaque : <nombre> h**.
      - **Tous les jours** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Chaque : <nombre> jour(s)**.
      - **Toutes les semaines** si vous souhaitez que la tâche soit exécutée selon une fréquence en semaines que vous aurez définie dans le champ **Chaque : <nombre> semaine(s)**. Précisez les jours de la semaine où la tâche sera lancée (par défaut, les tâches sont exécutées le lundi).
      - **Au lancement de l'application** si vous souhaitez que la tâche soit exécutée à chaque lancement de Kaspersky Embedded Systems Security.
      - **À la mise à jour des bases de l'application** si vous souhaitez que la tâche soit exécutée après chaque mise à jour des bases de l'application.
   b. Indiquez, dans le champ **Heure de lancement**, l'heure du premier lancement de la tâche.

c. Indiquez, dans le champ **Date de lancement**, la date d'entrée en vigueur de la planification.

Après avoir planifié la date et l'heure de lancement ainsi que la fréquence de la tâche, l'heure estimée du prochain lancement est affichée.

Accédez à l'onglet **Planification** et ouvrez la fenêtre **Paramètres de la tâche**. L'heure estimée de lancement s'affiche dans le champ **Prochain démarrage** en haute de la fenêtre. Chaque fois que vous ouvrez la fenêtre, l'estimation est mise à jour.

Le champ **Prochain démarrage** affiche la valeur **Interdit par la stratégie** si les paramètres de Kaspersky Security Center interdisent le lancement d'une tâche du système planifiée.

8. Sous l'onglet **Avancé**, configurez le reste des paramètres de planification en fonction de vos besoins.

- Dans la section **Paramètres d'arrêt de la tâche** :

  a. Cochez la case **Durée**, puis dans les champs à droite, saisissez le nombre maximum d'heures et de minutes pour l'exécution de la tâche.

  b. Cochez la case **Pause à partir de**, puis saisissez dans les champs de droite les heures de début et de fin de l'intervalle par 24 heures au cours duquel la tâche sera suspendue.

- Dans la section **Paramètres avancés** :

  a. Cochez la case **Suspendre la planification à partir du** et indiquez la date à partir de laquelle la planification ne sera plus active.

  b. Cochez la case **Lancer les tâches non exécutées** pour activer le lancement des tâches ignorées.

  c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.

9. Cliquez sur le bouton **OK**.

10. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

Si vous souhaitez configurer les paramètres de l'application pour une tâche unique à l'aide de Kaspersky Security Center, consultez la section Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center.

Création et configuration de la zone de protection de la tâche

Pour créer et configurer la zone de protection de la tâche via Kaspersky Security Center, procédez comme suit :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel**.

2. Ouvrez l'onglet **Zone de protection**.

   Tous les éléments déjà couverts par la protection sont repris dans le tableau **Zone de protection**.

3. Cliquez sur le bouton Ajouter**Ajouter** pour ajouter un nouvel élément à la liste.

   La fenêtre **Ajouter des objets à la zone de protection** s'ouvre.

4. Sélectionnez un type d'objet pour l'ajouter à une zone de protection :

   - **Zone prédéfinie**, si vous voulez insérer une des zones prédéfinies dans la zone de protection de l'appareil. Puis, dans la liste déroulante, choisissez la zone de protection souhaitée.
   - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone de protection un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone de protection souhaitée en cliquant sur le bouton **Parcourir**.
   - **Fichier**, si vous voulez insérer dans la zone de protection uniquement un fichier distinct. Puis choisissez la zone de protection souhaitée en cliquant sur le bouton **Parcourir**.

   Vous ne pouvez pas ajouter un objet à une zone de protection s'il est déjà ajouté en tant qu'exclusion d'une zone de protection.

5. Pour exclure certains éléments de la zone de protection, décochez les cases en regard des noms de ces éléments ou réalisez les opérations suivantes :

   a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.

   b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.

   c. Dans la fenêtre **Ajouter une exclusion**, choisissez un type d'objet que vous voulez ajouter à titre d'exclusion de la zone de protection en suivant la procédure utilisée pour ajouter un objet à la zone de protection.

6. Pour modifier la zone de protection ou une exclusion existante, choisissez l'option **Modifier la zone** dans le menu contextuel de la zone de protection souhaitée.

7. Pour masquer l'affichage d'une zone de protection ou d'une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, choisissez l'option **Supprimer une zone** dans le menu contextuel de la zone de protection souhaitée.

   Une zone de protection est exclue de la zone d'action de la tâche Protection des fichiers en temps réel lors de sa suppression de la liste des ressources de fichier réseau.

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

La fenêtre Configuration de la zone de protection se ferme. Les nouvelles valeurs des paramètres seront enregistrés.

Vous ne pourrez exécuter la tâche **Protection des fichiers en temps réel** que si au moins une entrée de l'arborescence des ressources de fichiers de l'appareil est incluse dans une zone de protection.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour un nœud sélectionné dans la liste des ressources de fichiers du périphérique , vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**.

Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Protection des fichiers en temps réel**.
2. Ouvrez l'onglet **Zone de protection**.
3. Dans la liste du périphérique protégé, sélectionnez un élément inclus dans la zone de protection afin de définir le niveau de sécurité prédéfini.
4. Cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de la protection des fichiers en temps réel** s'ouvre.
5. Sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité que vous souhaitez appliquer.

   La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau de sécurité que vous avez sélectionné.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : Protection des fichiers en temps réel**.

   Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à une tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Configuration manuelle des paramètres de sécurité

Par défaut, la tâche Protection des fichiers en temps réel applique les mêmes paramètres de sécurité à toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour des éléments individuels dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil.

Pour configurer manuellement les paramètres de sécurité du nœud sélectionnée :

1. Ouvrez la fenêtre **Protection des fichiers en temps réel**.
2. Sous l'onglet **Zone de protection**, choisissez le nœud dont vous souhaitez configurer les paramètres de sécurité, puis cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de la protection des fichiers en temps réel** s'ouvre.
3. Sous l'onglet **Niveau de sécurité**, cliquez sur le bouton **Configuration** pour personnaliser la configuration.
4. Vous pouvez configurer les paramètres de sécurité personnalisés pour le nœud sélectionné en fonction de vos exigences :

   - Paramètres généraux
   - Actions
   - Performances

5. Cliquez sur le bouton **OK** dans la fenêtre **Protection des fichiers en temps réel**.

Les paramètres de la nouvelle zone de protection sont enregistrés.

Configuration des paramètres de tâche généraux

Configuration des paramètres généraux de sécurité de la tâche Protection des fichiers en temps réel

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel**.
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Protection des objets**, indiquez les types d'objets que vous souhaitez inclure à la zone de protection :
   - Tous les objets
   - **Objets analysés en fonction du format**
   - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**
   - **Objets analysés en fonction de la liste d'extensions indiquée**
   - **Analyser les secteurs d'amorçage et la partition MBR**
   - **Analyser les flux NTFS alternatifs**
4. Dans le groupe **Optimisation**, cochez ou décochez la case Protection uniquement des nouveaux fichiers et des fichiers modifiés.

   Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous**/**Nouveaux uniquement** de chacun des types d'objets composés.

5. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :
   - **Toutes les** / **Les nouvelles archives**
   - **Toutes les** / **Les nouvelles archives SFX**
   - **Toutes les** / **Les nouvelles bases de données d'emails**
   - **Tous les** / **Les nouveaux objets compactés**
   - **Tous les** / **Les nouveaux messages de texte brut**
   - **Tous les** / **Les nouveaux objets OLE incorporés**
6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration des actions

Pour configurer les actions sur les objets infectés et les autres objets détectés lors de l'exécution de la tâche Protection des fichiers en temps réel :

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel**.
2. Sélectionnez l'onglet **Actions**.
3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
   - **Informer uniquement**.
   - **Bloquer l'accès**.
   - **Exécuter une action supplémentaire**.
     Sélectionnez l'action dans la liste déroulante.
     - **Désinfecter**.
     - **Désinfecter. Supprimer si la désinfection est impossible**.
     - **Supprimer**.
     - **Recommandé**.
4. Sélectionnez l'action à exécuter sur les objets probablement infectés :
   - **Informer uniquement**.
   - **Bloquer l'accès**.
   - **Exécuter une action supplémentaire**.
     Sélectionnez l'action dans la liste déroulante.
     - **Quarantaine**.
     - **Supprimer**.
     - **Recommandé**.
5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
   a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.
   b. Cliquez sur le bouton **Configuration**.
   c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (à exécuter si la première échoue) pour chaque type d'objet détecté.
   d. Cliquez sur le bouton **OK**.

6. Choisissez l'action à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré.

7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'optimisation

Pour configurer les performances de la tâche Protection des fichiers en temps réel :

1. Ouvrez la fenêtre **Paramètres de la protection des fichiers en temps réel**.

2. Sélectionnez l'onglet **Optimisation**.

3. Dans la section **Exclusions** :

   - Cochez ou décochez la case **Exclure les fichiers**.
   - Cochez ou décochez la case **Ne pas détecter**.
   - Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

4. Dans la section **Paramètres avancés** :

   - **Arrêter si l'analyse dure plus de (s.)**
   - **Ne pas analyser les objets composés de plus de (Mo)**
   - **Utiliser la technologie iSwift**
   - **Utiliser la technologie iChecker**

Administration de la tâche de protection des fichiers en temps réel via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un appareil protégé.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la tâche Protection des fichiers en temps réel

Pour ouvrir la fenêtre de configuration des paramètres généraux d'une tâche, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.
3. Dans le volet résultats, cliquez sur le lien **Propriétés**.

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

Accès aux paramètres de la zone d'action de la tâche Protection des fichiers en temps réel

Pour ouvrir la fenêtre des paramètres de la Zone de protection de la tâche Protection des fichiers en temps réel, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.
3. Dans le volet résultats, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.

Configuration de la tâche Protection des fichiers en temps réel

Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
   - Mode de protection d'objets
   - **Analyse heuristique**
   - **Intégration aux autres composants**
3. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche.
4. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

   Les modifications apportées aux paramètres seront enregistrées.
5. Dans le volet résultats du nœud **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.
6. Exécutez les actions suivantes :

- Dans l'arborescence ou la liste des ressources de fichier de l'appareil, sélectionnez les entrées ou les éléments à inclure dans la zone de protection de la tâche.
- Sélectionnez un des niveaux de sécurité prédéfinis ou configurez les paramètres de protection de l'objet manuellement.

7. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres à la tâche en cours d'exécution. La date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche définis avant et après leur modification, sont enregistrées dans le journal d'audit système.

Sélection du mode de protection

La tâche Protection des fichiers en temps réel permet de sélectionner le mode de protection. La section **Mode de protection d'objets** permet de définir le type de tentative d'accès pour lesquels Kaspersky Embedded Systems Security analyse les objets.

La valeur du paramètre **Mode de protection d'objets** s'applique à toute la zone de protection définie dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les entrées particulières de la zone de protection.

Pour sélectionner le mode de protection :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection que vous souhaitez définir :
   - **Mode intelligent**
   - **À l'accès et à la modification**
   - **À l'accès**
   - **À l'exécution**
   - **Analyse plus profonde du lancement de processus (le lancement de processus est bloqué jusqu'à la fin de l'analyse)**
3. Cliquez sur le bouton **OK**.

Le mode de protection des objets sélectionné sera adopté.

Configuration de l'analyse heuristique et de l'intégration aux autres composants de l'application

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Pour configurer l'analyse heuristique et l'intégration aux autres composants, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Sous l'onglet **Général**, cochez ou décochez la case **Utiliser l'analyse heuristique**.
3. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.
4. Configurez les paramètres suivants dans la section **Intégration aux autres composants** :
   - Cochez ou décochez la case **Appliquer la zone de confiance**.
     Le lien **Zone de confiance** permet d'accéder aux paramètres de la Zone de confiance.
   - Cochez ou décochez la case **Utiliser KSN pour la protection**.

     La case **Envoyer des données sur les fichiers analysés** doit être cochée dans les paramètres de la tâche Utilisation du KSN.
   - Cochez ou décochez la case B**Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante**.
   - Cochez ou décochez la case **Lancer une analyse rapide quand une infection active est détectée**.
5. Cliquez sur le bouton **OK**.

Les paramètres de la tâche définis seront appliqués.

Configuration des paramètres de planification d'une tâche

La Console de l'application permet de planifier le lancement des tâches système locales et des tâches définies par l'utilisateur. Cependant, il n'est pas possible de planifier le lancement des tâches de groupe.

Pour planifier une tâche :

1. Ouvrez le menu contextuel de la tâche à planifier.
2. Choisissez l'option **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, cochez la case **Exécuté selon la planification**.
4. Suivez ces étapes pour définir les paramètres de planification :
   a. Dans la liste déroulante **Fréquence**, sélectionnez une des options :
      - **Toutes les heures** : pour exécuter la tâche toutes les heures ; précisez le nombre d'heures dans le champ **Chaque** <chiffre> **heure(s)**.
      - **Tous les jours** : pour exécuter selon un intervalle en jours ; précisez le nombre de jours dans le champ **Chaque <chiffre> jour(s)**.
      - **Toutes les semaines** : pour exécuter la tâche selon un intervalle en semaines ; précisez le nombre de semaines dans le champ **Chaque les <chiffre> semaine(s) le**. Précisez les jours de la semaine où la tâche sera exécutée (par défaut les tâches sont exécutées le lundi).

- **Au lancement de l'application** : pour exécuter la tâche à chaque lancement de Kaspersky Embedded Systems Security.
- **À la mise à jour des bases de l'application** : pour exécuter la tâche après chaque mise à jour des bases de l'application.

b. Renseignez dans le champ **Heure de lancement** l'heure du premier lancement de la tâche.

c. Renseignez dans le champ **Date de lancement** la date du premier lancement de la tâche.

Après avoir indiqué la fréquence d'exécution de la tâche, l'heure de la première exécution et la date d'entrée en vigueur de la planification, les informations relatives au temps restant avant la nouvelle exécution de la tâche apparaissent dans le champ **Prochain démarrage** de la partie supérieure de la fenêtre. Des informations actualisées sur l'estimation de temps restant avant le prochain lancement de la tâche sont affichées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

Le champ **Prochain démarrage** affiche la valeur **Interdit par la stratégie** si les paramètres de la stratégie active de Kaspersky Security Center interdisent le lancement d'une tâche locales du système planifiée.

5. Utilisez l'onglet **Avancé** pour définir les paramètres de planification suivants :

- Dans la section **Paramètres d'arrêt de la tâche** :

  a. Cochez la case **Durée**. Dans les champs de droite, saisissez la durée maximale de la tâche en heures et en minutes.

  b. Cochez la case **Pause à partir de**. Dans les champs de droite, saisissez quand il faudra interrompre et reprendre la tâche (sous 24 heures).

- Dans la section **Paramètres avancés** :

  a. Cochez la case **Suspendre la planification à partir du** et renseignez la date de fin de la planification de la tâche.

  b. Cochez la case **Lancer les tâches non exécutées** pour lancer les tâches ignorées.

  c. Cochez la case **Répartir l'exécution dans un intervalle de** et indiquez la valeur du paramètre en minutes.

6. Cliquez sur le bouton **OK**.

Les paramètres de la planification de la tâche sont enregistrés.

Constitution d'une zone de protection

Cette section contient des informations sur la constitution et l'utilisation de la zone de protection dans la tâche Protection des fichiers en temps réel et sur son utilisation.

Configuration de l'affichage des ressources de fichier réseau

Pour sélectionner le mode d'affichage des ressources de fichier réseau lors de la configuration des paramètres de la zone de protection :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez l'une des options suivantes :
   - Choisissez le point **Afficher sous forme d'arborescence** si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une arborescence.
   - Choisissez le point **Afficher sous forme de liste**, si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une liste.

   Par défaut les ressources de fichier réseau de l'appareil protégé s'affichent sous la forme d'une liste.
3. Cliquez sur le bouton **Enregistrer**.

Constitution d'une zone de protection

La procédure de constitution de la zone de protection dans la tâche Protection des fichiers en temps réel dépend de l'affichage des ressources de fichier réseau sélectionné. Vous pouvez consulter les ressources de fichier réseau sous la forme d'une arborescence ou d'une liste (option par défaut).

Pour appliquer les nouveaux paramètres de la zone de protection à la tâche, il faut relancer la tâche Protection des fichiers en temps réel.

Pour créer une zone de protection à l'aide de l'arborescence des ressources de fichier réseau, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Dans la section gauche de la fenêtre, déployez l'arborescence des ressources de fichier réseau pour afficher tous les nœuds et les nœuds enfants.
3. Exécutez les actions suivantes :
   - Pour exclure certaines entrées de la zone de protection, décochez les cases à côté des noms de ces entrées.
   - Pour inclure certains nœuds à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :
     - Si vous souhaitez inclure tous les disques d'un même type dans la zone de protection, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur l'appareil, cochez la case **Disques amovibles**).

- Si vous souhaitez inclure un disque particulier du type requis dans la zone de protection, développez le nœud qui contient la liste des disques de ce type et cochez la case en regard du nom du disque. Par exemple, pour sélectionner le disque amovible F:, développez le nœud **Disques amovibles** et cochez la case en regard du disque **F:**.

- Si vous souhaitez inclure dans la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case en regard de ce dossier ou de ce fichier.

4. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** se ferme. Les nouvelles valeurs des paramètres seront enregistrés.

Pour créer une zone de protection à l'aide de la liste des ressources de fichier réseau, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.

2. Pour inclure certains nœuds à la zone de protection, décochez la case **Poste de travail** et procédez comme suit :

   a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.

   b. Dans le menu contextuel, sélectionnez l'option **Ajouter une zone de protection**.

   c. Dans la fenêtre **Ajouter une zone de protection**, choisissez un type d'objet que vous voulez ajouter à la zone de protection :

   - **Zone prédéfinie**, si vous voulez insérer une des zones prédéfinies dans la zone de protection de l'appareil. Puis, dans la liste déroulante, choisissez la zone de protection souhaitée.

   - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone de protection un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.

   - **Fichier**, si vous voulez insérer dans la zone de protection uniquement un fichier distinct. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.

   Vous ne pouvez pas ajouter un objet à une zone de protection s'il est déjà ajouté en tant qu'exclusion d'une zone de protection.

3. Pour exclure certaines entrées de la zone de protection, décochez les cases en regard des noms de ces entrées ou réalisez les opérations suivantes :

   a. Ouvrez le menu contextuel de la zone de protection d'un clic-droit de la souris.

   b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.

   c. Dans la fenêtre **Ajouter une exclusion**, choisissez un type d'objet que vous voulez ajouter à titre d'exclusion de la zone de protection en suivant la procédure utilisée pour ajouter un objet à la zone de protection.

4. Pour modifier la zone de protection ou une exclusion existante, choisissez l'option **Modifier la zone** dans le menu contextuel de la zone de protection souhaitée.

5. Pour masquer l'affichage d'une zone de protection ou d'une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone de protection nécessaire, choisissez l'option

Supprimer de la liste.

Une zone de protection est exclue de la zone d'action de la tâche Protection des fichiers en temps réel lors de sa suppression de la liste des ressources de fichier réseau.

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** se ferme. Les nouvelles valeurs des paramètres seront enregistrés.

Vous ne pourrez exécuter la tâche Protection des fichiers en temps réel que si au moins une entrée de l'arborescence des ressources de fichiers de l'appareil est incluse dans une zone de protection.

Si vous définissez une zone de protection complexe, par exemple en attribuant différentes valeurs aux paramètres de sécurité pour diverses entrées distinctes de l'arborescence des ressources fichiers de l'appareil, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.

Inclusion des objets réseau dans la zone de protection

Vous pouvez inclure dans la zone de protection des disques réseau, des répertoires ou des fichiers en indiquant leur chemin d'accès de réseau au format UNC (Universal Naming Convention).

Vous ne pouvez pas analyser les dossiers réseau en cas d'utilisation du compte système.

Pour ajouter un emplacement réseau à la zone de protection :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Afficher sous forme d'arborescence**.
3. Dans le menu contextuel du nœud **Réseau** :
   - Choisissez l'option **Ajouter un dossier de réseau** si vous souhaitez ajouter un dossier réseau à la zone de protection.
   - Choisissez l'option **Ajouter un fichier de réseau** si vous souhaitez ajouter un fichier réseau à la zone de protection.
4. Saisissez le chemin d'accès au dossier du réseau ou au fichier au format UNC.
5. Appuyez sur la touche **RETOUR**.
6. Cochez la case en regard du nom de l'objet réseau ajouté afin de l'inclure dans la zone de protection.
7. Le cas échéant, modifiez les paramètres de sécurité de l'objet réseau ajouté.

8. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Création d'une zone de protection virtuelle

Vous pouvez ajouter à la zone de protection/d'analyse des disques virtuels, des dossiers ou des fichiers distincts, uniquement si la zone de protection/d'analyse s'affiche sous la forme d'une arborescence de ressources de fichiers.

Pour ajouter un disque virtuel à la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arborescence**.
3. Ouvrez le menu contextuel du nœud **Disques virtuels**.
4. Sélectionnez l'option **Ajouter un disque virtuel** .
5. Dans la liste des noms disponibles, sélectionnez le nom du disque virtuel en cours de création.
6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone de protection.
7. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Les nouvelles valeurs des paramètres seront enregistrés.

Pour ajouter un dossier ou un fichier virtuel dans la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Afficher sous forme d'arborescence**.
3. Ouvrez le menu contextuel du disque virtuel auquel vous souhaitez ajouter un dossier ou un fichier, puis choisissez une des options suivantes :
   - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone de protection.
   - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone de protection.
4. Dans le champ, saisissez le nom du dossier ou du fichier.
5. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone de protection.
6. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Configuration manuelle des paramètres de sécurité

Par défaut, les tâches de protection en temps réel de l'ordinateur appliquent les mêmes paramètres de sécurité pour toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour des éléments individuels dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil.

Lorsque vous utilisez l'arborescence des ressources du fichier de l'appareil protégés, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Pour configurer manuellement les paramètres de sécurité :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Dans la section gauche de la fenêtre, sélectionnez le nœud dont vous souhaitez configurer les paramètres de sécurité.

   Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité à un nœud ou élément sélectionné dans la zone de protection.

   Dans la section gauche de la fenêtre, vous pouvez sélectionner la vue des ressources de fichier réseau, créer une zone de protection ou créer une zone de protection virtuelle.
3. Dans la partie droite de la fenêtre, exécutez l'une des actions suivantes :
   - Sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité que vous souhaitez appliquer.
   - Configurez les paramètres de sécurité requis pour le nœud ou l'élément sélectionné en fonction de vos exigences sous les onglets suivants :
     - **Général**
     - **Actions**
     - **Optimisation**
4. Dans la fenêtre **Configuration de la zone de protection**, cliquez sur le bouton **Enregistrer**.

Les paramètres de la nouvelle zone de protection sont enregistrés.

Sélection d'un niveau de sécurité prédéfini pour la tâche Protection des fichiers en temps réel

Pour le nœud sélectionné dans l'arborescence ou la liste des ressources de fichiers du périphérique protégé, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**.

Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Dans l'arborescence ou la liste des ressources de fichier réseau de l'appareil protégé, sélectionnez le nœud ou l'objet pour lequel vous souhaitez définir le niveau de sécurité.
3. Assurez-vous que le nœud ou l'élément sélectionné se trouve dans la zone de protection.
4. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez le niveau de sécurité à appliquer.

   La fenêtre reprend la liste des paramètres de sécurité correspondant au niveau de sécurité sélectionné.
5. Cliquez sur le bouton **Enregistrer**.

   Les paramètres de la tâche sont enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les paramètres modifiés sont appliqués au prochain lancement de la tâche.

Configuration des paramètres de tâche généraux

Configuration des paramètres généraux de sécurité de la tâche Protection des fichiers en temps réel

1. Ouvrez la fenêtre **Configuration de la zone de protection**.
2. Sélectionnez l'onglet **Général**.
3. Dans la section **Protection des objets**, indiquez les objets que vous souhaitez inclure dans la zone de protection :
   - **Tous les objets**
   - **Objets analysés en fonction du format**
   - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**
   - **Objets analysés en fonction de la liste d'extensions indiquée**
   - **Analyser les secteurs d'amorçage et la partition MBR**
   - **Analyser les flux NTFS alternatifs**
4. Dans le groupe **Optimisation**, cochez ou décochez la case Protection uniquement des nouveaux fichiers et des fichiers modifiés.

   > Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.
5. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :
   - **Toutes les / Les nouvelles archives**
   - **Toutes les / Les nouvelles archives SFX**
   - **Toutes les / Les nouvelles bases de données d'emails**

- Tous les / Les nouveaux objets compactés
- Tous les / Les nouveaux messages de texte brut
- Tous les / Les nouveaux objets OLE incorporés

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration des actions

Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Protection des fichiers en temps réel :

1. Ouvrez la fenêtre Configuration de la zone de protection.
2. Sélectionnez l'onglet **Actions**.
3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
   - Informer uniquement.
   - Bloquer l'accès.
   - **Exécuter une action supplémentaire**.
     Sélectionnez l'action dans la liste déroulante.
     - **Désinfecter**.
     - **Désinfecter. Supprimer si la désinfection est impossible**.
     - Supprimer.
     - Recommandé.
4. Sélectionnez l'action à exécuter sur les objets probablement infectés :
   - Informer uniquement.
   - Bloquer l'accès.
   - **Exécuter une action supplémentaire**.
     Sélectionnez l'action dans la liste déroulante.
     - **Quarantaine**.
     - Supprimer.
     - Recommandé.
5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
   a. Cochez ou décochez la case Exécuter les actions en fonction du type d'objet détecté.

b. Cliquez sur le bouton **Configuration**.

c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (à exécuter si la première échoue) pour chaque type d'objet détecté.

d. Cliquez sur le bouton **OK**.

6. Choisissez l'action à exécuter sur les fichiers composés non modifiables : cochez ou décochez la case Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré.

7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'optimisation

Pour configurer les performances de la tâche Protection des fichiers en temps réel :

1. Ouvrez la fenêtre **Configuration de la zone de protection**.

2. Sélectionnez l'onglet **Optimisation**.

3. Dans la section **Exclusions** :

   - Cochez ou décochez la case **Exclure les fichiers**.
   - Cochez ou décochez la case **Ne pas détecter**.
   - Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

4. Dans la section **Paramètres avancés** :

   - **Arrêter si l'analyse dure plus de (s.)**
   - **Ne pas analyser les objets composés de plus de (Mo)**
   - **Utiliser la technologie iSwift**
   - **Utiliser la technologie iChecker**

Statistiques de la tâche Protection des fichiers en temps réel

Pendant l'exécution de la tâche Protection des fichiers en temps réel, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Embedded Systems Security depuis le lancement de cette tâche.

Pour consulter les paramètres de la tâche Protection des fichiers en temps réel :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Protection des fichiers en temps réel**.

Le volet résultats du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Embedded Systems Security a traités depuis son lancement (cf. tableau ci-dessous).

Statistiques de la tâche Protection des fichiers en temps réel

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Embedded Systems Security. Par exemple, si Kaspersky Embedded Systems Security a découvert une objet malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	Nombre d'objets que Kaspersky Embedded Systems Security a détectés et classés comme infectés ou nombre de fichiers logiciels légitimes détectés et que des intrus peuvent utiliser pour endommager votre périphérirque ou vos données personnelles.
Objets probablement infectés détectés	Nombre d'objets détectés par Kaspersky Embedded Systems Security et considérés comme probablement infectés.
Objets non désinfectés	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu désinfecter pour les raisons suivantes : • L'objet détecté appartient à un type d'objet qui ne peut être désinfecté. • une erreur s'est produite lors de la désinfection.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Embedded Systems Security a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Embedded Systems Security a tenté de supprimer en vain, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone de protection que Kaspersky Embedded Systems Security n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
Objets non sauvegardés	Nombre d'objets pour lesquels Kaspersky Embedded Systems Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
Erreurs de traitement	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets désinfectés	Nombre d'objets désinfectés par Kaspersky Embedded Systems Security.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Embedded Systems Security.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la Sauvegarde par Kaspersky Embedded Systems Security.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Embedded Systems Security.
Objets protégés par	Nombre d'objets (archives, par exemple) que Kaspersky Embedded Systems Security a ignorés en raison d'une protection par mot de passe.

mot de passe	
Objets endommagés	Nombre d'objets que Kaspersky Embedded Systems Security a ignorés à cause de leur format endommagé.
Objets traités	Nombre d'objets traités par Kaspersky Embedded Systems Security.

Vous pouvez également consulter les statistiques de la tâche Protection des fichiers en temps réel dans le journal d'exécution de la tâche via le lien **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du panneau des résultats.

Si la valeur dans le champ Total des événements**Total des événements** de la fenêtre du journal d'exécution de la tâche Protection des fichiers en temps réel est supérieure à 0, il est recommandé de traiter manuellement les événements du journal d'exécution de la tâche sous l'onglet **Événements**.

Administration de la tâche de protection des fichiers en temps réel via le Plug-in Web

Cette section explique comment gérer la tâche Protection des fichiers en temps réel via l'interface du Plug-in Web.

Configuration de la tâche Protection des fichiers en temps réel

Le niveau de sécurité prédéfini ne peut pas être modifié pour la tâche de protection des fichiers en temps réel via le Plug-in Web.

Pour configurer la tâche Protection des fichiers en temps réel via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection des fichiers en temps réel**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la tâche Protection des fichiers en temps réel

Paramètre	Description
Mode intelligent	Kaspersky Embedded Systems Security sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si le processus accède à l'objet plusieurs fois et le modifie, Kaspersky Embedded Systems Security analyse l'objet uniquement après son dernier enregistrement par le processus.
À l'accès	Kaspersky Embedded Systems Security analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

À l'accès et à la modification	Kaspersky Embedded Systems Security analyse un objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié. Cette option est sélectionnée par défaut.
À l'exécution	Kaspersky Embedded Systems Security analyse le fichier uniquement en cas d'ouverture pour exécution.
Analyse plus profonde du lancement de processus (le lancement de processus est bloqué jusqu'à la fin de l'analyse)	Kaspersky Embedded Systems Security effectue une analyse plus longue des processus de lancement avec une probabilité plus élevée de détecter une menace. Le lancement du processus est bloqué jusqu'à la fin de l'analyse.
Utiliser l'analyse heuristique	La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets. Si la case est cochée, l'analyse heuristique est activée. Si la case est décochée, l'analyse heuristique est désactivée. Cette case est cochée par défaut.
Niveau de l'analyse heuristique	Le niveau de l'analyse heuristique définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Il existe trois niveaux de sensibilité pour l'analyse : • **Superficielle**. L'analyse heuristique exécute moins d'actions dans les fichiers exécutables. A ce niveau, la probabilité de détecter une menace diminue. L'analyse monopolise moins de ressources du système et se déroule plus rapidement. • **Moyenne**. L'analyse heuristique exécute le nombre d'instructions de fichier exécutable recommandé par les experts de Kaspersky. Il s'agit du niveau par défaut. • **Minutieuse**. L'analyse heuristique exécute plus d'actions contenues dans le fichier exécutable. A ce niveau, la probabilité de détecter une menace augmente. L'analyse consomme beaucoup de ressources du système, prend beaucoup de temps et le nombre fausses alarmes peut augmenter. Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.
Appliquer la zone de confiance	La case active ou désactive l'application de la zone de confiance dans l'exécution de la tâche. Si la case est cochée, Kaspersky Embedded Systems Security ajoute les opérations sur les fichiers des processus de confiance aux exclusions de l'analyse configurées dans les paramètres de la tâche. Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte les opérations sur les fichiers des processus de confiance lors de la création de la zone de protection pour la tâche. Cette case est cochée par défaut.
Utiliser KSN pour la protection	Cette case active ou désactive l'utilisation des services KSN.

	Si la case est cochée, l'application utilise les données du Kaspersky Security Network afin de pouvoir réagir plus vite aux nouvelles menaces et de réduire le risque de faux positifs. Si la case est décochée, la tâche n'utilise pas les services du KSN. Cette case est cochée par défaut.
Bloquer l'accès aux ressources réseau partagées pour les sessions réseau qui affichent une activité malveillante	La case active ou désactive le blocage de la session en cours et contrôle la disponibilité des ressources partagées du réseau en termes de session en cours. Si la case est cochée, Kaspersky Embedded Systems Security bloque la session en cours et, en termes de session en cours, rend les ressources réseau partagées inaccessibles pour les hôtes pour lesquels une activité malveillante a été détectée dans la section Stockage des ordinateurs bloqués. Si la case est décochée, les conditions ne sont pas appliquées et Kaspersky Embedded Systems Security fonctionne normalement. Cette case est décochée par défaut. Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués. Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.
Lancer une analyse rapide quand une infection active est détectée	Si cette case est cochée, Kaspersky Embedded Systems Security crée et lance une tâche temporaire d'analyse rapide quand une infection active est détectée. Une fois la tâche temporaire Analyse rapide terminée, Kaspersky Embedded Systems Security la supprime. Si cette case est décochée, Kaspersky Embedded Systems Security ne crée pas et ne lance pas une tâche Analyse rapide quand une infection active est détectée. Cette case est cochée par défaut.
Zone de protection	Vous pouvez configurer les paramètres de sécurité de la zone de protection.

Configuration de la zone de protection de la tâche

Pour configurer la zone de protection de la tâche Protection des fichiers en temps réel :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection des fichiers en temps réel**.

6. Sélectionnez la section **Zone de protection**.
7. Réalisez une des opérations suivantes :
   - Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
   - Sélectionnez une règle existante et cliquez sur le bouton **Modifier**.

   La fenêtre **Modifier la zone** s'ouvre.
8. Basculez le bouton bascule sur **Actif** et sélectionnez un type d'objet.
9. Configurez les paramètres suivants dans la section **Protection des objets** :
   - **Mode de protection d'objets** :
     - Tous les objets
     - Objets analysés en fonction du format
     - Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus
     - Objets analysés en fonction de la liste d'extensions indiquée
   - Analyser les secteurs d'amorçage et la partition MBR
   - Analyser les flux NTFS alternatifs
10. Dans la section **Protection des objets**, cochez ou décochez la case Protection uniquement des nouveaux fichiers et des fichiers modifiés.
11. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
    - Archives
    - Archives SFX
    - Objets compactés
    - Bases de données d'emails
    - Email en texte brut
    - Objets OLE intégrés
    - Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré
12. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
    - Informer uniquement.
    - Bloquer l'accès.
    - **Exécuter une action supplémentaire**.

Sélectionnez l'action dans la liste déroulante.

- **Désinfecter**.
- **Désinfecter. Supprimer si la désinfection est impossible**.
- **Supprimer**.
- **Recommandé**.

13. Sélectionnez l'action à exécuter sur les objets probablement infectés :

- **Informer uniquement**.
- **Bloquer l'accès**.
- **Exécuter une action supplémentaire**.

  Sélectionnez l'action dans la liste déroulante.

  - **Quarantaine**.
  - **Supprimer**.
  - **Recommandé**.

14. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

    a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.

    b. Cliquez sur le bouton **Configuration**.

    c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (à exécuter si la première échoue) pour chaque type d'objet détecté.

    d. Cliquez sur le bouton **OK**.

15. Configurez les paramètres suivants dans la section **Exclusions** :

- Cochez ou décochez la case **Exclure les fichiers**.
- Cochez ou décochez la case **Ne pas détecter**.

16. Configurez les paramètres suivants dans la section **Optimisation** :

- **Arrêter si l'analyse dure plus de (s.)**
- **Ne pas analyser les objets composés de plus de (Mo)**
- **Utiliser la technologie iSwift**
- **Utiliser la technologie iChecker**

17. Cliquez sur le bouton **OK**.

Utilisation du KSN

Cette section contient des informations sur la tâche Utilisation du KSN et les instructions sur la configuration de cette tâche.

A propos de la tâche Utilisation du KSN

Kaspersky Security Network (ci-après, "KSN") est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky concernant la réputation des fichiers, des ressources Internet et des applications. L'utilisation des données du Kaspersky Security Network assure une vitesse de réaction plus élevée de Kaspersky Embedded Systems Security face aux nouvelles menaces, augmente l'efficacité de certains modules la protection et réduit la possibilité de faux positifs.

Vous devez accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Kaspersky Embedded Systems Security obtient uniquement du Kaspersky Security Network les informations sur la réputation des applications.

La participation des utilisateurs au KSN permet à Kaspersky d'obtenir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des outils de neutralisation et de réduire le nombre de faux positifs des modules de l'application.

Pour de plus amples informations sur le transfert, le traitement, le stockage et la destruction des informations sur l'utilisation de l'application, vous pouvez consulter la fenêtre **Traitement des données** de la tâche Utilisation du KSN et la Politique de confidentialité sur le site Internet de Kaspersky.

La participation au Kaspersky Security Network est volontaire. La décision de participer à Kaspersky Security Network est prise pendant ou après l'installation de Kaspersky Embedded Systems Security. Vous pouvez changer d'avis quant à votre décision de participer au Kaspersky Security Network à n'importe quel moment.

Le réseau Kaspersky Security Network peut être utilisé dans les tâches suivantes de Kaspersky Embedded Systems Security :

- Protection des fichiers en temps réel.
- Analyse à la demande.
- Contrôle du lancement des applications.

Kaspersky Private Security Network

Vous trouverez toutes les informations détaillées sur la configuration de Kaspersky Private Security Network (ci-après « KSN privé ») dans *l'aide de Kaspersky Security Center*.

Si vous utilisez le KSN privé sur le périphérique, dans la fenêtre **Traitement des données** de la tâche Utilisation du KSN, vous pouvez lire la Déclaration de KSN et activer la tâche à tout moment en cochant la case **J'accepte les conditions de participation au programme Kaspersky Security Network**. En acceptant les conditions, vous acceptez d'envoyer tous types de données mentionnées dans la Déclaration de KSN (demandes de sécurité, données statistiques) aux services KSN.

Quand vous avez accepté les conditions du KSN privé, les cases qui règlent l'utilisation du KSN global sont indisponibles.

Si vous désactivez le KSN privé lorsque la tâche Utilisation du KSN est en cours d'exécution, l'erreur *Violation de la licence* se produit et la tâche s'arrête. Pour continuer à protéger le périphérique, vous devez accepter la Déclaration de KSN sous l'onglet **Traitement des données** et relancer la tâche.

Annulation de l'acceptation de la Déclaration de KSN

Vous pouvez annuler l'acceptation et arrêter tout échange de données avec Kaspersky Security Network à n'importe quel moment. Les actions suivantes sont considérées comme l'annulation complète ou partielle de la Déclaration de KSN :

- Si vous décochez la case **Envoyer des données sur les fichiers analysés**, l'application arrête d'envoyer des sommes de contrôle des fichiers analysés au service KSN pour analyse.
- Si vous décochez la case **Envoyer les statistiques de Kaspersky Security Network**, l'application arrête de traiter des données avec des statistiques KSN supplémentaires.
- Si vous décochez la case **J'accepte les conditions de participation au programme Kaspersky Security Network**, l'application arrête le traitement de toutes les données liées à KSN et la tâche Utilisation du KSN s'arrête.
- Désinstallation du composant Utilisation du KSN : le traitement de toutes les données liées à KSN s'arrête.
- Désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center : le traitement de toutes les données liées à KSN s'arrête.
- Désinstallation d'une clé de licence pour Kaspersky Embedded Systems Security ou suspension de la licence : tous les traitements de données relatifs à KSN s'arrêtent.

Paramètres de la tâche Utilisation du KSN par défaut

Vous pouvez modifier les paramètres de la tâche Utilisation du KSN précisés par défaut (cf. tableau ci-dessous).

Paramètres de la tâche Utilisation du KSN par défaut

Paramètre	Valeur par défaut	Description
Actions à exécuter sur les objets douteux selon KSN	Supprimer	Vous pouvez préciser les actions que Kaspersky Embedded Systems Security va exécuter sur les objets réputés comme douteux par KSN.
Transfert de données	La somme de contrôle (hash MD5) est calculée pour les	Vous pouvez définir la taille maximale des fichiers dont la somme de contrôle sera calculée à l'aide de l'algorithme MD5 pour envoi à KSN. Si la case est décochée, Kaspersky

	fichiers dont la taille ne dépasse pas 2 Mo.	Embedded Systems Security calcule les hash MD5 pour les fichiers de n'importe quelle taille.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	Vous pouvez lancer la tâche manuellement ou planifier son exécution.
Utiliser Kaspersky Security Center en tant que serveur proxy du KSN	Sélectionné	Par défaut, les données sont envoyées à KSN via Kaspersky Security Center. Vous pouvez modifier ce paramètre uniquement via le Plug-in d'administration.
J'accepte les conditions de participation au programme Kaspersky Security Network	Non cochée	Si cette option est sélectionnée, la participation à KSN après installation est acceptée. Vous pouvez modifier votre choix à tout moment.
Envoyer les statistiques de Kaspersky Security Network	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les statistiques de KSN seront envoyées automatiquement, sauf si vous décochez la case.
Envoyer des données sur les fichiers analysés	Sélectionné (appliqué uniquement si la Déclaration de KSN est acceptée)	Si la Déclaration de KSN est acceptée, les données sur les fichiers précédemment analysés depuis le démarrage de la tâche sont envoyées. Il est possible de décocher la case à tout moment.

Administration de l'utilisation du KSN via le plug-in d'administration

Cette section explique comment configurer la tâche Utilisation du KSN et le Traitement des données via le Plug-in d'administration.

Configuration de la tâche Utilisation du KSN

Pour configurer la tâche Utilisation du KSN :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel de l'ordinateur**, cliquez sur le bouton **Configuration** de la sous-section **Utilisation du KSN**.

   La fenêtre **Utilisation du KSN** s'ouvre.

5. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :

   - Dans la section **Actions à exécuter sur les objets douteux selon KSN**, indiquez l'action que Kaspersky Embedded Systems Security doit exécuter en cas de détection d'un objet identifié comme infecté par le KSN :
     - **Supprimer**
     - **Consigner les informations**
   - Dans la section **Transfert de données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :
     - Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi à KSN si la taille du fichier est supérieure à (Mo)**.
     - Le cas échéant, modifiez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Embedded Systems Security calcule la somme de contrôle.
   - Dans la section **Serveur proxy du KSN**, cochez ou décochez la case **Utiliser Kaspersky Security Center en tant que serveur proxy du KSN**.

     Pour activer le proxy KSN, la Déclaration de KSN doit être acceptée et Kaspersky Security Center correctement configuré. Cf. *Système d'aide de Kaspersky Security Center* pour plus de détails.

6. Le cas échéant, configurez la planification du lancement de la tâche sous l'onglet **Administration des tâches**. Par exemple, vous pouvez démarrer la tâche planifiée et choisir la fréquence **Au lancement de l'application** si vous souhaitez que la tâche soit lancée automatiquement au redémarrage du périphérique protégé.

   L'application lancera la tâche Utilisation du KSN selon la planification.

7. Configurez le traitement des données avant de lancer la tâche.

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

Les modifications des paramètres de la tâche seront appliquées. La date et l'heure de modification des paramètres, ainsi que les informations sur les paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Configuration du traitement des données

Pour configurer les données qui seront traitées par les services KSN et accepter la déclaration de KSN, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Protection en temps réel de l'ordinateur**, cliquez sur le bouton **Traitement des données en cours** de la sous-section **Utilisation du KSN**.

   La fenêtre **Traitement des données KSN** s'ouvre.
5. Sous l'onglet **Statistiques et services**, lisez la Déclaration et cochez la case **J'accepte les conditions de participation au programme Kaspersky Security Network**.
6. Pour augmenter le niveau de protection, les cases suivantes sont automatiquement cochées :
   - **Envoyer des données sur les fichiers analysés**.
   - **Envoyer les statistiques de Kaspersky Security Network**.

   Vous pouvez décocher ces cases et arrêter d'envoyer des données supplémentaires à tout moment.
7. La case **Envoyer les statistiques de Kaspersky Security Network** est cochée par défaut. Vous pouvez décocher la case à tout moment si vous ne souhaitez pas que Kaspersky Embedded Systems Security envoie des statistiques complémentaires à Kaspersky.
8. Cliquez sur le bouton **OK**.

   La configuration du traitement des données sera enregistrée.

Administration de l'utilisation du KSN via la Console de l'application

Cette section explique comment configurer la tâche Utilisation du KSN et le Traitement des données via la Console de l'application.

Configuration de la tâche Utilisation du KSN

Pour configurer la tâche Utilisation du KSN :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Utilisation du KSN**.

3. Dans le volet résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.

4. Configurez les paramètres de la tâche :

   - Dans la section **Actions à exécuter sur les objets douteux selon KSN**, indiquez l'action que Kaspersky Embedded Systems Security doit exécuter en cas de détection d'un objet identifié comme infecté par le KSN :

     - **Supprimer**
     - **Consigner les informations**

   - Dans la section **Transfert de données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :

     - Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi à KSN si la taille du fichier est supérieure à (Mo)**.
     - Le cas échéant, modifiez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Embedded Systems Security calcule la somme de contrôle.

5. Le cas échéant, configurez la planification du lancement de la tâche sous les onglets **Planification** et **Avancé**. Par exemple, vous pouvez activer le lancement d'une tâche planifiée et choisir la fréquence de lancement **Au lancement de l'application** si vous souhaitez que la tâche soit lancée automatiquement après le redémarrage de l'appareil protégé.

   L'application lancera la tâche Utilisation du KSN selon la planification.

6. Configurez le Traitement des données avant de lancer la tâche.

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

Les modifications des paramètres de la tâche seront appliquées. La date et l'heure de modification des paramètres, ainsi que les informations sur les paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Configuration du traitement des données

Pour configurer les données qui seront traitées par les services KSN et accepter la déclaration de KSN, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Utilisation du KSN**.

3. Dans le volet résultats, cliquez sur le lien **Traitement des données en cours**.

   La fenêtre **Traitement des données** s'ouvre.

4. Sous l'onglet **Statistiques et services**, lisez la Déclaration et cochez la case **J'accepte les conditions de participation au programme Kaspersky Security Network**.

5. Pour augmenter le niveau de protection, les cases suivantes sont automatiquement cochées :

   - Envoyer des données sur les fichiers analysés.
   - Envoyer les statistiques de Kaspersky Security Network.

   Vous pouvez décocher ces cases et arrêter d'envoyer des données supplémentaires à tout moment.

6. La case Envoyer les statistiques de Kaspersky Security Network est cochée par défaut. Vous pouvez décocher la case à tout moment si vous ne souhaitez pas que Kaspersky Embedded Systems Security envoie des statistiques complémentaires à Kaspersky.

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

La configuration du traitement des données sera enregistrée.

Administration de l'utilisation du KSN via le Plug-in Web

Pour configurer la tâche Utilisation du KSN et le Traitement des données via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Utilisation du KSN**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Tâche Utilisation du KSN et Traitement des données via les paramètres du Plug-in d'administration

Paramètre	Description
Supprimer	Kaspersky Embedded Systems Security supprime l'objet considéré comme douteux selon les données du KSN et place une copie de celui-ci dans la sauvegarde. Cette option est sélectionnée par défaut.
Consigner les informations	Kaspersky Embedded Systems Security consigne dans le journal d'exécution de la tâche les informations sur l'objet considéré comme douteux selon les données du KSN. Kaspersky Embedded Systems Security ne supprime pas l'objet douteux.
Ne pas calculer la somme de contrôle avant l'envoi à KSN si la taille du fichier dépasse	La case active ou désactive le calcul de la somme de contrôle des fichiers d'une taille définie pour l'envoi de ces informations au service KSN. La durée du calcul de la somme de contrôle dépend de la taille du fichier. Si la case est cochée, Kaspersky Embedded Systems Security ne calcule pas la somme de contrôle pour les fichiers dont la taille dépasse la valeur définie (Mo). Si la case est décochée, Kaspersky Embedded Systems Security calcule la somme de contrôle pour les fichiers de n'importe quelle taille. Cette case est cochée par défaut.
J'accepte les	

conditions de participation à Kaspersky Security Network	En cochant cette case, vous confirmez que vous avez lu et accepté les dispositions de la Déclaration de Kaspersky Security Network.
Envoyer des données sur les fichiers analysés	Si la case est décochée, Kaspersky Embedded Systems Security envoie la somme de contrôle des fichiers analysés à Kaspersky. La conclusion sur la sécurité de chaque fichier est basée sur la réputation reçue de KSN. Si la case est décochée, Kaspersky Embedded Systems Security n'envoie pas la somme de contrôle des fichiers à KSN. Remarque : les demandes concernant la réputation du fichier peuvent être envoyées en mode limité. Les limitations servent à la protection des serveurs de réputation Kaspersky contre les DDoS. Dans ce scénario, les paramètres des demandes de réputation des fichiers, en cours d'envoi, sont définis par les règles et méthodes établies par les experts de Kaspersky. L'utilisateur ne peut pas les configurer sur un périphérique protégé. Les mises à jour de ces règles et méthodes sont reçues avec les mises à jour des bases de données de l'application. Si les limitations sont appliquées, l'état *activé par Kaspersky pour protégé les serveurs de KSN contre les attaques DDoS* apparaît dans les statistiques de la tâche Utilisation du KSN. Cette case est cochée par défaut.
Accepter de traiter les données comme une partie des statistiques de Kaspersky Security Network	Si la case est cochée, Kaspersky Embedded Systems Security envoie des statistiques supplémentaires qui peuvent contenir des données personnelles. La liste de toutes les données envoyées comme des statistiques KSN est spécifiée dans la Déclaration de KSN. Les données reçues par Kaspersky servent à améliorer la qualité des applications et le niveau des taux de détection des menaces. Si la case est décochée, Kaspersky Embedded Systems Security n'envoie pas de statistiques supplémentaires. Cette case est cochée par défaut.
Administration des tâches	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Configuration du transfert de données supplémentaires

Kaspersky Embedded Systems Security peut être configuré pour envoyer à Kaspersky les données suivantes :

- Sommes de contrôle des fichiers analysés (case **Envoyer des données sur les fichiers analysés**).
- Statistiques supplémentaires, y compris des données personnelles (case **Envoyer les statistiques de Kaspersky Security Network**).

Consultez la section « Traitement des données locales » de ce manuel pour plus d'information sur les données envoyées à Kaspersky.

Les cases correspondantes peuvent être cochées ou décochées uniquement si la case **J'accepte les conditions de participation au programme Kaspersky Security Network** est cochée.

Par défaut, Kaspersky Embedded Systems Security calcule les sommes de contrôle des fichiers et des statistiques supplémentaires après l'acceptation de la Déclaration de KSN.

L'état de la case **J'accepte les conditions de participation au programme Kaspersky Security Network** ne peut pas être modifié uniquement si la stratégie de Kaspersky Security Center interdit les modifications des paramètres de traitement des données.

États possibles de la case à cocher et conditions correspondante

État de la case	Conditions pour l'état de la case Envoyer des données sur les fichiers analysés.	Conditions pour l'état de la case Envoyer les statistiques de Kaspersky Security Network	Conditions pour l'état de la case J'accepte les conditions de participation au programme Kaspersky Security Network
☑	• Des demandes sur la réputation sont envoyées • Case modifiable	• Des statistiques supplémentaires sont envoyées • Case modifiable	• Les conditions de la Déclaration de Kaspersky Security Network sont acceptées • Case modifiable
☑	• Des demandes sur la réputation sont envoyées • Case non modifiable	• Des statistiques supplémentaires sont envoyées • Case non modifiable	• Les conditions de la Déclaration de Kaspersky Security Network sont acceptées • Case non modifiable
☐	• Aucune demande sur la réputation n'est envoyée • Case modifiable	• Aucune statistique supplémentaire n'est envoyée • Case modifiable	• Les conditions de la Déclaration de Kaspersky Security Network ne sont pas acceptées • Case modifiable
☐	• Aucune demande sur la réputation n'est envoyée • Case non modifiable	• Aucune statistique supplémentaire n'est envoyée • Case non modifiable	• Les conditions de la Déclaration de Kaspersky Security Network ne sont pas acceptées • Case non modifiable

Statistiques de la tâche Utilisation du KSN

Pendant l'exécution de la tâche Utilisation du KSN, vous pouvez consulter en temps réel des informations détaillées sur le nombre d'objets traités par Kaspersky Embedded Systems Security depuis son lancement jusqu'à maintenant. Les informations relatives à tous les événements survenus pendant l'exécution de la tâche sont enregistrées dans le Journal d'exécution de la tâche.

Pour consulter les statistiques de la tâche Utilisation du KSN :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Utilisation du KSN**.

Le panneau de détails du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Vous pouvez consulter les informations sur les objets que Kaspersky Embedded Systems Security a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Statistiques de la tâche Utilisation du KSN

Champ	Description
Erreurs d'envoi des requêtes	Nombre de requêtes à KSN dont le traitement a entraîné une erreur de tâche.
Statistiques collectées	Nombre de paquets de statistiques générés envoyés à KSN.
Objets supprimés	Nombre d'objets que Kaspersky Embedded Systems Security a supprimés suite au fonctionnement de la tâche Utilisation du KSN.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la sauvegarde par Kaspersky Embedded Systems Security.
Objets non supprimés	Nombre d'objets que Kaspersky Embedded Systems Security a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.
Objets non sauvegardés	Nombre d'objets dont Kaspersky Embedded Systems Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque. L'application ne désinfecte pas et ne supprime pas les fichiers qui n'ont pas pu être placés dans la sauvegarde. Les informations relatives à ces objets sont consignées dans le journal d'exécution de la tâche.
Mode limité	L'état indique si l'application envoie des requêtes sur la réputation des fichiers en mode limité. En mode limité, Kaspersky Embedded Systems Security n'envoie qu'une partie des demandes de réputation de fichiers selon les recommandations des experts de Kaspersky.

Protection contre les menaces réseau

Cette section contient des informations sur la tâche Protection contre les menaces réseau et les instructions sur la configuration de cette tâche.

À propos de la tâche Protection contre les menaces réseau

La Protection contre les menaces réseau ne peut être installée que sur un périphérique tournant sous Microsoft Windows 7 et toute version ultérieure ou Windows Server 2008 R2 et toute version ultérieure.

La tâche Protection contre les menaces réseau analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau ciblant votre ordinateur, Kaspersky Embedded Systems Security bloque l'activité réseau de l'ordinateur attaquant. Votre écran affiche alors un avertissement indiquant la tentative d'attaque réseau et affiche des informations sur l'ordinateur attaquant.

Par défaut, la tâche Protection contre les menaces réseau s'exécute dans le mode **Bloquer les connexions quand une attaque est détectée**. Dans ce mode, Kaspersky Embedded Systems Security ajoute à la liste des ordinateurs douteux les adresses IP des hôtes affichant l'activité typique des attaques réseau.

Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.

Les adresses IP des hôtes affichant une activité typique des attaques réseau sont supprimées de la liste des ordinateurs douteux dans les cas suivants :

- Kaspersky Embedded Systems Security est désinstallé.
- L'adresse IP a été supprimée manuellement de la liste des hôtes douteux.
- Le délai de blocage des hôtes a expiré.
- La tâche Protection contre les menaces réseau a été arrêtée et la case **Ne pas arrêter l'analyse du trafic quand la tâche n'est pas en cours d'exécution** n'est pas cochée.
- Le mode **Bloquer les connexions quand une attaque est détectée** été désactivé.

Paramètres de tâche Protection contre les menaces réseau par défaut

La tâche Protection contre les menaces réseau utilise les paramètres par défaut décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres de tâche Protection contre les menaces réseau par défaut

Paramètre	Valeur par défaut	Description
Mode de traitement	**Bloquer les connexions quand une attaque est détectée**	La tâche Protection contre les menaces réseau peut être démarrée en mode **Pass-through**, **Informer uniquement sur**

		les attaques réseau ou **Bloquer les connexions quand une attaque est détectée**. La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués. Le mode est sélectionné par défaut. Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués. Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée, mais ne bloque pas l'activité réseau de l'ordinateur attaquant. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, mais n'enregistre pas les événements concernant l'activité détectée et ne bloque pas l'activité réseau de l'ordinateur attaquant. Par exemple, vous pouvez utiliser ce mode en cas de diminution des performances du périphérique protégé.
Exclusions	La liste d'exclusion n'est pas appliquée.	Spécifiez les zones que vous souhaitez inclure dans la zone de protection de la tâche.
Paramètres de planification	Par défaut, la tâche Protection contre les menaces réseau se lance automatiquement au démarrage de Kaspersky Embedded Systems Security.	Vous pouvez configurer la planification.

Configuration de la tâche Protection contre les menaces réseau via la Console de l'application

Cette section explique comment administrer la tâche Protection contre les menaces réseau via l'interface de la Console de l'application.

Paramètres des tâches de groupe

Pour configurer les paramètres d'une tâche locale :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les menaces réseau**.
3. Dans le panneau de détails du nœud **Protection contre les menaces réseau**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Ouvrez l'onglet **Général**.
5. Dans la section **Mode de traitement**, indiquez le mode de traitement :

   - **Pass-through**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, mais n'enregistre pas les événements concernant l'activité détectée et ne bloque pas l'activité réseau de l'ordinateur attaquant.

     Par exemple, vous pouvez utiliser ce mode en cas de diminution des performances du périphérique protégé.

   - **Informer uniquement sur les attaques réseau**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée, mais ne bloque pas l'activité réseau de l'ordinateur attaquant.

   - **Bloquer les connexions quand une attaque est détectée**.

     La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

     Le mode est sélectionné par défaut.

     Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

     Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.
6. Cochez ou décochez la case **Ne pas arrêter l'analyse du trafic quand la tâche n'est pas en cours d'exécution**.

Si cette case est cochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security recherche dans le trafic réseau entrant toute activité typique des attaques réseau et bloque l'activité réseau de l'ordinateur attaquant en fonction du mode de traitement sélectionné.

Si cette case est décochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security ne recherche pas dans le trafic réseau entrant les activités typiques des attaques réseau et ne bloque pas l'activité réseau de l'ordinateur attaquant.

Cette case est décochée par défaut.

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

Ajout de règles d'exclusion

Pour ajouter des exclusions pour la tâche Protection contre les menaces réseau, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les menaces réseau**.
3. Dans le panneau de détails du nœud **Protection contre les menaces réseau**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Exclusions**, cochez la case **Ne pas contrôler les adresses IP exclues**.

   Si cette case est cochée, Kaspersky Embedded Systems Security n'analyse pas le trafic réseau entrant pour les adresses IP exclues.

   Si la case est décochée, Kaspersky Embedded Systems Security ne suit pas la liste d'exclusion.
5. Spécifiez l'adresse IP, puis cliquez sur le bouton **Ajouter**.
6. Cliquez sur le bouton **OK**.

Configuration de la tâche Protection contre les menaces réseau via le plug-in d'administration

Cette section explique comment gérer la tâche Protection contre les menaces réseau via l'interface du plug-in d'administration.

Paramètres des tâches de groupe

Pour configurer les paramètres d'une tâche locale :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel de l'ordinateur**, cliquez sur le bouton **Configuration** de la sous-section **Protection contre les menaces réseau**.

   La fenêtre **Protection contre les menaces réseau** s'ouvre.

5. Ouvrez l'onglet **Général**.

6. Dans la section **Mode de traitement**, indiquez le mode de traitement :

   - **Pass-through**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, mais n'enregistre pas les événements concernant l'activité détectée et ne bloque pas l'activité réseau de l'ordinateur attaquant.

     Par exemple, vous pouvez utiliser ce mode en cas de diminution des performances du périphérique protégé.

   - **Informer uniquement sur les attaques réseau**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée, mais ne bloque pas l'activité réseau de l'ordinateur attaquant.

   - **Bloquer les connexions quand une attaque est détectée**.

     La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

     Le mode est sélectionné par défaut.

     Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

     Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.

7. Cochez ou décochez la case **Ne pas arrêter l'analyse du trafic quand la tâche n'est pas en cours d'exécution**.

   Si cette case est cochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security recherche dans le trafic réseau entrant toute activité typique des attaques réseau et bloque l'activité réseau de l'ordinateur attaquant en fonction du mode de traitement sélectionné.

   Si cette case est décochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security ne recherche pas dans le trafic réseau entrant les activités typiques des attaques réseau et ne bloque pas l'activité réseau de l'ordinateur attaquant.

   Cette case est décochée par défaut.

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

Ajout de règles d'exclusion

Pour ajouter des exclusions pour la tâche Protection contre les menaces réseau, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel de l'ordinateur**, cliquez sur le bouton **Configuration** de la sous-section **Protection contre les menaces réseau**.

   La fenêtre **Protection contre les menaces réseau** s'ouvre.

5. Sous l'onglet **Exclusions**, cochez la case **Ne pas contrôler les adresses IP exclues**.

   Si cette case est cochée, Kaspersky Embedded Systems Security n'analyse pas le trafic réseau entrant pour les adresses IP exclues.

   Si la case est décochée, Kaspersky Embedded Systems Security ne suit pas la liste d'exclusion.

6. Spécifiez l'adresse IP, puis cliquez sur le bouton **Ajouter**.
7. Cliquez sur le bouton **OK**.

Configuration de la tâche Protection contre les menaces réseau via le Plug-in Web

Cette section explique comment gérer la tâche Protection contre les menaces réseau via l'interface du Plug-in Web.

Paramètres des tâches de groupe

Pour configurer les paramètres d'une tâche locale :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection contre les menaces réseau**.
6. Ouvrez l'onglet **Général**.
7. Dans la section **Mode de traitement**, indiquez le mode de traitement :

- Pass-through.

  Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, mais n'enregistre pas les événements concernant l'activité détectée et ne bloque pas l'activité réseau de l'ordinateur attaquant.

  Par exemple, vous pouvez utiliser ce mode en cas de diminution des performances du périphérique protégé.

- Informer uniquement sur les attaques réseau.

  Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée, mais ne bloque pas l'activité réseau de l'ordinateur attaquant.

- Bloquer les connexions quand une attaque est détectée.

La case active ou désactive l'ajout d'hôtes affichant l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau, enregistre les événements concernant l'activité détectée et ajoute les adresses IP des hôtes qui affichent l'activité typique des attaques réseau à la liste des ordinateurs bloqués.

Le mode est sélectionné par défaut.

Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

Vous pouvez restaurer l'accès aux ordinateurs bloqués et spécifier le nombre de jours, d'heures et de minutes après lesquels ces ordinateurs peuvent à nouveau accéder aux ressources de fichier réseau en configurant les paramètres de stockage des ordinateurs bloqués.

8. Cochez ou décochez la case **Ne pas arrêter l'analyse du trafic quand la tâche n'est pas en cours d'exécution**.

Si cette case est cochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security recherche dans le trafic réseau entrant toute activité typique des attaques réseau et bloque l'activité réseau de l'ordinateur attaquant en fonction du mode de traitement sélectionné.

Si cette case est décochée, lorsque la tâche Protection contre les menaces réseau est arrêtée, Kaspersky Embedded Systems Security ne recherche pas dans le trafic réseau entrant les activités typiques des attaques réseau et ne bloque pas l'activité réseau de l'ordinateur attaquant.

Cette case est décochée par défaut.

9. Cliquez sur le bouton **OK**.

Ajout de règles d'exclusion

Pour ajouter des exclusions pour la tâche Protection contre les menaces réseau, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection contre les menaces réseau**.
6. Sous l'onglet **Exclusions**, cochez la case **Ne pas contrôler les adresses IP exclues**.

Si cette case est cochée, Kaspersky Embedded Systems Security n'analyse pas le trafic réseau entrant pour les adresses IP exclues.

Si la case est décochée, Kaspersky Embedded Systems Security ne suit pas la liste d'exclusion.

7. Spécifiez l'adresse IP, puis cliquez sur le bouton **Ajouter**.
8. Cliquez sur le bouton **OK**.

Contrôle du lancement des applications

Cette section contient des informations sur la tâche de Contrôle du lancement des applications et les instructions sur la configuration de cette tâche.

A propos de la tâche Contrôle du lancement des applications

Dans le cadre de la tâche Contrôle du lancement des applications, Kaspersky Embedded Systems Security surveille les tentatives de lancement d'applications par l'utilisateur et autorise ou refuse ces lancements. La tâche Contrôle du lancement des applications repose sur le principe Interdire par défaut, ce qui signifie que toute application qui n'est pas autorisée dans les paramètres de la tâche sera bloquée automatiquement.

Vous pouvez autoriser le lancement des applications d'une des manières suivantes :

- définir des règles d'autorisation pour les applications de confiance ;
- Vérifier la réputation des applications de confiance dans KSN au moment de leur lancement.

Cette tâche accorde la plus haute priorité à l'interdiction du lancement des applications. Par exemple, si le lancement d'une application est interdit par une des règles de blocage, le lancement de l'application est interdit quelle que soit la conclusion de confiance du KSN. Dans ce cas, si les services KSN considèrent que l'application est douteuse, mais qu'elle est couverte par une règle d'autorisation, le démarrage de cette application sera interdit.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution de la tâche.

Le Contrôle du lancement des applications s'opère selon un des deux modes suivants :

- **Actif**. Kaspersky Embedded Systems Security contrôle, à l'aide de règles définies, le lancement des applications qui font partie de la zone d'application des règles du Contrôle du lancement des applications. La zone d'application des règles du Contrôle du lancement des applications peut être définie dans les paramètres de cette tâche. Si une application entre dans la zone d'application des règles du Contrôle du lancement des applications, et que les paramètres de la tâche ne respectent aucune des règles définie, le lancement de cette application sera interdit.

  Le lancement des applications n'entrant pas dans la zone d'application d'aucune règle définie dans les paramètres de la tâche Contrôle du lancement des applications est interdit, indépendamment des paramètres de la tâche Contrôle du lancement des applications.

  Il est impossible de lancer la tâche **Contrôle du lancement des applications** en mode Actif, si aucune règle n'a été créée ou s'il existe plus de 65 535 règles pour un appareil protégé.

- **Statistiques seulement**. Kaspersky Embedded Systems Security ne prend pas en charge les règles du Contrôle du lancement des applications pour autoriser ou interdire le lancement des applications. Il se content d'enregistrer les informations relatives aux lancements des applications, aux règles respectées par l'exécution des applications et aux actions qui auraient été exécutées si la tâche avait été lancée en mode **Actif**. Le lancement de toutes les applications est autorisé. Il s'agit du mode par défaut.

  Vous pouvez utiliser ce mode pour créer les règles du Contrôle du lancement des applications sur la base des informations consignées dans le journal d'exécution de la tâche.

Vous pouvez configurer le fonctionnement de la tâche Contrôle du lancement des applications conformément à un des scénarios suivants :

- Configuration des règles avancées et utilisation pour le Contrôle du lancement des applications.
- Configuration des règles de référence et Utilisation du KSN pour le Contrôle du lancement des applications.

Si des fichiers du système d'exploitation sont couverts par la tâche de Contrôle du lancement des applications, il est conseillé, lors de la création des règle du Contrôle du lancement des applications, de confirmer que ces applications sont autorisées par les nouvelles règles. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Kaspersky Embedded Systems Security intercepte également les processus lancés sous le Sous-système Windows pour Linux (sauf les scripts exécutés à partir du shell UNIX™ ou d'interpréteurs de ligne de commande). Pour ces processus, la tâche Contrôle du lancement des applications applique l'action définie par la configuration en cours. La tâche Génération des règles du Contrôle du lancement des applications détecte les lancements de l'application et génère les règles correspondantes pour les application exécutées sous le Sous-système Windows pour Linux.

A propos des règles du Contrôle du lancement des applications

Principe de fonctionnement des règles du Contrôle du lancement des applications

Le fonctionnement des règles du Contrôle du lancement des applications est basé sur les composantes suivantes :

- Type de règle.

  Les règles du Contrôle du lancement des applications peuvent autoriser ou interdire le lancement de l'application. Pour cette raison, il peut s'agir de règles *d'autorisation* ou de règles *d'interdiction*. Pour créer une liste de règles d'autorisation du Contrôle du lancement des applications, vous pouvez utiliser la tâche de génération des règles d'autorisation ou la tâche Contrôle du lancement des applications en mode **Statistiques seulement**. Il est également possible d'ajouter des règle d'autorisation manuellement.

- Utilisateur et/ou groupe d'utilisateurs.

  Les règles du Contrôle du lancement des applications contrôlent les lancements des applications définies par l'utilisateur et / ou le groupe d'utilisateurs.

- Zone d'application des règles.

  Les règles du Contrôle du lancement des applications peuvent s'appliquer aux *fichiers exécutables des applications*, aux *scripts* et aux *paquets MSI*.

- Critères de déclenchement de la règle.

  Les règles du Contrôle du lancement des applications contrôlent le lancement des fichiers répondant à un ou plusieurs critères définis dans les paramètres de la règle : signés par le *certificat numérique* indiqué, correspondant au *hash SHA256* indiqué, situés sur le *chemin indiqué* et correspondant aux arguments de la *ligne de commande*. Vous devez sélectionner au moins une option. Dans le cas contraire, la règle du Contrôle du lancement des applications n'est pas ajoutée.

  Si le critère de déclenchement de la règle est le paramètre **Certificat numérique**, la règle créée contrôle le lancement de n'importe quelle application de confiance dans le système d'exploitation. Vous pouvez créer des conditions plus strictes pour ce critère en cochant les cases suivantes :

  - **Utiliser l'objet**
  - **Utiliser l'empreinte**

L'empreinte limite de manière plus stricte le déclenchement des règles de lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée, à la différence de l'en-tête du certificat numérique.

Vous pouvez définir des exclusions pour une règle du Contrôle du lancement des applications. Les exclusions d'une règle du Contrôle du lancement des applications sont basées sur les mêmes critères que ceux déclenchant les règles : certificat numérique, hash SHA256 ou chemin d'accès au fichier. Des exclusions des règles du Contrôle du lancement des applications peuvent se justifier pour certaines règles d'autorisation : par exemple, si vous souhaitez permettre aux utilisateurs de lancer les applications depuis le chemin C:\Windows, mais que vous souhaitez interdire l'exécution du fichier Regedit.exe.

Si des fichiers du système d'exploitation sont couverts par la tâche de Contrôle du lancement des applications, il est conseillé, lors de la création des règle du Contrôle du lancement des applications, de confirmer que ces applications sont autorisées par les nouvelles règles. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Administration des règles du Contrôle du lancement des applications

Vous pouvez réaliser les opérations suivantes au niveau des règles du Contrôle du lancement des applications :

- Ajouter les règles manuellement.
- Créer et ajouter des règles automatiquement.
- Supprimer les règles.
- Exporter des règles dans un fichier de configuration.
- Vérifier si les fichiers sélectionnés contiennent des règles d'autorisation de leur lancement.
- Filtrer la liste des règles selon le critère spécifié.

A propos du contrôle de la distribution des logiciels

La création de règles du Contrôle du lancement des applications peut s'avérer complexe s'il faut contrôler également la distribution de logiciels sur un appareil protégé, par exemple sur les ordinateurs où le logiciel installé est automatiquement mis à jour à intervalles réguliers. Dans ce cas, la liste de règles d'autorisation doit être mise à jour après chaque mise à jour de logiciel afin que les fichiers juste créés soient pris en compte dans les paramètres de la tâche Contrôle du lancement des applications. Pour simplifier le contrôle du lancement dans les scénarios de distribution des logiciels, vous pouvez utiliser le sous-système Contrôle de la distribution des logiciels.

Un *paquet de distribution des logiciels* (ci-après appelé « paquet ») représente une application logicielle à installer sur un périphérique protégé. Chaque paquet contient au moins une application et peut également contenir des fichiers séparés, des mises à jour, voire une commande séparée en plus des applications, notamment lorsque vous installée une application ou une mise à jour logicielle.

Le sous-système Contrôle de la distribution des logiciels est mis en œuvre en tant que liste supplémentaire d'exclusions. Quand vous ajoutez un paquet de distribution de logiciels à cette liste, l'application autorise la décompression de ces paquets de confiance ainsi que le lancement automatique de l'installation ou la modification par un paquet de confiance. Les fichiers extraits peuvent hériter de l'attribut de confiance du paquet de distribution principal. Un *paquet de distribution principal* est un paquet qui a été ajouté à la liste d'exclusions du Contrôle de la distribution des logiciels par l'utilisateur et qui est devenu un paquet de confiance.

Kaspersky Embedded Systems Security contrôle uniquement les cycles de distribution de logiciels complets. L'application ne peut pas traiter correctement le lancement des fichiers qui sont modifiés par un paquet de confiance si, lors du premier lancement du paquet, le Contrôle de la distribution des logiciels est désactivé ou si le composant Contrôle du lancement des applications n'est pas installé.

Le Contrôle de la distribution des logiciels n'est pas disponible si la case **Utiliser les règles pour les fichiers exécutables** est décochée dans les paramètres de la tâche Contrôle du lancement des applications.

Cache de la distribution des logiciels

Kaspersky Embedded Systems Security établit le rapport entre les paquets de confiance et les fichiers créés lors de la distribution des logiciels à l'aide d'un cache de la distribution des logiciels généré automatiquement ("cache de distribution"). Au premier lancement d'un paquet, Kaspersky Embedded Systems Security détecte tous les fichiers créés par ce paquet lors de du processus de distribution de logiciels et stocke les sommes de contrôles et les chemins d'accès des fichiers dans le cache de distribution. Ensuite, le lancement de tous les fichiers repris dans le cache de distribution est autorisé par défaut.

Vous ne pouvez pas réviser, effacer ou modifier manuellement le cache de distribution via l'interface utilisateur. Le cache est rempli et contrôlé par Kaspersky Embedded Systems Security.

Vous pouvez exporter le cache de distribution dans un fichier de configuration (au format XML) et aussi effacer le cache à l'aide des options de ligne de commande.

Pour exporter le cache de distribution dans un fichier de configuration, exécutez la commande suivante :

```
kavshell appcontrol /config /savetofile:<chemin complet> /sdc
```

Pour effacer le cache de distribution, exécutez la commande suivante :

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security met à jour le cache de distribution toutes les 24 heures. En cas de modification de la somme de contrôle d'un fichier qui était autorisé, l'application supprime l'enregistrement de ce fichier dans le cache de distribution. Si la tâche Contrôle du lancement des applications est lancée en mode actif, les tentatives de lancement ultérieures de ce fichier sont bloquées. Si le chemin complet d'accès au fichier précédemment autorisé est modifié, les tentatives ultérieures de démarrer ce fichier ne seront pas bloquées car la somme de contrôle est stockée dans le cache de distribution.

Traitement des fichiers extraits

Tous les fichiers extraits d'un paquet de confiance hérite de l'attribut de confiance au premier lancement du paquet. Si vous décochez la case après le premier lancement, tous les fichiers extraits du paquet conservent l'attribut hérité. Pour réinitialiser l'attribut hérité sur tous les fichiers extraits, vous devez effacer le cache de distribution et décocher la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution** avant de redémarrer le paquet de distribution de confiance.

Les fichiers extraits et les paquets, créés par un paquet de distribution principal de confiance, acquièrent l'attribut de confiance quand leurs sommes de contrôle sont ajoutées au cache de distribution lorsque le paquet de distribution de logiciels de la liste d'exclusions est ouvert pour la première fois. Par conséquent, le paquet de distribution proprement dit et tous les fichiers inclus sont également de confiance. Par défaut, le nombre de niveaux d'héritage d'attribut de confiance est illimité.

Les fichiers extraits conservent l'attribut de confiance après le redémarrage du système d'exploitation.

Pour configurer le traitement des fichiers dans les paramètres de contrôle de la distribution des logiciels, vous devez cocher ou décocher la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution**.

Par exemple, supposons que vous ajoutez un paquet test.msi contenant plusieurs autres paquets et applications à la liste d'exclusions et cochez la case. Dans ce cas, tous les paquets et applications contenus dans le paquet test.msi peuvent être exécutés ou extraits s'ils contiennent d'autres fichiers. Ce scénario est valable pour les fichiers extraits sur tous les niveaux imbriqués.

Si vous ajoutez un paquet test.msi à la liste d'exclusions et décochez la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution**, l'application affecte l'attribut de confiance uniquement aux paquets et aux fichiers exécutables extraits directement d'un paquet de confiance principal (imbriqué au premier niveau). Les sommes de contrôle de ces fichiers sont stockées dans le cache de distribution. Tous les fichiers imbriqués au second niveau et plus sont bloqués par le principe Interdire par défaut.

Utilisation de la liste des règles du Contrôle du lancement des applications

La liste des paquets de confiance du sous-système de contrôle de la distribution des logiciels est une liste d'exclusions, ce qui amplifie, mais ne remplace pas la liste générale de règles de contrôle du lancement des applications.

Les règles d'interdiction de contrôle du lancement des applications a la priorité la plus élevé : la décompression des paquets de confiance et le démarrage de fichiers nouveaux ou modifiés sont bloqués si ces paquets est fichiers sont affectés par les règles d'interdiction du contrôle du lancement des applications.

Les exclusions de contrôle de la distribution des logiciels sont appliquées à la fois pour les paquets de confiance et les fichiers créés ou modifiés par ces paquets si aucune règle d'interdiction dans la liste de contrôle du lancement des applications n'est appliquée pour ces paquets et fichiers.

Utilisation des conclusions KSN

Les conclusions de KSN sur le caractère douteux d'un fichier ont priorité sur les exclusions du Contrôle de la distribution des logiciels : la décompression des paquets de confiance et le lancement des fichiers créés ou modifiés par ces paquets sont interdits si KSN signale que ces fichiers sont douteux.

Ensuite, après le décompactage à partir d'un programme de confiance, tous les fichiers enfants pourront s'exécuter, quelle que soit l'utilisation du KSN dans la zone Contrôle du lancement des applications. Dans ce cas, les états des cases **Interdire les applications douteuses selon le KSN** et **Autoriser les applications de confiance selon le KSN** n'affectent pas le fonctionnement de la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution**.

A propos l'utilisation du KSN dans la tâche Contrôle du lancement des applications

Vous devez accepter la Déclaration de KSN afin de lancer la tâche Utilisation du KSN.

Si les données de KSN relatives à la réputation d'une application sont utilisées par la tâche du Contrôle du lancement des applications, la réputation de l'application selon KSN est considérée comme un critère d'autorisation ou d'interdiction du lancement de cette application. Si KSN signale à Kaspersky Embedded Systems Security qu'une application est douteuse lorsque l'utilisateur tente de la lancer, le lancement est refusé. Si KSN signale à Kaspersky Embedded Systems Security qu'une application est de confiance lorsque l'utilisateur tente de la lancer, le lancement est autorisé. Vous pouvez appliquer KSN avec les règles du Contrôle du lancement des applications ou à titre de critère indépendant pour interdire le lancement des applications.

Application des conclusions du KSN en tant que critère indépendant de l'interdiction du lancement des applications

Ce scénario permet de contrôler sans danger le lancement des applications sur un appareil protégé sans configuration avancée de la liste des règles.

Vous pouvez appliquer les conclusions du KSN à Kaspersky Embedded Systems Security avec la seule règle définie. L'application autorisera uniquement le lancement d'applications considérées comme des applications de confiance dans KSN ou qui sont autorisées par une règle définie.

Si vous adoptez ce scénario, il est conseillé de définir une règle d'autorisation du lancement des applications selon un certificat numérique.

Toutes les autres applications seront bloquées conformément à la stratégie Interdire par défaut. L'application du KSN en l'absence de règles permet de protéger l'appareil contre les applications qui constituent une menace d'après KSN.

Application des conclusions du KSN avec les règles du Contrôle du lancement des applications

Lors de l'utilisation des conclusions du KSN avec les règles du Contrôle du lancement des applications, les conditions suivantes s'appliquent :

- Kaspersky Embedded Systems Security interdit toujours le lancement d'une application si elle est couverte par au moins une règle d'interdiction. Si l'application est considérée comme une application de confiance par KSN, la conclusion correspondante possède une priorité inférieure et n'est pas prise en compte ; le lancement l'application sera toujours interdit. Cela permet de développer la liste des applications bloquées.

- Kaspersky Embedded Systems Security interdit toujours le lancement d'une application si le lancement est interdit pour les applications considérées comme douteuses dans KSN et qu'il s'avère que cette application est considérée comme douteuse dans KSN. Si une règle d'autorisation a été définie pour l'application, elle possède une priorité inférieure et n'est pas prise en compte ; l'application sera de toute manière interdite. Cela permet de protéger l'appareil contre les applications qui constituent une menace d'après les données du KSN et qui n'ont pas été prises en considération lors de la configuration initiale des règles.

A propos de la génération des règles du Contrôle du lancement des applications

Vous pouvez créer des listes de règles du Contrôle du lancement des applications à l'aide de tâches et de stratégies de Kaspersky Security Center simultanément pour tous les appareils protégés et groupes d'appareils protégés du réseau de l'organisation. Les scénarios énumérés ci-dessous sont recommandés si le réseau de l'organisation ne comporte pas une machine modèle et si vous n'êtes pas en mesure de créer une liste de règles d'autorisation sur la base des applications installées sur cette machine modèle.

Vous pouvez exécuter localement la tâche Génération des règles du Contrôle du lancement des applications via la Console de l'application pour créer une liste de règles basées sur les applications exécutées sur un seul périphérique protégé.

Le composant Contrôle du lancement des applications est installé avec deux règles d'autorisation prédéfinies :

- Règle d'autorisation pour les scripts et les paquets Windows Installer dotés d'un certificat reconnu par le système d'exploitation.
- Règle d'autorisation pour les fichiers exécutables dotés d'un certificat reconnu par le système d'exploitation.

Vous pouvez créer des listes de règles du Contrôle du lancement des applications dans Kaspersky Security Center d'une des manières suivantes :

- Avec l'aide d'une tâche de groupe Génération des règles du Contrôle du lancement des applications.

  Dans ce scénario, une tâche de groupe crée pour chaque appareil protégé du réseau sa propre liste de règles du Contrôle du lancement des applications et les enregistre dans un fichier XML dans le dossier partagé indiqué. Le fichier XML créé par la tâche Génération des règles du Contrôle du lancement des applications contient les règles d'autorisation définies dans les paramètres de la tâche avant le lancement de la tâche. Aucune règle ne sera créée pour les applications dont le lancement n'est pas autorisé par les paramètres définis de la tâche. Le lancement de ces applications est interdit par défaut. Par la suite, vous pouvez importer manuellement les listes de règles créées dans la tâche Contrôle du lancement des applications pour la stratégie Kaspersky Security Center.

  Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles de la tâche Contrôle du lancement des applications.

  Il est recommandé d'utiliser ce scénario quand il faut créer rapidement des listes de règles du Contrôle du lancement des applications. Nous conseillons de configurer le lancement de la tâche Génération des règles du Contrôle du lancement des applications selon une planification uniquement si la zone d'application des règles d'autorisation contient des dossiers et des fichiers réputés sûrs.

  Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier partagé a été configuré pour tous les appareils protégés. Au cas où l'utilisation d'un dossier partagé n'est pas prévue par la stratégie de l'organisation, nous vous conseillons de lancer la tâche Génération des règles du Contrôle du lancement des applications sur un périphérique protégé appartenant à un groupe de périphériques protégés d'essai ou sur une machine modèle.

- Sur la base du rapport relatif aux événements de la tâche généré dans Kaspersky Security Center pour le fonctionnement du Contrôle du lancement des applications en mode **Statistiques seulement**.

Dans le cadre de ce scénario, Kaspersky Embedded Systems Security n'interdit pas le lancement des applications. Au contraire, alors que le Contrôle du lancement des applications fonctionne en mode **Statistiques seulement**, il signale toutes les interdictions et autorisation de lancement d'application sur l'ensemble des appareils protégés du réseau dans la section **Événements** de l'espace de travail du nœud Serveur d'administration dans Kaspersky Security Center. Kaspersky Security Center utilise les rapports pour crée une liste unique d'événements caractérisés par l'interdiction du lancement de l'application.

Il faut configurer la période d'exécution de la tâche de telle sorte que tous les scénarios envisageables qui impliquent tous les appareils protégés et les groupes d'appareils protégés et qu'au moins le redémarrage d'un appareil protégé puisse être réalisé au cours de l'intervalle indiqué. Après la fin de la période d'exécution des tâches, vous pouvez importer les données relatives aux lancements d'application depuis le fichier de rapport sur les événements de Kaspersky Security Center enregistré au format TXT et créer, sur la base de ces données, des règles d'autorisation pour le Contrôle du lancement des applications.

Ce scénario est recommandé si le réseau de l'entreprise compte un nombre important d'appareils protégés de types différents (et dotés de logiciels différents).

- Sur la base des événements d'interdiction de lancement des applications reçus via Kaspersky Security Center, sans création et importation du fichier de configuration.

  Pour pouvoir exploiter cette possibilité, la tâche Contrôle du lancement des applications sur l'appareil protégé doit être placée sous une stratégie active de Kaspersky Security Center. Dans ce cas, tous les événements sur l'appareil protégés sont transmis au Serveur d'administration.

Nous conseillons d'actualiser les listes de règles après toute modification de la composition des applications installées sur les appareils protégés du réseau (par exemple, en cas d'installation d'une mise à jour ou de réinstallation du système d'exploitation). Il est conseillé de créer une liste mise à jour de règles en exécutant la tâche Génération des règles du Contrôle du lancement des applications ou la tâche Contrôle du lancement des applications en mode **Statistiques seulement** sur les appareils protégés du groupe d'administration test. Le groupe d'administration d'essai réunit les appareils protégés indispensables à la vérification du lancement de nouvelles applications avant leur installation sur les appareils protégés du réseau.

Les fichiers XML qui contiennent la liste des règles d'autorisation, sont créés sur la base de l'analyse des tâches lancées sur l'appareil protégé. Pour comptabiliser toutes les applications utilisées sur le réseau lors de la création des listes de règles, il est conseillé de lancer la tâche Génération des règles du Contrôle du lancement des applications en mode **Statistiques seulement** sur une machine modèle.

Avant de créer des règles d'autorisation sur la base des applications lancées sur une machine modèle, assurez-vous que celle-ci est sûre et qu'elle n'est infectée par aucune application malveillante.

Avant d'ajouter des règles d'autorisation, sélectionnez un des modes d'application de règle disponible. La liste des règles de la stratégie de Kaspersky Security Center affiche uniquement les règles définies dans cette stratégie, quel que soit le mode d'application des règles. La liste des règles locale affiche toutes les règles appliquées, quelles soient locales ou ajoutées via une stratégie.

Paramètres de la tâche Contrôle du lancement des applications par défaut

La tâche Contrôle du lancement des applications possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres de la tâche Contrôle du lancement des applications par défaut

Paramètre	Valeur par défaut	Description

Mode de tâche	**Statistiques seulement**. La tâche enregistre les lancements interdits et autorisés sur la base des règles définies. Le lancement de l'application n'est pas interdit.	Vous pouvez sélectionner le mode **Actif** après la création de la liste définitive des règles.
Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs	Pas appliqué	Vous pouvez répéter les actions adoptées au premier lancement du fichier à tous ses lancements ultérieurs.
Interdire le lancement de l'interpréteur de commande sans commande à exécuter	Pas appliqué.	Vous pouvez interdire le lancement des interpréteurs de ligne commande sans commande à exécuter.
Gestion des règles	**Ajouter les règles de la stratégie aux règles locales**	Vous pouvez choisir le mode d'application commune des règles spécifiées dans la stratégie et les règles sur l'appareil protégé.
Zone d'application de la règle	La tâche contrôle le lancement des fichiers exécutables, des scripts et des paquets MSI. La tâche contrôle également le chargement des modules DLL.	Vous pouvez indiquer les types de fichier dont le lancement sera contrôlé par les règles.
Utilisation du KSN	Les données de KSN relatives à la réputation des applications ne sont pas utilisées.	Vous pouvez utiliser les données sur la réputation des applications de KSN dans le fonctionnement de la tâche Contrôle du lancement des applications.
Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste	Pas appliqué.	Vous pouvez autoriser la diffusion de l'application à l'aide des paquets d'installation et des applications indiqués dans les paramètres. Par défaut, seule l'autorisation des applications à l'aide du service Windows Installer est autorisée.
Toujours autoriser la diffusion de logiciel via Windows Installer	Appliqué (peut être modifié uniquement lorsque le paramètre **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** est activé).	Vous pouvez autoriser l'installation ou la mise à jour de n'importe quel logiciel si les opérations sont exécutées via Windows Installer.
Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)	Non appliqué (peut être modifié uniquement lorsque le paramètre **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** est activé).	Vous pouvez activer ou désactiver la diffusion automatique du logiciel à l'aide de la solution System Center Configuration Manager.
Lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

Paramètre	Valeur par défaut	Description
Préfixe des noms des règles d'autorisation	Correspond au nom du périphérique protégé sur lequel Kaspersky Embedded Systems Security est installé.	Vous pouvez modifier le préfixe des noms des règles d'autorisation.
Zone d'application des règles d'autorisation	La zone d'application des règles d'autorisation reprend par défaut les catégories de fichiers suivantes : • Fichiers portant l'extension EXE et placés dans les dossiers C:\Windows, C:\Program Files (x86) et C:\Program Files ; • Paquets MSI, placés dans le dossier C:\Windows ; • Scripts placés dans le dossier C:\Windows. La tâche crée également des règles pour toutes les applications déjà en cours d'exécution, quels que soient leur emplacement ou leur format.	Vous pouvez modifier la zone de protection en ajoutant ou en supprimant des chemins d'accès aux dossiers et en définissant les types de fichiers dont le lancement sera autorisé par les règles créées automatiquement. Vous pouvez également ne pas tenir compte des applications déjà en cours d'exécution lors de la création des règles d'autorisation.
Critères de génération de règles d'autorisation.	Utilisation de l'en-tête et de l'empreinte du certificat numérique ; les règles sont générées pour tous les utilisateurs et groupes d'utilisateurs.	Vous pouvez utiliser le hash SHA256 lors de la génération de règles d'autorisation. Vous pouvez sélectionner l'utilisateur ou le groupe d'utilisateurs pour lesquels les règles d'autorisation doivent être générées automatiquement.
Actions une fois la tâche terminée	Les règles d'autorisation sont ajoutées à la liste des règles du Contrôle du lancement des applications ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont supprimés.	Vous pouvez ajouter des règles aux règles existantes sans fusion et sans suppression des doublons, ou remplacer les règles existantes par de nouvelles règles d'autorisation, ainsi que configurer les paramètres d'exportation des règles d'autorisation dans un fichier.
Paramètres du lancement de la tâche avec autorisations	La tâche est lancée sous les autorisations du compte système.	Vous pouvez autoriser le lancement de la tâche de Génération des règles du Contrôle du lancement des applications sous l'autorisation du compte système ou du compte d'un utilisateur que vous aurez choisi.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Génération des règles du Contrôle du lancement des applications n'est pas lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

Administration du Contrôle du lancement des applications via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des appareils protégés du réseau.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la stratégie pour la tâche Contrôle du lancement des applications

Pour accéder aux paramètres de la tâche Contrôle du lancement des applications via une stratégie de Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle du lancement des applications**.
   La fenêtre **Contrôle du lancement des applications** s'ouvre.

Configurez la stratégie en fonction des besoins.

Accès à la liste des règles du Contrôle du lancement des applications

Pour accéder à la liste des règles du Contrôle du lancement des applications via Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.

5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.

6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.

7. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

Configurez la liste des règles en fonction des besoins.

Ouverture de l'assistant de la tâche Génération des règles du Contrôle du lancement des applications

Pour créer une tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.

3. Sélectionnez l'onglet **Tâches**.

4. Cliquez sur le bouton **Créer une tâche**.

   La fenêtre **Assistant de nouvelle tâche** s'ouvre.

5. Sélectionnez la tâche **Génération des règles du Contrôle du lancement des applications**.

6. Cliquez sur **Suivant**.

   La fenêtre **Configuration** s'ouvre.

Pour configurer la tâche existante Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.

3. Sélectionnez l'onglet **Tâches**.

4. Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** s'ouvre.

Consultez la section Configuration de la tâche Génération des règles du Contrôle du lancement des applications pour en savoir plus sur la configuration de la tâche.

Configuration des paramètres de la tâche Contrôle du lancement des applications

Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Contrôle du lancement des applications**.

2. Sous l'onglet **Général**, sélectionnez les paramètres suivants dans la section **Mode de tâche** :

   - Dans la liste déroulante **Mode de tâche**, définissez le mode de la tâche.
   - Décochez ou cochez la case Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs.
   - Décochez ou cochez la case Interdire le lancement de l'interpréteur de commande sans commande à exécuter.

3. Dans la section **Gestion des règles**, configurez les paramètres d'application des règles :

   a. Cliquez sur le bouton **Liste des règles** pour ajouter des règles d'autorisation de la tâche Contrôle du lancement des applications.

   > Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

   b. Sélectionnez le mode d'application des règles :

   - **Remplacer les règles locales par les règles de la stratégie**.

     L'application applique la liste de règles indiquées dans la stratégie dans le cadre du contrôle centralisé du lancement des applications sur le groupe d'appareils protégés. La création, la modification ou l'application de règles locales ne sont pas disponibles.

   - **Ajouter les règles de la stratégie aux règles locales**.

     L'application applique la liste de règles définie dans la stratégie en même temps que les listes de règles locales. Vous pouvez modifier les listes de règles locales à l'aide de tâches de Génération des règles du Contrôle du lancement des applications.

4. Définissez les paramètres suivants dans la section **Zone d'application de la règle** :

   - **Utiliser les règles pour les fichiers exécutables**.
   - **Contrôle du chargement des modules DLL**.

   > Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation.

   - **Utiliser les règles pour les scripts et les paquets MSI**.

5. Dans la zone **Utilisation du KSN**, configurez les paramètres suivants du lancement des applications :

   - **Interdire les applications douteuses selon le KSN**.
   - **Autoriser les applications de confiance selon le KSN**.
   - Utilisateurs et/ou groupes d'utilisateurs pour lesquels le lancement d'applications considérées comme des applications de confiance dans le KSN est autorisé.

6. Sous l'onglet **Contrôle de la distribution des logiciels**, configurez les paramètres du contrôle de distribution des logiciels.

7. Sous l'onglet **Administration des tâches**, configurez les paramètres du lancement de la tâche programmée.

8. Cliquez sur **OK** dans la fenêtre **Contrôle du lancement des applications**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Configuration du contrôle de la distribution des logiciels

Pour ajouter un paquet de distribution de confiance, procédez comme suit :

1. Ouvrez la fenêtre **Contrôle du lancement des applications**.

2. Sous l'onglet **Contrôle de la distribution des logiciels**, cochez la case Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste.

> Vous pouvez cocher la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** si la case **Utiliser les règles pour les fichiers exécutables** sous l'onglet **Général** est cochée dans les paramètres de la tâche **Contrôle du lancement des applications**.

3. Le cas échéant, décochez la case **Toujours autoriser la diffusion de logiciel via Windows Installer**

> Il est conseillé de décocher la case **Toujours autoriser la diffusion de logiciel via Windows Installer** uniquement dans les cas extrêmes. La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.

4. Le cas échéant, cochez la case Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS).

> L'application contrôle le cycle de distribution de logiciels sur l'appareil protégé, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de l'application sur l'appareil protégé.

5. Pour créer une liste d'autorisation ou pour modifier la liste des paquets de distribution de confiance, cliquez sur le bouton **Modifier la liste de paquets** et sélectionnez une des méthodes suivantes dans la fenêtre qui s'ouvre :

- **Ajouter un paquet de distribution**.

  a. Cliquez sur le bouton **Parcourir**.

  b. Sélectionnez le fichier exécutable ou le paquet de distribution.

  Les données du fichier sélectionné sont ajoutées automatiquement à la section **Critères de confiance**.

c. Cochez ou décochez la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution**.

d. Choisissez une de deux options proposées pour les critères de confiance qui vont déterminer si un fichier ou un paquet d'installation peut être considéré comme étant de confiance :

- **Utiliser un certificat numérique**
- **Utiliser le hash SHA256**

- **Ajouter plusieurs paquets selon le hash**.

  Vous pouvez choisir un nombre illimité de fichiers de lancement et de paquets d'installation et les ajouter simultanément à la liste. Kaspersky Embedded Systems Security tient compte du hash et autorise le lancement le système d'exploitation à lancer les fichiers indiqués.

- **Modifier le paquet sélectionné**.

  Cette option permet de sélectionner un autre fichier de lancement ou un autre paquet d'installation. Elle permet également la modification des critères de confiance.

- Importer la liste des paquets de distribution depuis un fichier

  Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des paquets de distribution de confiance.

6. Si vous voulez supprimer de la liste des éléments de confiance une application ou un paquet d'installation qui avait été ajouté antérieurement, cliquez sur le bouton **Supprimer les paquets d'installation**. Le lancement des fichiers extraits sera autorisé.

   Pour interdire le lancement des fichiers extraits, désinstallez l'application de l'appareil protégé ou créez une règle d'interdiction dans les paramètres de la tâche Contrôle du lancement des applications.

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

Les nouvelles valeurs des paramètres seront enregistrés.

Configuration de la tâche Génération des règles du Contrôle du lancement des applications

Pour configurer la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications**.

2. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

3. La section **Configuration** permet de configurer les paramètres suivants :

- Ajoutez un préfixe pour les noms des règles.
- Sélectionnez comment créer des règles d'autorisation :
  - Créer des règles d'autorisation sur la base des applications en cours d'exécution
  - Créer des règles d'autorisation pour les applications des dossiers

4. Vous pouvez indiquer les actions à réaliser lors de la création des règles d'autorisation du Contrôle du lancement des applications dans la section **Options** :
   - Utiliser un certificat numérique
   - Utiliser l'objet et l'empreinte du certificat numérique
   - En cas d'absence de certificat, utiliser
     - **Hash SHA256**. La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
     - **chemin du fichier**. Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.
   - Utiliser le hash SHA256
   - Créer des règles pour un utilisateur ou un groupe d'utilisateurs

   Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.
5. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).
6. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.
7. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.
8. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

   Les paramètres de la tâche de groupe définis seront enregistrés.

Configuration des règles du Contrôle du lancement des applications via Kaspersky Security Center

Apprenez à créer une liste de règles sur la base de différents critères ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle du lancement des applications.

Ajout d'une règle du Contrôle du lancement des applications

Pour ajouter une règle du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.

   La fenêtre **Paramètres de règle** s'ouvre.
4. Spécifiez les paramètres suivants :
   a. Dans le champ **Nom**, saisissez le nom de la règle.
   b. Dans la liste déroulante **Type**, sélectionnez le type de règle :
      - **Autorisation**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
      - **Interdiction**, si vous souhaitez que la règle interdise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
   c. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
      - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
      - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
   d. Dans le champ **Utilisateur ou groupe d'utilisateurs**, indiquez les utilisateurs qui pourront ou non lancer des applications en fonction du type de règle. Pour ce faire, procédez comme suit :
      1. Cliquez sur le bouton **Parcourir**.
      2. La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.
      3. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.
      4. Cliquez sur le bouton **OK**.
   e. Réalisez les opérations suivantes si vous souhaitez extraire les valeurs pour les critères de déclenchement de la règle listés dans la section **Critères de déclenchement de la règle**, depuis un fichier :
      1. Cliquez sur le bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**.

         La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.
      2. Sélectionnez le fichier.

3. Cliquez sur le bouton **Ouvrir**.

   Les valeurs des critères dans le fichier sont affichées dans les champs de le groupe **Critères de déclenchement de la règle**. Par défaut, c'est le premier critère de la liste dont les données figurent dans les propriétés du fichier qui est sélectionné.

f. Dans le groupe **Critères de déclenchement de la règle**, sélectionnez une ou plusieurs des options suivantes selon les cas :

- **Certificat numérique**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique :
  - Cochez la case **Utiliser l'objet**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'en-tête indiqué.
  - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle uniquement le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'empreinte indiquée.
- **Hash SHA256**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers dont la somme de contrôle correspond à celle indiquée.
- **Chemin du fichier**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.
  - **Ligne de commande** si vous souhaitez que la règle contrôle les applications lancées à l'aide des arguments indiqués dans le champ de la ligne de commande. Le champ est activé une fois que vous avez sélectionné l'option **Chemin d'accès au fichier**. Vous pouvez utiliser ? et * comme masque lors de la définition des arguments de la ligne de commande pour les processus lancés en tant que critère.

> Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

> Lors de la désignation des objets, vous pouvez utiliser ? et * en tant que masques de fichiers.

Vous devez sélectionner au moins une option. Dans le cas contraire, la règle du Contrôle du lancement des applications n'est pas ajoutée.

g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :

1. Dans la section **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion de la règle** s'ouvre.

2. Dans le champ **Nom**, saisissez le nom de l'exclusion.

3. Indiquez les paramètres d'exclusions des fichiers des applications de la règle du Contrôle du lancement des applications. Vous pouvez remplir les champs des paramètres depuis les propriétés du fichier en cliquant sur le bouton **Définir l'exclusion selon les propriétés du fichier**.

   - Certificat numérique
   - **Utiliser l'objet**
   - **Utiliser l'empreinte**

- Hash SHA256
- Chemin du fichier

4. Cliquez sur le bouton **OK**.
5. Si nécessaire, répétez les étapes (i) à (iv) pour ajouter des exclusions supplémentaires.

5. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

Activation du mode Autoriser par défaut

La règle Autoriser par défaut autorise le lancement de toutes les applications si celui-ci n'est pas interdit par des règles ou par une conclusion de KSN qui les considère comme douteuses. Il est possible d'activer le mode Autoriser par défaut en ajoutant des règles d'autorisation spécifiques. Vous pouvez activer Autoriser par défaut uniquement pour les scripts ou pour tous les fichiers exécutables.

Pour ajouter une nouvelle règle Autoriser par défaut :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez **Ajouter une règle**.
   La fenêtre **Paramètres de règle** s'ouvre.
3. Dans le champ **Nom**, saisissez le nom de la règle.
4. Dans la liste déroulante **Type**, sélectionnez le type de règle **Autorisation**.
5. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
   - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
   - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
6. Dans le groupe **Critères de déclenchement de la règle**, sélectionnez l'option **Chemin du fichier**.
7. Saisissez le masque suivant : `?:\`
8. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security applique le mode Autoriser par défaut.

Création de règles d'autorisation au départ d'événements de Kaspersky Security Center

Afin de créer des règles d'autorisation pour les applications au départ des événements de Kaspersky Security Center dans le Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Créer des règles d'autorisation des applications à partir des événements de Kaspersky Security Center**.

3. Sélectionnez le principe d'ajout des règles à la liste des règles du Contrôle du lancement des applications déjà créées :

   - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
   - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   La fenêtre **Génération des règles du Contrôle du lancement des applications** s'ouvre.

4. Sélectionnez les types d'événements qui vont être utilisé par la tâche de création de règle :

   - **mode Statistiques seulement : lancement de l'application interdit**.
   - **Lancement de l'application interdit**.

5. Sélectionnez la période dans la liste déroulante **Événements de requête générés au cours de la période**.

6. Cochez ou décochez la case **Accorder une priorité supérieure à l'utilisation du hash lors de la création de règles**.

   Si la case est cochée, Kaspersky Embedded Systems Security utilise la somme de contrôle du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

   Si la case n'est pas cochée, Kaspersky Embedded Systems Security utilise le certificat numérique du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

7. Cliquez sur le bouton **Créer des règles**.

8. Cliquez sur le bouton **Enregistrer** dans la fenêtre **Règles du contrôle du lancement des applications**.

   La liste des règles dans la stratégie Contrôle du lancement des applications est enrichie de nouvelles règles formées sur la base des données du système de l'appareil protégé sur lequel la Console d'administration Kaspersky Security Center est installée.

   Si la liste des règles du Contrôle du lancement des applications est déjà définie dans la stratégie, Kaspersky Embedded Systems Security ajoute les règles choisies parmi les événements du verrouillage aux règles déjà définies. Les règles possédant le même hash ne sont pas ajoutées car toutes les règles d'une liste doivent être uniques.

Importation des règles depuis un rapport de Kaspersky Security Center sur les applications bloquées

Vous pouvez importer les données relatives aux lancements d'application bloqués depuis un rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche Contrôle du lancement des applications en mode **Statistiques seulement** et utiliser ces données pour générer une liste de règles d'autorisation du Contrôle du lancement d'applications dans la stratégie configurée.

Lors de la création d'un rapport sur les événements survenus pendant l'exécution de la tâche de Contrôle du lancement des applications, vous pouvez surveiller le lancement des applications qu'il faudra bloquer.

Lors de l'importation depuis un rapport des données sur les applications bloquées dans les paramètres de la stratégie, confirmez que la liste à utiliser contient uniquement les applications dont vous souhaitez autoriser le lancement.

Pour définir les règles d'autorisation du Contrôle du lancement des applications pour un groupe d'appareils protégés sur la base du rapport des applications bloquées de Kaspersky Security Center :

1. Ouvrez la fenêtre **Contrôle du lancement des applications**.
2. Dans la section **Mode de tâche**, sélectionnez le mode **Statistiques seulement**.
3. Dans la section **Notifications sur les événements** des propriétés de la stratégie, assurez-vous que :
   - S'agissant des **Événements critiques**, la durée de conservation du journal d'exécution de la tâche pour les événements **Lancement de l'application interdit** est supérieure à la période prévue d'exécution de la tâche en mode **Statistiques seulement** (30 jours est la valeur par défaut).
   - S'agissant des événements qui possèdent le niveau d'importance **Avertissement**, la durée de conservation du journal d'exécution de la tâche pour les événements **mode Statistiques seulement : lancement de l'application interdit** est supérieure à la période prévue d'exécution de la tâche en mode **Statistiques seulement** (30 jours est la valeur par défaut).

     A l'issue de la période de conservation des événements, les informations relatives aux événements enregistrés sont supprimées et ne figurent pas dans le fichier du rapport. Avant de lancer la tâche Contrôle du lancement des applications en mode **Statistiques seulement**, assurez-vous que la durée d'exécution de la tâche n'est pas supérieure à la période configurée pour les événements indiqués.
4. Une fois la tâche terminée, exportez les événements enregistrés dans un fichier .TXT :
   a. Dans l'espace de travail du nœud **Serveur d'administration** de Kaspersky Security Center, sélectionnez l'onglet **Événements**.
   b. Cliquez sur le bouton **Créer une sélection** pour créer une sélection d'événements sur la base de la caractéristique Bloqués afin de voir les applications dont le lancement sera bloqué par la tâche de Contrôle du lancement des applications.
   c. Dans le volet résultats de la sélection, cliquez sur **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites dans un fichier au format TXT.

   Avant d'importer et d'appliquer un rapport créé dans une stratégie, assurez-vous qu'il contient uniquement les données relatives aux applications dont vous souhaitez autoriser le lancement.
5. Importez les données relatives aux lancements d'application bloqués dans la tâche de Contrôle du lancement des applications. Pour ce faire, réalisez les opérations suivantes dans les propriétés de la stratégie, dans les paramètres de la tâche Contrôle du lancement des applications :

a. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.

La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, sélectionnez l'option **Importer les données relatives aux applications bloquées depuis le rapport de Kaspersky Security Center**.

c. Sélectionnez le principe d'ajout des règles depuis la liste créée sur la base d'un rapport de Kaspersky Security Center à la liste des règles du Contrôle du lancement des applications existantes :

- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

d. Dans la fenêtre Microsoft Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les lancements d'application bloqués ont été exportés.

e. Cliquez sur **Enregistrer** dans la fenêtre **Règles du contrôle du lancement des applications**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les applications bloquées seront ajoutées à la liste des règles du Contrôle du lancement des applications.

Importation des règles du Contrôle du lancement des applications depuis un fichier XML

Vous pouvez importer les rapports créés par la tâche de groupe Génération des règles du Contrôle du lancement des applications et les appliquer en guise de liste de règles d'autorisation dans la stratégie configurée.

A la fin de la tâche de groupe de Génération des règles du Contrôle du lancement des applications, l'application exporte les règles d'autorisation créées dans un fichier au format XML enregistré dans le dossier partagé indiqué. Chaque fichier contenant une liste de règles est créé en analysant les fichiers exécutés et les applications lancées sur chaque appareil protégé distinct du réseau de l'organisation. Les listes contiennent les règles d'autorisation du lancement pour les fichiers et les applications dont le type correspond au type repris dans les paramètres de la tâche de groupe Génération des règles du Contrôle du lancement des applications.

Pour définir les règle d'autorisation du Contrôle du lancement des applications pour un groupe d'appareils protégés sur la base d'une liste de règles d'autorisation créée automatiquement, procédez comme suit :

1. Sous l'onglet **Tâches** dans le panneau de détails du groupe de périphériques protégés configuré, créez une tâche de groupe Génération des règles du Contrôle du lancement des applications ou choisissez une tâche existante.

2. Dans les propriétés de la tâche de groupe de Génération des règles du Contrôle du lancement des applications créée ou dans l'Assistant de création de tâche, configurez les paramètres suivants :

- Dans la section **Notifications**, configurez les paramètres de conservation du rapport sur l'exécution de la tâche.

Les détails sur la configuration des paramètres de cette section sont repris dans l'*aide de Kaspersky Security Center*.

- Dans la section **Configuration**, indiquez les types d'applications dont le lancement sera autorisé par les règles créées. Vous pouvez également modifier la sélection de dossiers contenant les applications qui pourront être lancées : exclure les dossiers indiqués par défaut de la zone d'application de la tâche et ajouter manuellement de nouveaux dossiers.
- Dans la section **Options**, indiquez les actions de la tâche pendant son exécution et à son issue. Définissez le critère de génération de règle et le nom du fichier dans lequel les règles créées vont être exportées.
- Dans la section **Planification**, configurez les paramètres de planification du lancement de la tâche.
- Dans la section **Compte**, désignez le compte utilisateur sous les privilèges duquel la tâche sera exécutée.
- Dans la section **Exclusions de la zone de la tâche**, définissez les groupes d'appareils protégés qu'il faut exclure de la zone d'action de la tâche.

Kaspersky Embedded Systems Security ne crée pas de règles d'autorisation pour les applications lancées sur les périphériques protégés exclus.

3. Sous l'onglet **Tâches** du panneau de détails du groupe de périphériques protégés configurés, sélectionnez la Génération des règles du Contrôle du lancement des applications créée dans la liste des tâches de groupe et cliquez sur le bouton **Démarrer** pour lancer la tâche.

   Quand la tâche est finie, les listes de règles d'autorisation générées automatiquement sont enregistrées dans un fichier XML au sein d'un dossier partagé.

Avant d'appliquer la stratégie de Contrôle du lancement des applications, assurez-vous que l'accès au dossier partagé a été configuré pour tous les appareils protégés. Au cas où l'utilisation d'un dossier partagé n'est pas prévue par la stratégie de l'organisation, nous vous conseillons de lancer la tâche Génération des règles du Contrôle du lancement des applications sur un appareil protégé appartenant à un groupe d'appareils protégés d'essai ou sur une machine modèle.

4. Pour ajouter les listes de règles d'autorisation créées à la tâche de Contrôle du lancement des applications, procédez comme suit :

   a. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

   b. Cliquez sur le bouton **Ajouter** et dans la liste qui s'ouvre, choisissez l'option **Importer les règles depuis un fichier au format XML**.

   c. Sélectionnez le principe d'ajout des règles d'autorisation générées automatiquement à la liste des règles du Contrôle du lancement des applications déjà créées :

      - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
      - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
      - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la

règle est ajoutée si au moins un des paramètres a une valeur différente.

d. Dans la fenêtre Microsoft Windows standard qui s'ouvre, choisissez les fichiers au format XML créés à l'issue de la tâche de groupe Génération des règles du Contrôle du lancement des applications.

e. Cliquez sur **Enregistrer** dans la fenêtre **Règles du contrôle du lancement des applications**.

5. Si vous souhaitez appliquer les règles créées pour contrôler le lancement des application, sélectionnez le mode **Actif** pour la tâche dans les propriétés de la tâche Contrôle du lancement des applications dans la stratégie.

Les règles d'autorisation générées automatiquement sur la base des lancements de tâches sur chaque appareil protégé distinct seront appliquées à tous les appareils protégés du réseau soumis à la stratégie configurée. Pour ces appareils protégés, l'application autorise le lancement uniquement des applications pour lesquelles des règles d'autorisation ont été créées.

Vérification du lancement des applications

Avant d'appliquer les règles configurées du Contrôle du lancement des applications, vous pouvez tester n'importe quelle application afin d'identifier les règles du Contrôle du lancement des applications déclenchées par cette application.

Kaspersky Embedded Systems Security bloque par défaut le lancement des applications si celui-ci n'est autorisé par aucune règle. Pour éviter l'interdiction du lancement d'applications importantes, il faut créer des règles d'autorisation pour celles-ci.

Si le lancement de l'application est régi par plusieurs règles de différents types, les règles d'interdiction sont prioritaires : le lancement de l'application est interdit si celle-ci tombe sous le coup d'une seule règle d'interdiction.

Pour tester les règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Afficher les règles pour le fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.

3. Sélectionnez le fichier pour lequel vous souhaitez tester la règle de contrôle.

Le chemin d'accès au fichier indiqué apparaît dans la ligne de recherche. La liste contient toutes les règles qui vont être déclenchées au lancement du fichier sélectionné.

Création d'une tâche Génération des règles du Contrôle du lancement des applications

Pour créer une tâche Génération des règles du contrôle du lancement des applications et configurer ses paramètres, procédez comme suit :

1. Ouvrez la fenêtre **Configuration** dans l'Assistant Nouvelle tâche.

2. Configurez les éléments suivants :

   - Indiquez le Préfixe pour les noms des règles.
   - Configurez la zone d'application des règles d'autorisation.

3. Cliquez sur **Suivant**.
4. Définissez les actions que Kaspersky Embedded Systems Security doit réaliser :
   - Lors de la génération des règles d'autorisation.
   - Une fois la tâche terminée.
5. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.
6. Cliquez sur **Suivant**.
7. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.
8. Cliquez sur **Suivant**.
9. Définissez un nom de tâche.
10. Cliquez sur **Suivant**.

    Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants : " * < > & \ : |

    La fenêtre **Terminer la création de la tâche** s'ouvre.
11. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.
12. Cliquez sur **Terminer** pour terminer la création de la tâche.

Pour configurer une règle existante dans Kaspersky Security Center, procédez comme suit :

Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications** et ajustez les paramètres décrits ci-dessus.

Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Restriction de la zone d'application de la tâche

Pour limiter la zone d'application de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications**.
2. Sélectionnez comment créer des règles d'autorisation :
   - **Créer des règles d'autorisation sur la base des applications en cours d'exécution**
   - **Créer des règles d'autorisation pour les applications des dossiers**

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Actions à réaliser lors de la génération automatique de règles

Pour configurer les actions que Kaspersky Embedded Systems Security doit réaliser pendant l'exécution de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications**.
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Lors de la génération des règles d'autorisation** :
   - **Utiliser un certificat numérique**
   - **Utiliser l'objet et l'empreinte du certificat numérique**
   - **En cas d'absence de certificat, utiliser**
     - **Hash SHA256**. La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
     - **chemin du fichier**. Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.
   - **Utiliser le hash SHA256**
   - **Créer des règles pour un utilisateur ou un groupe d'utilisateurs**
4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Actions à réaliser à la fin de la génération automatique de règles

Pour configurer les actions que Kaspersky Embedded Systems Security doit réaliser à la fin de la Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Génération des règles du Contrôle du lancement des applications**.
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Une fois la tâche terminée** :
   - **Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications**.
   - **Principe d'ajout**.

- **Exporter les règles d'autorisation vers un fichier**.
- Ajouter des informations sur l'appareil protégé au nom du fichier.

4. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Administration du Contrôle du lancement des applications via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un appareil protégé.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la tâche Contrôle du lancement des applications

Pour accéder aux paramètres généraux de la tâche Contrôle du lancement des applications via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Contrôle du lancement des applications**.
3. Dans le panneau de détails du nœud enfant **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

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

Ouverture de la fenêtre des règle du Contrôle du lancement des applications

Pour accéder à la liste des règles du Contrôle du lancement des applications via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Contrôle du lancement des applications**.
3. Dans le volet résultats du nœud **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

   La fenêtre **Règles du contrôle du lancement des applications** s'ouvre.

4. Configurez la liste des règles en fonction des besoins.

Accès aux paramètres de la tâche Génération des règles du Contrôle du lancement des applications

Pour configurer la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Sélectionnez le nœud enfant **Génération des règles du Contrôle du lancement des applications**.
3. Dans le volet résultats du nœud enfant **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez la tâche en fonction des besoins.

Configuration des paramètres de la tâche Contrôle du lancement des applications

Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Configurez les paramètres de la tâche suivants :
   - Sous l'onglet **Général** :
     - Mode de la tâche du Contrôle du lancement des applications.
     - Zone d'application de la règle dans la tâche.
     - Utilisation du KSN.
   - Paramètres du Contrôle de la distribution des logiciels sous l'onglet **Contrôle de la distribution des logiciels**.
   - Paramètres de planification du lancement de la tâche sous les onglets **Planification** et **Avancé**.
3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Sélection du mode de la tâche Contrôle du lancement des applications

Pour configurer le mode de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Désignez le mode de la tâche dans la liste déroulante **Mode de tâche** sous l'onglet **Général**.
3. Décochez ou cochez la case Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs.

   Kaspersky Embedded Systems Security dresse une nouvelle liste d'événements dans le cache à chaque modification des paramètres de la tâche Contrôle du lancement des applications. Cela signifie que le Contrôle du lancement des applications est organisé selon les paramètres de sécurité en cours.

4. Cochez ou décochez la case **Interdire le lancement de l'interpréteur de commande sans commande à exécuter**.
5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution de la tâche.

Configuration de la zone d'application de la tâche Contrôle du lancement des applications

Pour définir la zone d'application de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Définissez les paramètres suivants dans la section **Zone d'application de la règle** de l'onglet **Général** :
   - **Utiliser les règles pour les fichiers exécutables**
   - **Contrôle du chargement des modules DLL**

     Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation.

   - **Utiliser les règles pour les scripts et les paquets MSI**
3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Configuration de l'utilisation du KSN

Pour configurer l'utilisation des services KSN pour la tâche Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Sous l'onglet **Général**, dans la section **Utilisation du KSN**, définissez les paramètres relatifs à l'utilisation des services du KSN :
   - Le cas échéant, cochez la case **Interdire les applications douteuses selon le KSN**.
   - Le cas échéant, cochez la case **Autoriser les applications de confiance selon le KSN**.
   - Si la case **Autoriser les applications de confiance selon le KSN** est cochée, indiquez les utilisateurs et/ou les groupes d'utilisateurs qui peuvent lancer les applications considérées comme des applications de confiance dans KSN. Pour ce faire, procédez comme suit :
     a. Cliquez sur le bouton **Modifier**.
     La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

     > Par défaut, l'accès aux programmes approuvés dans KSN est autorisé à tous les utilisateurs.

     b. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.
     c. Cliquez sur le bouton **OK**.
3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Contrôle de la distribution des logiciels

Pour ajouter un paquet de distribution de confiance, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Sous l'onglet **Contrôle de la distribution des logiciels**, cochez la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste**.

   > Vous pouvez cocher la case **Autoriser automatiquement la diffusion du logiciel pour les applications et les paquets de la liste** si la case **Utiliser les règles pour les fichiers exécutables** sous l'onglet **Général** est cochée dans les paramètres de la tâche **Contrôle du lancement des applications**.

3. Le cas échéant, décochez la case **Toujours autoriser la diffusion de logiciel via Windows Installer**

Il est conseillé de décocher la case **Toujours autoriser la diffusion de logiciel via Windows Installer** uniquement dans les cas extrêmes. La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.

4. Le cas échéant, cochez la case Toujours autoriser la diffusion d'applications via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS).

   L'application contrôle le cycle de distribution de logiciels sur l'appareil protégé, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de l'application sur l'appareil protégé.

5. Pour créer une liste d'autorisation ou pour modifier la liste des paquets de distribution de confiance, cliquez sur le bouton **Modifier la liste de paquets** et sélectionnez une des méthodes suivantes dans la fenêtre qui s'ouvre :

   - **Ajouter un paquet de distribution**.

     a. Cliquez sur le bouton **Parcourir**.

     b. Sélectionnez le fichier exécutable ou le paquet de distribution.

     Les données du fichier sélectionné sont ajoutées automatiquement à la section **Critères de confiance**.

     c. Cochez ou décochez la case **Autoriser la distribution supplémentaire d'applications créées à partir de ce paquet de distribution**.

     d. Choisissez une de deux options proposées pour les critères de confiance qui vont déterminer si un fichier ou un paquet d'installation peut être considéré comme étant de confiance :

     - **Utiliser un certificat numérique**
     - **Utiliser le hash SHA256**

   - **Ajouter plusieurs paquets selon le hash**.

     Vous pouvez choisir un nombre illimité de fichiers de lancement et de paquets d'installation et les ajouter simultanément à la liste. Kaspersky Embedded Systems Security tient compte du hash et autorise le lancement le système d'exploitation à lancer les fichiers indiqués.

   - **Modifier le paquet sélectionné**.

     Cette option permet de sélectionner un autre fichier de lancement ou un autre paquet d'installation. Elle permet également la modification des critères de confiance.

   - Importer la liste des paquets de distribution depuis un fichier.

     Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des paquets de distribution de confiance.

6. Si vous voulez supprimer de la liste des éléments de confiance une application ou un paquet d'installation qui avait été ajouté antérieurement, cliquez sur le bouton **Supprimer les paquets d'installation**. Le lancement des fichiers extraits sera autorisé.

Pour interdire le lancement des fichiers extraits, désinstallez l'application de l'appareil protégé ou créez une règle d'interdiction dans les paramètres de la tâche Contrôle du lancement des applications.

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

Les nouvelles valeurs des paramètres seront enregistrés.

Configuration des règles du Contrôle du lancement des applications

Apprenez à créer, importer et exporter une liste de règles ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle du lancement des applications.

Ajout d'une règle du Contrôle du lancement des applications

Pour ajouter une règle du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.
   La fenêtre **Paramètres de règle** s'ouvre.
4. Spécifiez les paramètres suivants :
   a. Dans le champ **Nom**, saisissez le nom de la règle.
   b. Dans la liste déroulante **Type**, sélectionnez le type de règle :
      - **Autorisation**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
      - **Interdiction**, si vous souhaitez que la règle interdise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
   c. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :
      - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
      - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.
   d. Dans le champ **Utilisateur ou groupe d'utilisateurs**, indiquez les utilisateurs qui pourront ou non lancer des applications en fonction du type de règle. Pour ce faire, procédez comme suit :
      1. Cliquez sur le bouton **Parcourir**.
      2. La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.
      3. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

4. Cliquez sur le bouton **OK**.

e. Réalisez les opérations suivantes si vous souhaitez extraire les valeurs pour les critères de déclenchement de la règle listés dans la section **Critères de déclenchement de la règle**, depuis un fichier :

1. Cliquez sur le bouton **Définir les critères de déclenchement de la règle à partir des propriétés du fichier**.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

2. Sélectionnez le fichier.

3. Cliquez sur le bouton **Ouvrir**.

   Les valeurs des critères dans le fichier sont affichées dans les champs de le groupe **Critères de déclenchement de la règle**. Par défaut, c'est le premier critère de la liste dont les données figurent dans les propriétés du fichier qui est sélectionné.

f. Dans le groupe **Critères de déclenchement de la règle**, sélectionnez une ou plusieurs des options suivantes selon les cas :

- **Certificat numérique**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique :
  - Cochez la case **Utiliser l'objet**, si vous souhaitez que la règle contrôle le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'en-tête indiqué.
  - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle uniquement le lancement des fichiers disposant de la signature d'un certificat numérique uniquement s'ils ont l'empreinte indiquée.
- **Hash SHA256**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers dont la somme de contrôle correspond à celle indiquée.
- **Chemin du fichier**, si vous souhaitez que la règle contrôle le lancement des applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.
  - **Ligne de commande** si vous souhaitez que la règle contrôle les applications lancées à l'aide des arguments indiqués dans le champ de la ligne de commande. Le champ est activé une fois que vous avez sélectionné l'option **Chemin d'accès au fichier**. Vous pouvez utiliser ? et * comme masque lors de la définition des arguments de la ligne de commande pour les processus lancés en tant que critère.

> Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inversée "\" pour saisir correctement le chemin.

> Lors de la désignation des objets, vous pouvez utiliser ? et * en tant que masques de fichiers.

Vous devez sélectionner au moins une option. Dans le cas contraire, la règle du Contrôle du lancement des applications n'est pas ajoutée.

g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :

1. Dans la section **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion de la règle** s'ouvre.

2. Dans le champ **Nom**, saisissez le nom de l'exclusion.

3. Indiquez les paramètres d'exclusions des fichiers des applications de la règle du Contrôle du lancement des applications. Vous pouvez remplir les champs des paramètres depuis les propriétés du fichier en cliquant sur le bouton **Définir l'exclusion selon les propriétés du fichier**.

   - **Certificat numérique**
   - **Utiliser l'objet**
   - **Utiliser l'empreinte**
   - **Hash SHA256**
   - **Chemin du fichier**

4. Cliquez sur le bouton **OK**.

5. Si nécessaire, répétez les étapes (i) à (iv) pour ajouter des exclusions supplémentaires.

5. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

Activation du mode Autoriser par défaut

La règle Autoriser par défaut autorise le lancement de toutes les applications si celui-ci n'est pas interdit par des règles ou par une conclusion de KSN qui les considère comme douteuses. Il est possible d'activer le mode Autoriser par défaut en ajoutant des règles d'autorisation spécifiques. Vous pouvez activer Autoriser par défaut uniquement pour les scripts ou pour tous les fichiers exécutables.

Pour ajouter une nouvelle règle Autoriser par défaut :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Cliquez sur **Ajouter**.

3. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.
   La fenêtre **Paramètres de règle** s'ouvre.

4. Dans le champ **Nom**, saisissez le nom de la règle.

5. Dans la liste déroulante **Type**, sélectionnez le type de règle **Autorisation**.

6. Dans la liste déroulante **Zone d'application**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :

   - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
   - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.

7. Dans le groupe **Critères de déclenchement de la règle**, sélectionnez l'option **Chemin du fichier**.

8. Saisissez le masque suivant : `?:\`

9. Dans la fenêtre **Paramètres de règle**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security applique le mode Autoriser par défaut.

Création de règles d'autorisation au départ des événements de la tâche Contrôle du lancement des applications

Pour créer un fichier de configuration qui contient les règles d'autorisation créées au départ des événements de la tâche Contrôle du lancement des applications, procédez comme suit :

1. Lancez la tâche Contrôle du lancement des applications en mode **Statistiques seulement** pour consigner dans le journal d'exécution de la tâche les informations sur tous les lancements d'applications sur un périphérique protégé.

2. A la fin de l'exécution de la tâche en mode **Statistiques seulement**, ouvrez le journal d'exécution de la tâche via le bouton **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du panneau des résultats du nœud **Contrôle du lancement des applications**.

3. Dans la fenêtre **Journaux**, appuyez sur **Créer des règles selon les événements**.

Kaspersky Embedded Systems Security crée un fichier de configuration au format XML avec la liste des règles formées sur la base des événements de la tâche Contrôle du lancement des applications en mode **Statistiques seulement**. Vous pouvez utiliser cette liste de règles dans la tâche Contrôle du lancement des applications.

Avant d'appliquer la liste des règles générées au départ des événements de tâche enregistrés, nous vous conseillons de réviser et de traiter manuellement la liste afin de confirmer que le lancement de fichiers critiques (par exemple, des fichiers systèmes) est autorisé par les règles définies.

Tous les événements de la tâche sont enregistrés dans le journal d'exécution de la tâche, quel que soit le mode de la tâche. Vous pouvez créer un fichier de configuration contenant une liste de règles basée sur le journal créé pour la tâche exécutée en mode **Actif**. Ce scénario est déconseillé, sauf pour les cas urgents, car une liste de règle définitive doit être créée avant de pouvoir exécuter la tâche en mode **Actif** afin de renforcer son efficacité.

Exportation des règles du Contrôle du lancement des applications

Pour exporter les règles du Contrôle du lancement des applications dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.

2. Cliquez sur le bouton **Exporter vers un fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.

3. Dans la fenêtre qui s'ouvre, indiquez le fichier vers lequel vous souhaitez exporter les règles. Si ce fichier n'existe pas, il sera créé. Si un fichier portant ce nom existe déjà, son contenu sera écrasé après l'exportation des règles.

4. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la règle seront exportés dans le fichier indiqué.

Importation des règles du Contrôle du lancement des applications depuis un fichier XML

Pour importer les règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Importer les règles depuis un fichier au format XML**.
4. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez une des options du menu contextuel du bouton **Importer les règles depuis un fichier au format XML** :
   - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
   - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.
5. Dans la fenêtre **Ouvrir**, sélectionnez le fichier XML qui contient les règles du Contrôle du lancement des applications.
6. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du contrôle du lancement des applications**.

Suppression des règles du Contrôle du lancement des applications

Pour supprimer les règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Règles du contrôle du lancement des applications**.
2. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer la sélection**.
4. Cliquez sur le bouton **Enregistrer**.

Les règles du Contrôle du lancement des applications sélectionnées seront supprimées.

Configuration d'une tâche Génération des règles du Contrôle du lancement des applications

Pour configurer les paramètres de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Configurez les paramètres suivants :
   - Sous l'onglet **Général** :
     - Indiquez le **Préfixe pour les noms des règles**.
     - Configurez la zone d'application des règles d'autorisation.
   - Sous l'onglet **Actions**, définissez les actions que Kaspersky Embedded Systems Security doit réaliser.
   - Sous les onglets **Planification** et **Avancé**, configurez les paramètres de la planification du lancement de la tâche.
   - L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte.
3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Informations sur la date et l'heure de modification des paramètres, et valeurs des paramètres de la tâche avant et après leur modification.

Restriction de la zone d'application de la tâche

Pour limiter la zone d'application de la tâche Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche** de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Sélectionnez comment créer des règles d'autorisation :
   - **Créer des règles d'autorisation sur la base des applications en cours d'exécution**.
   - **Créer des règles d'autorisation pour les applications des dossiers**.
3. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Actions à réaliser lors de la génération automatique de règles

Pour configurer les actions de Kaspersky Embedded Systems Security pendant l'exécution et à la fin de la tâche Génération des règles du Contrôle du lancement des applications :

1. Ouvrez la fenêtre Paramètres de la tâche de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Lors de la génération des règles d'autorisation** :
   - Utiliser un certificat numérique
   - Utiliser l'objet et l'empreinte du certificat numérique
   - En cas d'absence de certificat, utiliser
     - **Hash SHA256**. La somme de contrôle du fichier utilisé pour créer la règle est indiquée en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la somme de contrôle indiquée.
     - **chemin du fichier**. Le chemin d'accès au fichier utiliser pour créer la règle est indiqué en tant que critère de la règle d'autorisation pour le contrôle du lancement des applications. Par la suite, l'application autorisera le lancement des applications via les fichiers qui se trouvent dans les dossiers indiqués dans le tableau **Créer des règles d'autorisation pour les applications des dossiers** de la section **Configuration**.
   - Utiliser le hash SHA256
   - Créer des règles pour un utilisateur ou un groupe d'utilisateurs.
4. Configurez les paramètres suivants dans la section **Une fois la tâche terminée** :
   - Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications.
   - Principe d'ajout.
   - **Exporter les règles d'autorisation vers un fichier**.
   - Ajouter des informations sur l'appareil protégé au nom du fichier.
5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Actions à réaliser à la fin de la génération automatique de règles

Pour configurer les actions que Kaspersky Embedded Systems Security doit réaliser à la fin de la Génération des règles du Contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre Paramètres de la tâche de la tâche **Génération des règles du Contrôle du lancement des applications**.
2. Ouvrez l'onglet **Options**.
3. Configurez les paramètres suivants dans la section **Une fois la tâche terminée** :
   - Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications.

- Principe d'ajout.
- **Exporter les règles d'autorisation vers un fichier**.
- Ajouter des informations sur l'appareil protégé au nom du fichier.

4. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés.

Administration du Contrôle du lancement des applications via le Plug-in Web

Pour configurer les tâches Contrôle du lancement des applications via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôle de l'activité locale**.
5. Cliquez sur **Configuration** dans la sous-section **Contrôle du lancement des applications**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la tâche Contrôle du lancement des applications

Paramètre	Description
Mode de tâche	La liste déroulante permet de sélectionner un des modes de la tâche Contrôle du lancement des applications : • **Actif**. Kaspersky Embedded Systems Security utilise les règles définies pour contrôler le lancement de n'importe quelle application. • **Statistiques seulement**. Kaspersky Embedded Systems Security n'utilise pas les règles définies pour contrôler les lancements d'application. Il se contente d'enregistrer les informations relatives aux événements de lancement dans le journal d'exécution de la tâche. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles du Contrôle du lancement des applications sur la base des informations relatives aux lancements d'applications interdits qui ont été consignées dans le journal d'exécution de la tâche. Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques seulement**.
Appliquer l'action adoptée au premier lancement du fichier à tous ses lancements ultérieurs	La case active ou désactive le contrôle d'un nouveau lancement de l'application en fonction des informations d'incidents stockées dans le cache. Quand la case est cochée, Kaspersky Embedded Systems Security autorise ou interdit les lancements suivants d'une application sur la base de la conclusion de la tâche suite au premier lancement de l'application. Par exemple, si le premier lancement de l'application avait été autorisé par les règles, l'enregistrement relatif à cet événement est enregistré dans le cache et les lancements ultérieurs de cette application sont également autorisés, sans vérification additionnelle.

	Si la case est désactivée, Kaspersky Embedded Systems Security analyse l'application à chacune des tentatives de lancement. Cette case est décochée par défaut.
Interdire le lancement de l'interpréteur de commande sans commande à exécuter	Si la case est cochée, Kaspersky Embedded Systems Security refuse le lancer les interpréteurs de ligne de commande même si ce lancement est autorisé. Il est possible de lancer un interpréteur de ligne de commande sans commande uniquement si les deux conditions suivantes sont remplies : • Le lancement de l'interpréteur de ligne de commande est autorisé. • La commande à exécuter est autorisée. Si la case est décochée, Kaspersky Embedded Systems Security tient uniquement compte des règles d'autorisation pour lancer un interpréteur de ligne de commande. Le lancement est interdit si aucune règle d'autorisation n'est appliquée ou si le processus exécutable n'est pas considéré comme processus de confiance par KSN. Si une règle d'autorisation s'applique ou si KSN considère qu'il s'agit d'un processus de confiance, il est possible de lancer un interpréteur de ligne de commande avec ou sans commande à exécuter. Kaspersky Embedded Systems Security reconnaît les interpréteurs de ligne de commande suivants : • cmd.exe • powershell.exe • python.exe • perl.exe Cette case est décochée par défaut.
Utiliser les règles pour les fichiers exécutables	La case active ou désactive le contrôle de lancement des fichiers exécutables. Si la case est cochée, Kaspersky Embedded Systems Security autorise ou interdit le lancement des fichiers exécutables à l'aide des règles indiquées dont les paramètres désignent les **Fichiers exécutables** comme zone d'action. Si la case est décochée, Kaspersky Embedded Systems Security ne contrôle pas le lancement des fichiers exécutables à l'aide des règles indiquées. Le lancement des fichiers exécutables est autorisé. Cette case est cochée par défaut.
Contrôle du chargement des modules DLL	La case active ou désactive le contrôle du chargement des modules DLL. Si la case est cochée, Kaspersky Embedded Systems Security autorise ou interdit le chargement des modules DLL à l'aide des règles indiquées dont les paramètres incluent les **Fichiers exécutables** dans la zone d'action. Si la case est décochée, Kaspersky Embedded Systems Security ne contrôle pas le chargement des modules DLL à l'aide des règles indiquées. Le chargement des modules DLL est autorisé. La case est active si la case **Utiliser les règles pour les fichiers exécutables** est cochée. Cette case est cochée par défaut.
Utiliser les règles pour les scripts et les paquets MSI	La case active ou désactive le lancement des scripts et des paquets MSI.

	Si la case est cochée, Kaspersky Embedded Systems Security autorise ou interdit le lancement des scripts et paquets MSI à l'aide des règles indiquées dont les paramètres incluent les scripts et les paquets MSI dans la zone. Si la case est décochée, Kaspersky Embedded Systems Security ne contrôle pas le lancement des scripts et des paquets MSI à l'aide des règles indiquées. Le lancement des scripts et des paquets MSI est autorisé. Cette case est cochée par défaut.
Interdire les applications douteuses selon le KSN	La case active ou désactive le Contrôle du lancement des applications selon les données relatives à leur réputation dans KSN. Si la case est cochée, Kaspersky Embedded Systems Security interdit le lancement de toute application que KSN considère comme douteuse. Les règle d'autorisation du Contrôle du lancement des applications applicables aux applications considérées comme douteuses par KSN ne sont pas déclenchées. Cocher cette case permet d'assurer une protection complémentaire contre les applications malveillantes. Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte la réputation des applications douteuses selon KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications. Cette case est décochée par défaut.
Autoriser les applications de confiance selon le KSN	La case active ou désactive le Contrôle du lancement des applications selon les données relatives à leur réputation dans KSN. Si la case est cochée, Kaspersky Embedded Systems Security autorise le lancement des applications considérées comme de confiance dans le KSN. Les règles d'interdiction du Contrôle du lancement des applications qui s'appliquent aux applications de confiance dans KSN ont une priorité supérieure : si l'application est considérée comme une application de confiance par les services KSN, son lancement est interdit. Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte la réputation des applications de confiance dans KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications. Cette case est décochée par défaut.
Utilisateurs et/ou groupes d'utilisateurs autorisés à lancer les applications de confiance d'après KSN	Si la case **Autoriser les applications de confiance selon le KSN** est cochée, vous pouvez renseigner ici les utilisateurs et les groupes d'utilisateurs autorisés à lancer les applications de confiance selon le KSN. Les utilisateurs suivants sont indiqués par défaut : **Tout le monde** et **AUTORITÉ NT\SYSTÈME**.
Règles	Configurer les règles d'autorisation ou d'interdiction pour la tâche Contrôle du lancement des applications.
Contrôle de la distribution des logiciels	Vous pouvez ajouter des paquets de distribution de confiance.
Administration des tâches	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Contrôle des périphériques

Cette section contient des informations sur la tâche Contrôle des périphériques et les instructions sur la configuration de cette tâche.

A propos de la tâche Contrôle des périphériques

Kaspersky Embedded Systems Security contrôle l'enregistrement et l'utilisation des périphériques externes et des lecteurs CD/DVD-ROM afin de protéger le périphérique contre les menaces sur la sécurité de l'information qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou d'autres types de périphérique externe connecté par USB.

Kaspersky Embedded Systems Security contrôle les connexions USB des périphériques externes suivants :

- Disques flash USB
- Lecteurs de CD
- Lecteurs de disquettes USB
- Adaptateurs réseau connectés via USB
- Périphériques mobiles MTP.USB

Kaspersky Embedded Systems Security vous informe des périphériques connectés via USB avec l'événement correspondant dans les journaux d'exécution de la tâche et des événements. Les détails des événements incluent le type de périphérique et le chemin de connexion. Lors la tâche Contrôle des périphériques est lancée, Kaspersky Embedded Systems Security analyse et énumère tous les périphériques connectés via USB. Vous pouvez configurer les notifications dans la section Configuration des notifications de Kaspersky Security Center.

La tâche Contrôle des périphériques surveille les tentatives de connexions USB de périphériques externes à l'appareil protégé et bloque la connexion s'il n'existe pas de règles d'autorisation pour ces appareils. En raison du blocage, il est impossible de consulter le contenu du périphérique ou d'exécuter des opérations sur les fichiers de ce périphérique (par exemple, lecture ou écriture des fichiers).

L'application attribue à chaque périphérique externe connecté un des états suivants :

- *De confiance*. Périphérique avec lequel l'échange de fichiers est autorisé. Lors de la génération d'une liste de règles, la valeur *Chemin d'accès à l'instance du périphérique* est incluse pour au moins une règle d'application.
- *Douteuse*. Périphérique avec lequel l'échange de données est interdit. Le chemin d'accès à l'instance du périphérique ne tombe pas sous le coup de la définition des règles d'autorisation.

Vous pouvez créer les règles d'autorisation pour les périphériques externes avec lesquels vous souhaitez autoriser l'échange de données à l'aide de la tâche Générateur de règles pour le Contrôle des périphériques. Vous pouvez aussi élargir la zone d'application des règles d'autorisation déjà créées. Vous pouvez également créer des règles d'autorisation manuellement.

Kaspersky Embedded Systems Security identifie les périphériques externes enregistrés dans le système sur la base de la valeur du chemin d'accès à l'instance du périphérique. Le chemin d'accès à l'instance du périphérique est un élément unique pour chaque périphérique externe. La valeur du chemin d'accès à l'instance du périphérique est définie pour chaque périphérique externe dans ses propriétés Windows et est définie automatiquement par Kaspersky Embedded Systems Security au moment de la création des règles.

La tâche Contrôle des périphériques peut être exécutée selon un des deux modes suivants :

- **Actif**. Kaspersky Embedded Systems Security contrôle, à l'aide de règles, la connexion de disques flash et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe Interdire par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.

  Si un périphérique externe que vous considérez douteux est connecté à un appareil protégé avant le lancement de la tâche Contrôle des périphériques en mode **Actif**, cet appareil n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement l'appareil douteux ou de redémarrer l'appareil protégé. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

- **Statistiques seulement**. Kaspersky Embedded Systems Security ne contrôle pas la connexion des disques flash et autres périphériques externes mais consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le périphérique protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

  Vous pouvez utiliser ce mode pour générer des règles sur la base des informations concernant le blocage des périphériques consignées pendant l'exécution de la tâche.

A propos des règles du Contrôle des périphériques

Kaspersky Embedded Systems Security n'applique pas les règles d'autorisation pour les périphériques mobiles MTP.

Les règles sont créées individuellement pour chaque périphérique connecté au moment donné ou connecté auparavant à l'appareil protégé, si les données relatives à cet appareil ont été mémorisées dans le registre système.

Pour créer des règles d'autorisation du contrôle des périphériques :

- Appliquer la tâche Générateur de règles pour le Contrôle des périphériques.
- Exécuter la tâche Contrôle des périphériques en mode Statistiques seulement.
- Utiliser les informations système relatives aux appareils connectés antérieurement.
- élargir le domaine d'application des règles existantes.

Le nombre maximum de règles du Contrôle des périphériques pris en charge par Kaspersky Embedded Systems Security est égal à 3 072.

Les règles du Contrôle des périphériques sont décrites ci-après.

Type de règle

Les règles sont toujours des règles *Autorisé*. La tâche Contrôle des périphériques bloque par défaut les connexions de tous les disques flash et autres périphériques externes s'ils ne sont couverts par aucune règle d'autorisation.

Critères de déclenchement et zone d'application des règles

Les règles du Contrôle des périphériques identifient les disques flash et autres périphériques externes connectés à l'aide du *Chemin d'accès à l'instance du périphérique*. Le chemin d'accès à l'instance du périphérique est un identifiant unique qui est attribué au périphérique par le système au moment de sa connexion et de l'enregistrement en tant que périphérique externe ou de lecteur de CD/DVD (par exemple, IDE ou SCSI).

> Kaspersky Embedded Systems Security contrôle la connexion des lecteurs de CD/DVD, quel que soit le bus de connexion. Lors du montage de ces périphériques par connexion USB, le système d'exploitation enregistre deux valeurs du chemin d'accès à l'instance du périphérique : pour le périphérique externe et pour le lecteur de CD/DVD (par exemple, IDE ou SCSI). La connexion adéquate de ces périphériques requiert l'existence de règles d'autorisation pour chaque valeur du chemin d'accès à l'instance du périphérique.

Kaspersky Embedded Systems Security détermine automatiquement le chemin d'accès à l'instance du périphérique et scinde la valeur selon les composants suivants :

- Fabricant (VID) ;
- Type de contrôleur (PID) ;
- Numéro de série du périphérique.

Il est impossible de définir manuellement le chemin d'accès à l'instance du périphérique. Les critères de déclenchement de la règle définis dans les propriétés de la règle d'autorisation déterminent la zone d'application des règles. Par défaut, la zone d'application d'une règle qui vient d'être créée contient un périphérique dont les propriétés ont été exploitées par Kaspersky Embedded Systems Security pour générer la règle. Vous pouvez configurer les valeurs dans les paramètres de la règle créée en utilisant un masque afin d'élargir la zone d'application de la règle.

Données du périphérique d'origine

Les propriétés du périphérique sur la base desquelles Kaspersky Embedded Systems Security a créé la règle d'autorisation et qui s'affichent dans le gestionnaire de périphérique Windows pour chaque périphérique connecté.

Les données du périphérique contiennent les informations suivantes :

- **Chemin d'accès à l'instance du périphérique**. Kaspersky Embedded Systems Security utilise cette propriété pour définir les critères de déclenchement de la règle et remplir les champs **Fabricant (VID)**, **Type de contrôleur (PID)**, **Numéro de série** dans la section **Zone d'application de la règle** de la fenêtre **Propriétés des règles**.
- **Nom convivial**. Nom attribué par le fabricant dans les propriétés du périphérique.

Kaspersky Embedded Systems Security identifie automatiquement les données du périphérique d'origine lors de la création de la règle. Vous pourrez utiliser par la suite ces valeurs pour déterminer sur la base des données de quel périphérique la règle a été créée. Les données du périphérique d'origine ne peuvent être modifiées.

Description

Vous pouvez ajouter des informations complémentaires pour chaque règle du Contrôle des périphériques créée dans le champ **Utilisateur ou groupe d'utilisateurs**, par exemple, le nom du disque flash connecté ou le nom de son propriétaire. La description s'affiche dans la colonne correspondante du tableau de la fenêtre **Règles du Contrôle des périphériques**.

Les commentaires et les données du périphérique d'origine ne sont pas pris en compte lors du fonctionnement de la règle et servent uniquement à simplifier l'identification des appareils et des règles par l'utilisateur.

A propos de la génération des règles du Contrôle des périphériques

Vous pouvez importer une liste de règles d'autorisation de contrôle des périphériques depuis des fichiers XML créés automatiquement lors de l'exécution de la tâche Contrôle des périphériques ou de la tâche Générateur de règles pour le Contrôle des périphériques.

Par défaut Kaspersky Embedded Systems Security interdit les connexions de n'importe quel disque flash et autre périphérique externe qui n'est pas soumis à l'action des règles du Contrôle des périphériques indiquées.

Cibles et scénarios de génération de règles de contrôle des périphériques

Scénarios de création de la liste des règles	Tâche à exécuter
Tâche Générateur de règles pour le Contrôle des périphériques	• Il faut créer des règles d'autorisation pour les périphériques de confiance déjà utilisés avant le premier lancement de la tâche Contrôle des périphériques. • Générez une liste des règles pour les périphériques de confiance dans le réseau d'appareils protégés.
Génération de règles sur la base des données du système	Ajoutez des règles d'autorisation pour un ou plusieurs périphériques externes dont les données ont été stockées dans le système.
Génération de règles basée sur les données des périphériques actuellement connectés	Mettez à jour la liste des règles s'il faut autoriser l'utilisation d'un nombre limité de nouveaux périphériques externes.
Tâche Contrôle des périphériques en mode **Statistiques seulement**	Générez des règles d'autorisation pour un nombre important de nouveaux périphériques de confiance.

Utilisation de la tâche Générateur de règles pour le Contrôle des périphériques

Le fichier XML formé à la fin de la tâche Générateur de règles pour le Contrôle des périphériques contient les règles d'autorisation pour les disques flash et autres périphériques externes dont les données de connexion sont mémorisées dans le système.

Utilisez ce scénario lors du processus de création de règles afin de tenir compte de tous les périphériques externes jamais connectés qui sont enregistrés par les systèmes sur tous les périphériques protégés réseau ou pour tenir compte uniquement des données relatives aux périphériques protégés connectés actuellement à tous les périphériques protégés réseau. La tâche tient également compte de tous les périphériques externes connectés au moment de l'exécution de la tâche de groupe. À la fin de l'exécution de la tâche de groupe, Kaspersky Embedded Systems Security compose les listes des règles d'autorisation pour tous les périphériques externe du réseau enregistrés et enregistre ces listes dans un fichier XML dans le dossier indiqué. Vous pouvez ensuite importer manuellement les listes de règles composées dans les propriétés de la stratégie Contrôle des périphériques. A la différence d'une tâche sur l'appareil protégé, la stratégie n'accepte pas la configuration de l'ajout automatique des règles créées dans la liste des règles de contrôle des périphériques à la fin de la tâche de groupe Générateur de règles pour le Contrôle des périphériques.

Il est conseillé d'utiliser ce scénario pour générer la liste des règles d'autorisation avant le premier lancement de la tâche Contrôle des périphériques afin que les règles d'autorisation créées tiennent compte de tous les périphériques externes de confiance utilisés sur un appareil protégé.

Utilisation des données système relatives à tous les périphériques connectés

Lors de l'exécution de la tâche, Kaspersky Embedded Systems Security obtient les données système sur tous les périphériques externes connectés à un moment donné ou actuellement au périphérique protégé et affiche les périphériques trouvés dans la liste de la fenêtre **Créer les règles sur la base des informations du système**.

Pour chaque périphérique trouvé, Kaspersky Embedded Systems Security définit le fabricant (VID), le type de contrôleur (PID), le nom convivial, le numéro de série et le chemin d'accès à l'instance du périphérique. Vous pouvez créer des règles d'autorisation pour n'importe quel périphérique externe dont les données ont été trouvées et ajouter directement les nouvelles règles à la liste des règles de contrôle des périphériques définies.

Dans le cadre ce scénario, Kaspersky Embedded Systems Security compose les règles d'autorisation pour les périphériques externes connectés auparavant ou connectés actuellement au périphérique protégé doté de Kaspersky Security Center.

Il est recommandé d'utiliser ce scénario pour mettre à jour la liste des règles s'il faut autoriser l'utilisation d'un nombre limité de nouveaux périphériques externes.

Utilisation des données sur les périphériques actuellement connectés

Dans le cadre de ce scénario, Kaspersky Embedded Systems Security crée des règles d'autorisation uniquement pour les périphériques externes connectés actuellement. Vous pouvez sélectionner un ou plusieurs périphériques externes pour lesquels vous souhaitez confirmer des règles d'autorisation.

Utilisation du rapport de la tâche Contrôle des périphériques en mode Statistiques seulement

Le fichier XML obtenu à la fin de la tâche Contrôle des périphériques en mode **Statistiques seulement** est créé sur la base du journal d'exécution de la tâche.

Au cours de l'exécution de la tâche, Kaspersky Embedded Systems Security consigne les informations relatives à toutes les connexions de disques flash et autres périphériques externes à un périphérique protégé. Vous pouvez créer des règles d'autorisation en fonction des événements de la tâche et les exporter dans un fichier XML. Avant le lancement de la tâche en mode **Statistiques seulement**, il est recommandé de configurer la période d'exécution de la tâche de telle sorte que toutes les connexions possibles de périphériques externes à l'appareil protégé puissent être réalisées dans le délai spécifié.

Ce scénario est recommandé pour actualiser une liste déjà générée de règles en cas de nécessité pour autoriser l'utilisation d'un grand nombre de nouveaux périphériques externes.

Si la composition de la liste des règles selon ce scénario se déroule sur une machine modèle, vous pouvez appliquer la liste créée des règles d'autorisation lors de la configuration de la stratégie du Contrôle des périphériques dans Kaspersky Security Center. Ainsi, vous pourrez autoriser l'utilisation des périphériques externes connectés à la machine modèle sur tous les périphériques protégés.

A propos de la tâche Générateur de règles pour le Contrôle des périphériques

La tâche Générateur de règles pour le Contrôle des périphériques permet de créer automatiquement une liste de règles d'autorisation pour les disques flash et autres périphériques externes connectés sur la base des données du système relatives aux périphériques externes qui avaient été connectés auparavant à un périphérique protégé.

À la fin de l'exécution de la tâche, Kaspersky Embedded Systems Security crée un fichier de configuration au format XML qui contient la liste des règles d'autorisation pour tous les périphériques externes détectés ou ajoute directement les règles formées à la tâche Contrôle des périphériques en fonction des paramètres de la tâche Générateur de règles pour le Contrôle des périphériques. L'application autorisera par la suite les périphériques pour lesquels des règles d'autorisation ont été générées automatiquement.

Les règles créées et ajoutées à la tâche figurent dans la fenêtre **Règles du Contrôle des périphériques**.

Paramètres par défaut de la tâche Contrôle des périphériques

La tâche Contrôle des périphériques possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres par défaut de la tâche Contrôle des périphériques

Paramètre	Valeur par défaut	Description
Mode de tâche	**Statistiques seulement**	La tâche consigne dans le journal d'exécution tous les événements d'interdiction et d'autorisation de connexion de périphériques externes conformément aux paramètres définis. Les périphériques externes ne sont pas vraiment bloqués. Vous pouvez choisir le mode **Actif** pour la protection d'un appareil afin d'appliquer l'interdiction de fait des appareils externes.
Autoriser l'utilisation de tous les périphériques externes quand la tâche Contrôle des périphériques n'est pas exécutée	Pas appliqué	Kaspersky Embedded Systems Security interdit l'utilisation des périphériques externes quel que soit l'état de l'exécution de la tâche Contrôle des périphériques. Cela garantit la protection maximale contre les menaces sur la sécurité informatique qui surgissent lors de l'échange de fichiers avec des périphériques externes. Vous pouvez configurer le paramètres de telle sorte que Kaspersky Embedded Systems Security autorise l'utilisation de tous les périphériques externes si la tâche Contrôle des périphériques n'est pas exécutée.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Contrôle des périphériques n'est pas lancée automatiquement au démarrage de Kaspersky Embedded Systems Security.

		Vous pouvez configurer la planification du lancement de la tâche.

Paramètres par défaut de la tâche Générateur de règles pour le Contrôle des périphériques

Paramètre	Valeur par défaut	Description
Mode de tâche	**Tenir compte des données du système sur tous les périphériques externes connectés à un moment donné**	Mode de fonctionnement de la tâche. Vous pouvez sélectionner le mode de la tâche **Tenir compte uniquement des périphériques externes connectés actuellement**.
Actions une fois la tâche terminée	Les règles d'autorisation sont ajoutées à la liste des règles de contrôle des périphériques ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont effectués.	Vous pouvez ajouter des règles à des règles existantes sans fusion et sans suppression des doublons, ou remplacer les règles existantes par de nouvelles règles d'autorisation, ainsi que configurer les paramètres d'exportation des règles d'autorisation dans un fichier.
Planification du lancement de la tâche	Le premier lancement n'est pas défini.	La tâche Générateur de règles pour le Contrôle des périphériques n'est pas lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer la tâche manuellement ou planifier son exécution.

Administration du Contrôle des périphériques via le plug-in d'administration

Cette section explique la navigation dans l'interface du plug-in d'administration et la gestion des connexions de n'importe quel périphérique externe à tous les périphériques protégés du réseau via la création de listes de règles à l'aide de Kaspersky Security Center pour les groupes de périphériques protégés.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la stratégie pour la tâche Contrôle des périphériques

Pour accéder aux paramètres de la tâche Contrôle des périphériques via une stratégie de Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.

6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle des périphériques**.
   La fenêtre **Contrôle des périphériques** s'ouvre.
7. Configurez la stratégie en fonction des besoins.

Accès à la liste des règles du Contrôle des périphériques

Pour accéder à la liste des règles du Contrôle des périphériques via Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Contrôle de l'activité locale**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Contrôle des périphériques**.
   La fenêtre **Contrôle des périphériques** s'ouvre.
7. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles**.
   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
8. Configurez la stratégie en fonction des besoins.

Accès à l'assistant de la tâche Générateur de règles pour le Contrôle des périphériques et aux propriétés

Pour lancer la tâche Générateur de règles pour le Contrôle des périphériques, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Cliquez sur le bouton **Créer une tâche**.
   La fenêtre **Assistant de nouvelle tâche** s'ouvre.
5. Sélectionnez la tâche **Générateur de règles pour le Contrôle des périphériques**.
6. Cliquez sur **Suivant**.
   La fenêtre **Configuration** s'ouvre.

Pour configurer la tâche Générateur de règles pour le Contrôle des périphériques existante, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Tâches**.
4. Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **Propriétés : Générateur de règles pour le Contrôle des périphériques** s'ouvre.

Consultez la section Configuration de la tâche Générateur de règles pour le Contrôle des périphériques pour en savoir plus sur la configuration de la tâche.

Configuration de la tâche Contrôle des périphériques

Pour configurer les paramètres de la tâche Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Contrôle des périphériques**.
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
   - Dans la section **Mode de tâche**, indiquez le mode de tâche :
     - **Actif**.

       Si un périphérique externe que vous considérez douteux est connecté à un appareil protégé avant le lancement de la tâche Contrôle des périphériques en mode Actif, cet appareil n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement l'appareil douteux ou de redémarrer l'appareil protégé. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

     - **Statistiques seulement**.
   - Décochez ou cochez la case **Autoriser l'utilisation de tous les périphériques externes quand la tâche Contrôle des périphériques n'est pas exécutée**.
3. Cliquez sur le bouton **Liste des règles** de la liste pour modifier la liste des règles du Contrôle des périphériques.
4. Le cas échéant, configurez les paramètres de la planification du lancement de la tâche sous l'onglet **Administration des tâches**.
5. Cliquez sur **OK** dans la fenêtre **Contrôle des périphériques**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Configuration de la tâche Générateur de règles pour le Contrôle des périphériques

Pour configurer la tâche Générateur de règles pour le Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Générateur de règles pour le Contrôle des périphériques**.

2. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres dans cette section dans le *Système d'aide de Kaspersky Security Center*.

3. La section **Configuration** permet de configurer les paramètres suivants :

   - Sélectionnez le mode de fonctionnement :tenir compte des données système relatives à tous les périphériques de stockage de masse jamais connectés ou tenir compte uniquement des périphériques externes connectés actuellement.

   - Configurez les paramètres pour les fichiers de configuration contenant les listes des règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.

4. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

5. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

6. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

7. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

   Les paramètres de la tâche de groupe définis seront enregistrés.

Configuration de la tâche Contrôle des périphériques via Kaspersky Security Center

Apprenez à créer une liste de règles sur la base de différents critères ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle des périphériques.

Création de règles d'autorisation sur la base des données du système dans une stratégie de Kaspersky Security Center

*Pour définir les règles d'autorisation à l'aide de l'option **Créer les règles sur la base des données du système**, dans les paramètres de la tâche Contrôle des périphériques, procédez comme suit :*

1. Le cas échéant, connectez au périphérique protégé doté de la Console d'administration de Kaspersky Security Center un nouveau périphérique externe dont vous souhaitez autoriser l'utilisation.

2. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

3. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.

4. Dans la liste de périphériques de la fenêtre **Créer les règles sur la base des informations du système**, sélectionnez un périphérique.

5. Cliquez sur **Ajouter des règles pour les périphériques sélectionnés**.

6. Cliquez sur **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

La liste des règles dans la tâche Contrôle des périphériques sera enrichie de nouvelles règles formées sur la base des données du système de l'appareil protégé sur lequel la Console d'administration de Kaspersky Security Center est installée.

Création de règles pour les périphériques connectés

*Pour définir les règles d'autorisation à l'aide de l'option **Créer des règles sur la base des périphériques connectés**, dans la tâche Contrôle des périphériques, procédez comme suit :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer des règles sur la base des périphériques connectés**.

   La fenêtre **Créer les règles sur la base des informations du système** s'ouvre.

3. Dans la liste des périphériques détectés qui sont connectés à l'appareil protégé, choisissez les périphériques pour lesquels vous voulez créer des règles d'autorisation.

4. Cliquez sur le bouton **Ajouter des règles pour les périphériques sélectionnés**.

5. Cliquez sur **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

La liste des règles dans la tâche Contrôle des périphériques sera enrichie de nouvelles règles formées sur la base des données du système de l'appareil protégé sur lequel la Console d'administration de Kaspersky Security Center est installée.

Génération de règles basées sur le registre de Kaspersky Security Center

*Pour définir les règles d'autorisation à l'aide de l'option **Créer des règles sur la base des périphériques connectés** dans les paramètres de la tâche Contrôle des périphériques :*

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

2. Cliquez sur le bouton **Ajouter** et dans le menu contextuel du bouton, choisissez l'option **Créer des règles sur la base des périphériques connectés**.

   La fenêtre **Créer les règles sur la base des informations du système** s'ouvre.

3. Cliquez sur **Actualiser la liste** pour obtenir la liste des périphériques disponibles et sélectionnez les périphériques pour lesquels vous souhaitez générer des règles d'autorisation. Vous pouvez également renseigner le **Nom convivial** dans le champ **Rechercher** afin de filtrer les périphériques et accélérer la sélection.

4. Cliquez sur le bouton **Ajouter des règles pour les périphériques sélectionnés**.

5. Cliquez sur **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

La liste des règles de la tâche Contrôle des périphériques sera remplie par les nouvelles règles générées sur la base du registre de Kaspersky Security Center.

Affichage des propriétés des règles du Contrôle des périphériques

Pour consulter les propriétés des règles du **Contrôle des périphériques** :

1. Ouvrez la fenêtre **Contrôle des périphériques**.
2. Sous l'onglet **Général**, cliquez sur le bouton **Liste des règles** et double-cliquez sur la règle sélectionnée.

   La fenêtre **Propriétés de la règle** s'ouvre.

Propriétés des règles du Contrôle des périphériques

Propriétés	Description
Appliquer la règle	Choisissez cette option pour activer ou désactiver l'application de la règle.
Fabricant (VID)	Vous pouvez renseigner le VID complet du fabricant de l'appareil ou utiliser * comme masque. * signifie n'importe quel fabricant. Si la case Utiliser un masque est cochée pour le champ Fabricant (VID), les données du champ dont la case est cochée sont remplacées par * et ne sont pas prises en compte lors du déclenchement de la règle.
Type de contrôleur (PID)	Vous pouvez indiquer le PID complet du contrôleur ou utiliser * comme masque. * signifie n'importe quel type de contrôleur. Si la case Utiliser un masque est cochée pour le champ Type de contrôleur (PID), les données du champ dont la case est cochée sont remplacées par * et ne sont pas prises en compte lors du déclenchement de la règle.
Numéro de série	Vous pouvez renseigner le numéro de série complet de l'appareil ou utiliser * et ? en guise de masque. * représente n'importe quelle séquence de caractères, y compris une séquence vide. ? représente un caractère dans une séquence. Si la case Utiliser un masque est cochée pour le champ Numéro de série, les données du champ dont la case est cochée sont remplacées par * et ne sont pas prises en compte lors du déclenchement de la règle. Si vous avez sélectionné l'option **Utiliser un masque**, mais que vous ne saisissez aucun caractère dans le champ **Numéro de série**, puis enregistrez les paramètres et fermez la fenêtre, l'application applique * comme masque pour la propriété **Numéro de série** et ne prend pas en compte le champ lorsque la règle est appliquée.
Chemin d'accès à l'instance du périphérique	Identifiant du périphérique connecté. Vous ne pouvez pas modifier la propriété. Le champ est proposé à titre informatif seulement. L'application n'applique pas le champ pour le contrôle des périphériques.
Nom convivial.	Nom de l'appareil défini par le fabricant. Vous ne pouvez pas modifier la propriété. Le champ est proposé à titre informatif seulement. L'application n'applique pas le champ pour le contrôle des périphériques.
Utilisateur ou groupe d'utilisateurs	Vous pouvez désigner un compte utilisateur ou un groupe d'utilisateurs qui ont accès aux périphériques USB sélectionnés.

	Le système d'exploitation affiche tous les périphériques USB connectés. Vous pouvez accéder uniquement aux clés USB pour lesquelles vous disposez des privilèges d'accès respectifs.
Description	La description du périphérique par défaut. Le cas échéant, ajoutez des informations dans le champ Description pour expliquer la règle. Par exemple, précisez les périphériques auxquels la règle doit s'appliquer.

Importation des règles depuis un rapport de Kaspersky Security Center sur les périphériques bloqués

Vous pouvez importer les données relatives aux connexions des périphériques bloqués depuis le rapport créé dans Kaspersky Security Center à l'issue de l'exécution de la tâche Contrôle des périphériques en mode **Statistiques seulement** utiliser ces données pour générer une liste de règles d'autorisation du lancement d'applications dans la stratégie configurée.

Lors de la création du rapport sur les événements survenus pendant l'exécution de la tâche de contrôle des périphériques, vous pouvez surveiller la connexion des périphériques qu'il faudra bloquer.

Pour spécifier des règles d'autorisation de connexion des périphériques pour un groupe d'appareils protégés sur la base d'un rapport de Kaspersky Security Center relatif aux appareils bloqués, procédez comme suit :

1. Dans la section **Notifications sur les événements** des propriétés de la stratégie, assurez-vous que :

   - S'agissant du niveau d'importance **Événements critiques**, la durée de conservation du journal d'exécution de la tâche pour l'événement *Périphérique externe douteux détecté et restreint* dépasse la période de fonctionnement prévue du mode **Statistiques seulement** (la valeur par défaut est de 30 jours).

   - S'agissant du niveau d'importance **Avertissement**, la durée de conservation du journal d'exécution de la tâche pour l'événement *Statistiques seulement : périphérique externe douteux détecté* dépasse la période de fonctionnement prévue du mode **Statistiques seulement** (la valeur par défaut est de 30 jours).

     A l'échéance de la période de conservation des événements, les informations relatives aux événements enregistrés seront supprimées et ne figureront pas dans le fichier du rapport. Avant de lancer la tâche Contrôle des périphériques en mode **Statistiques seulement**, assurez-vous que la durée d'exécution de la tâche n'est pas supérieure à la durée de conservation établie pour les événements indiqués.

2. Lancez la tâche Contrôle des périphériques en mode **Statistiques seulement**.

   a. Dans l'espace de travail du nœud **Serveur d'administration** de Kaspersky Security Center, sélectionnez l'onglet **Événements**.

   b. Cliquez sur le bouton **Créer une sélection** pour créer une sélection d'événements sur la base du critère *Périphérique externe douteux détecté et restreint* pour voir les périphériques dont les connexions vont être limitées par la tâche Contrôle des périphériques.

   c. Dans le volet résultats de la sélection, cliquez sur le lien **Exporter les événements dans un fichier** afin d'enregistrer le rapport sur les applications interdites dans un fichier au format TXT.

Avant d'importer et d'appliquer un rapport créé dans une stratégie, assurez-vous qu'il contient les données relatives uniquement aux périphériques dont vous souhaitez autoriser la connexion.

3. Importez les données sur les tentatives bloquées de connexion des périphériques dans la tâche du Contrôle des périphériques :

   a. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

   b. Cliquez sur le bouton **Ajouter** et dans le menu contextuel, sélectionnez l'option **Importer les données relatives aux périphériques bloqués depuis le rapport de Kaspersky Security Center**.

   c. Sélectionnez le principe d'ajout des règles depuis la liste créée sur la base du rapport de Kaspersky Security Center à la liste des règles du Contrôle des périphériques existantes :

      - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
      - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
      - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

   d. Dans la fenêtre Windows standard qui s'ouvre, choisissez le fichier au format TXT dans lequel les événements du rapport sur les périphériques bloqués ont été exportés.

   e. Cliquez sur **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

4. Cliquez sur **OK** dans la fenêtre **Contrôle des périphériques**.

Les règles créées sur la base du rapport de Kaspersky Security Center sur les périphériques bloqués seront ajoutées à la liste des règles de la stratégie de contrôle des périphériques.

Création de règles à l'aide de la tâche Générateur de règles pour le Contrôle des périphériques

Pour définir les règles d'autorisation du contrôle des périphériques pour un groupe d'appareils protégés à l'aide de la tâche Générateur de règles pour le Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Configuration** dans l'Assistant Nouvelle tâche.

2. Configurez les éléments suivants :

   - Dans la section **Mode** :
     - **Tenir compte des données du système sur tous les périphériques externes connectés à un moment donné**.
     - **Tenir compte uniquement des périphériques externes connectés actuellement**.
   - Dans la section **Une fois la tâche terminée** :
     - Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques.
     - Principe d'ajout.
     - Exporter les règles d'autorisation vers un fichier.

- Ajouter des informations sur l'appareil protégé au nom du fichier.

3. Cliquez sur **Suivant**.
4. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.
5. Cliquez sur **Suivant**.
6. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.
7. Cliquez sur **Suivant**.
8. Définissez un nom de tâche.
9. Cliquez sur **Suivant**.

   Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants : " * < > & \ : |

   La fenêtre **Terminer la création de la tâche** s'ouvre.
10. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.
11. Cliquez sur **Terminer** pour terminer la création de la tâche.
12. Sous l'onglet **Tâches** de l'espace de travail du groupe de périphériques protégés configurés, sélectionnez la tâche Générateur de règles pour le Contrôle des périphériques dans la liste des tâches de groupe.
13. Cliquez sur le bouton **Démarrer** pour démarrer la tâche.

    A l'issue de la tâche, les listes de règles d'autorisation générées automatiquement seront enregistrées dans le dossier partagé dans des fichiers XML.

    Avant d'appliquer la stratégie de Contrôle des périphériques, assurez-vous que l'accès au dossier réseau partagé a été configuré pour tous les appareils protégés. Au cas où l'utilisation d'un dossier réseau partagé n'est pas prévue par la stratégie de l'organisation, il est recommandé de lancer la tâche Générateur de règles pour le Contrôle des périphériques pour les règles de Contrôle de l'appareil protégé sur un groupe d'appareils protégés d'essai ou sur une machine modèle.

Ajout des règles créées à la liste des règles du Contrôle des périphériques

Pour ajouter les listes de règles d'autorisation créées à la tâche Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Importer les règles depuis un fichier au format XML**.

4. Sélectionnez le principe d'ajout des règles d'autorisation générées automatiquement à la liste des règles de contrôle des périphériques déjà créées :

   - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.

   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.

   - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

5. Dans la fenêtre Windows standard qui s'ouvre, choisissez les fichiers au format XML créés à l'issue de la tâche de groupe Générateur de règles pour le Contrôle des périphériques.

6. Cliquez sur **Ouvrir**.

   Toutes les règles générées depuis le fichier XML sont ajoutées à la liste conformément au principe sélectionné.

7. Cliquez sur **Enregistrer** dans la fenêtre **Règles du Contrôle des périphériques**.

8. Si vous voulez appliquer les règles créées pour le Contrôle des périphériques, sélectionnez le mode de tâche **Actif** dans les paramètres de la stratégie **Contrôle des périphériques**.

Les règles d'autorisation générées automatiquement sur la base des données du système sur chaque appareil protégé distinct sont appliquées à tous les appareils protégés du réseau soumis à la stratégie configurée. Pour ces appareils protégés, l'application autorise la connexion des périphériques pour lesquels des règles d'autorisation ont été créées.

Administration du Contrôle des périphériques via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un appareil protégé.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la tâche Contrôle des périphériques

Pour accéder aux paramètres de la tâche Contrôle des périphériques via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.

2. Sélectionnez le nœud enfant **Contrôle des périphériques**.

3. Dans le panneau de détails du nœud enfant **Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

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

4. Configurez la tâche en fonction des besoins.

Ouverture de la fenêtre des règles du Contrôle des périphériques

Pour ouvrir la liste des règles du Contrôle des périphériques via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Contrôle des périphériques**.
3. Dans le volet résultats du nœud **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
4. Configurez la liste des règles en fonction des besoins.

Accès aux paramètres de la tâche Générateur de règles pour le Contrôle des périphériques

Pour configurer la tâche Générateur de règles pour le Contrôle des périphériques, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Choisissez le nœud enfant **Générateur de règles pour le Contrôle des périphériques**.
3. Dans le volet résultats du nœud enfant **Générateur de règles pour le Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez la tâche en fonction des besoins.

Configuration des paramètres de la tâche Contrôle des périphériques

Pour configurer les paramètres de la tâche Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres de la tâche**.
2. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :
   - Dans la section **Mode de tâche**, indiquez le mode de tâche :
     - Actif.

Si un périphérique externe que vous considérez douteux est connecté à un appareil protégé avant le lancement de la tâche Contrôle des périphériques en mode Actif, cet appareil n'est pas bloqué par l'application. Nous conseillons de déconnecter manuellement l'appareil douteux ou de redémarrer l'appareil protégé. Dans le cas contraire, le principe Interdire par défaut ne sera pas appliqué à l'appareil.

- **Statistiques seulement**.

- Décochez ou cochez la case **Autoriser l'utilisation de tous les périphériques externes quand la tâche Contrôle des périphériques n'est pas exécutée**.

3. Les onglets **Planification** et **Avancé** permettent de configurer, le cas échéant, les paramètres de lancement planifié de la tâche.

4. Pour modifier la liste des règles du Contrôle des périphériques, cliquez sur le lien **Règles du Contrôle des périphériques** dans la partie inférieure du volet résultats du nœud **Contrôle des périphériques**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Configuration des règles du Contrôle des périphériques

Apprenez à créer, importer et exporter une liste de règles ou à créer manuellement des règles d'autorisation ou d'interdiction à l'aide de la tâche Contrôle des périphériques.

Importation des règles de contrôle des périphériques depuis un fichier XML

Pour importer des règles du Contrôle des périphériques :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

2. Cliquez sur **Ajouter**.

3. Dans le menu contextuel du bouton, choisissez l'option **Importer les règles depuis un fichier au format XML**.

4. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez une des options du menu contextuel du bouton **Importer les règles depuis un fichier au format XML** :

   - **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.

   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.

   - **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

5. Dans la fenêtre **Ouvrir**, sélectionnez le fichier XML qui contient les paramètres des règles du Contrôle des périphériques.

6. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du Contrôle des périphériques**.

Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques

Pour créer un fichier de configuration contenant la liste des règles du Contrôle des périphériques créées sur la base des événements de la tâche Contrôle des périphériques, procédez comme suit :

1. Lancez la tâche Contrôle des périphériques en mode **Statistiques seulement** afin d'enregistrer toutes les connexions de disques Flash ou d'autres périphériques externes au périphérique protégé.

2. A la fin de la tâche en mode **Statistiques seulement**, ouvrez le journal d'exécution de la tâche via le bouton **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du volet résultats du nœud **Contrôle des périphériques**.

3. Dans la fenêtre **Journaux**, cliquez sur le bouton **Créer des règles selon les événements**.

Kaspersky Embedded Systems Security crée un fichier de configuration au format XML qui contient une liste des règles composées selon les événements de la tâche Contrôle des périphériques en mode **Statistiques seulement**. Vous pouvez utiliser cette liste dans la tâche Contrôle des périphériques.

Avant d'appliquer la liste des règles formée selon les événements de la tâche, il est recommandé de l'examiner, et puis de traiter manuellement la liste des règles pour confirmer que les règles définies interdisent la connexion des périphériques douteux.

Lors de la conversion du fichier XML contenant les événements d'exécution de la tâche en liste de règles de contrôle des périphériques, l'application crée les règles d'autorisation pour tous les événements fixés, y compris pour les événements d'interdiction de périphériques.

Tous les événements de la tâche sont enregistrés dans le journal d'exécution de la tâche dans chacun des deux modes. Vous pouvez créer le fichier de configuration contenant une liste des règles sur la base des événements de la tâche en mode **Actif**. Ce scénario n'est pas recommandé, sauf en cas d'urgence, car l'exécution efficace de la tâche requiert la composition d'une liste de règles finale avant le lancement de la tâche en mode actif.

Ajout d'une règle d'autorisation pour un ou plusieurs périphériques externes

La tâche du contrôle des périphériques ne prévoit pas la fonction d'ajout d'une règle manuellement. Cependant, si vous devez ajouter des règles d'autorisation pour un ou plusieurs nouveaux périphériques externes, vous pouvez utiliser l'option **Créer les règles sur la base des données du système**. Lors de l'utilisation de ce scénario, l'application utilise les données de Windows relatives à tous les périphériques externes connectés et autorise les périphériques externes connectés en ce moment de remplir une liste des règles d'autorisation.

Pour ajouter une règle d'autorisation pour un ou plusieurs périphériques externes utilisés en ce moment, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.
2. Cliquez sur **Ajouter**.
3. Dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.
4. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste des périphériques détectés le ou les périphériques dont vous souhaitez autoriser l'utilisation sur un appareil protégé.
5. Cliquez sur le bouton **Ajouter des règles pour les périphériques sélectionnés**.

Les nouvelles règles seront ajoutées à la liste des règles de contrôle des périphériques.

Suppression des règles de Contrôle des périphériques

Pour supprimer des règles du Contrôle des périphériques :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.
2. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer la sélection**.
4. Cliquez sur le bouton **Enregistrer**.

Les règles de contrôle des périphériques sélectionnées seront supprimées.

Exportation des règles de Contrôle des périphériques

Pour exporter les règles du Contrôle des périphériques dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.
2. Cliquez sur le bouton **Exporter vers un fichier**.
   La fenêtre standard de Microsoft Windows s'ouvre.
3. Dans la fenêtre qui s'ouvre, indiquez le fichier vers lequel vous souhaitez exporter les règles. Si ce fichier n'existe pas, il sera créé. Si un fichier portant ce nom existe déjà, son contenu sera écrasé après l'exportation des règles.
4. Cliquez sur le bouton **Enregistrer**.

Les règles et leurs paramètres seront exportés dans le fichier indiqué.

Activation et désactivation des règles de Contrôle des périphériques

Vous pouvez activer et désactiver l'application des règles d'autorisation créées pour le contrôle des périphériques sans les supprimer.

Pour activer ou désactiver une règle du Contrôle des périphériques créée :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

2. Dans la liste des règles définies, ouvrez la fenêtre **Propriétés des règles** d'un double clic sur la règle dont vous souhaitez configurer les propriétés.

3. Dans la fenêtre qui s'ouvre, décochez ou cochez la case **Appliquer la règle**.

4. Cliquez sur le bouton **OK**.

L'état de l'application de la règle est enregistré et s'affiche pour la règle indiquée.

Extension de la zone d'application des règles de Contrôle des périphériques

Chaque règle du contrôle des périphériques créée automatiquement autorise la connexion d'un seul périphérique externe. Vous pouvez élargir manuellement la zone d'application des règles en introduisant un masque de chemin d'accès à l'instance du périphérique dans les paramètres de n'importe quelle règle de contrôle des périphériques créée.

L'application du masque du chemin d'accès à l'instance du périphérique diminue la quantité de règles d'autorisation du contrôle des périphériques et simplifie le processus de leur traitement manuel. Cependant, l'extension de la zone d'application des règles peut réduire l'efficacité du contrôle des périphériques externes.

Pour appliquer le masque de chemin d'accès à l'instance du périphérique dans les propriétés d'une règle du Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre **Règles du Contrôle des périphériques**.

2. Dans la fenêtre qui s'ouvre, choisissez une règle afin d'utiliser ses propriétés pour l'application d'un masque.

3. Ouvrez la fenêtre **Propriétés des règles** d'un double clic sur la règle du Contrôle des périphériques choisie.

4. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

   - Cochez la case **Utiliser un masque** en face du champ **Fabricant (VID)** si vous souhaitez que la règle sélectionnée autorise la connexion de tous les périphériques externes qui satisfont à l'information indiquée relative au fabricant du périphérique.

   - Cochez la case **Utiliser un masque** en regard du champ **Type de contrôleur (PID)** si voulez que la règle sélectionnée autorise la connexion de tous les périphériques externes qui satisfont à l'information indiquée relative au type de contrôleur.

   - Cochez la case **Utiliser un masque** en face du champ **Numéro de série** si vous souhaitez que la règle sélectionnée autorise la connexion de tous les périphériques externes qui satisfont à l'information indiquée relative au numéro de série du périphérique.

   Si la case **Utiliser un masque** est cochée dans un champ au moins, les données des champs dont la case est cochée sont remplacées par le caractère * et ne sont pas prises en compte lors du déclenchement de la règle.

5. Renseignez un compte utilisateur ou un groupe d'utilisateurs qui ont accès aux périphériques USB sélectionnés. Le système d'exploitation affiche tous les périphériques USB connectés. Vous pouvez accéder uniquement aux périphériques USB pour lesquels vous disposez des privilèges d'accès respectifs.

6. Le cas échéant, ajoutez des informations dans le champ **Utilisateur ou groupe d'utilisateurs** pour expliquer la règle. Par exemple, précisez les périphériques auxquels la règle doit s'appliquer.

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

Les paramètres de la règle définis seront enregistrés. La zone d'application des règles sera élargie conformément au masque indiqué du chemin d'accès à l'instance du périphérique.

Configuration de la tâche Générateur de règles pour le Contrôle des périphériques

Pour configurer la tâche Générateur de règles pour le Contrôle des périphériques, procédez comme suit :

1. Dans l'arborescence de la console de l'application, développez le nœud **Génération automatique de règles**.
2. Choisissez le nœud enfant **Générateur de règles pour le Contrôle des périphériques**.
3. Dans le volet résultats du nœud **Générateur de règles pour le Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général**, sélectionnez le mode de fonctionnement de la tâche dans la section **Mode de tâche** :
   - **Tenir compte des données du système sur tous les périphériques externes connectés à un moment donné**.
   - **Tenir compte uniquement des périphériques externes connectés actuellement**.
5. Dans la section **Une fois la tâche terminée**, indiquez les actions que Kaspersky Embedded Systems Security doit réaliser à la fin de la tâche :
   - Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques.
   - Principe d'ajout.
   - Exporter les règles d'autorisation vers un fichier.
   - Ajouter des informations sur l'appareil protégé au nom du fichier.
6. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche.
7. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres de la tâche avant et après leur modification, seront enregistrées dans le journal d'audit système.

Administration du Contrôle des périphériques via le Plug-in Web de la Console de l'application

Cette section présente la navigation dans l'interface du Plug-in Web et la configuration des paramètres d'une tâche sur un périphérique protégé.

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur **Configuration** dans la sous-section **Contrôle des périphériques**.

6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la tâche Contrôle des périphériques

Paramètre	Description
Actif	Kaspersky Embedded Systems Security contrôle, à l'aide de règles, la connexion de disques amovibles et autres périphériques externes et autorise ou interdit l'utilisation des périphériques sur la base du principe Interdire par défaut et des règles d'autorisation définies. L'utilisation des périphériques externes de confiance est autorisée. L'utilisation des périphériques externes douteux est interdite par défaut.
Statistiques seulement	Kaspersky Embedded Systems Security ne contrôle pas la connexion des disques amovibles et autres périphériques externes mais consigne seulement les informations relatives aux connexions ou aux enregistrements de périphériques externes sur le périphérique protégé ainsi que les informations relatives aux règles d'autorisation du Contrôle des périphériques déclenchées par les périphériques connectés. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.
Autoriser l'utilisation de tous les périphériques externes quand la tâche Contrôle des périphériques n'est pas exécutée	La case autorise ou interdit l'utilisation des périphériques externes quand la tâche Contrôle des périphériques est arrêtée. Si la case est cochée et que la tâche Contrôle des périphériques n'est pas exécutée, Kaspersky Embedded Systems Security autorise l'utilisation de n'importe quel périphérique externe sur un périphérique protégé. Si la case est décochée, l'application interdit l'utilisation des périphériques externes douteux sur un périphérique protégé quand la tâche Contrôle des périphériques n'est pas exécutée ou que le service Kaspersky Security est désactivé. Il est conseillé d'utiliser cette option pour garantir la protection maximale contre les menaces sur la sécurité informatique qui surgissent lors de l'échange de fichiers avec des périphériques externes. Cette case est décochée par défaut.
Règles du Contrôle des périphériques	Vous pouvez modifier la liste des règles du Contrôle des périphériques.
Administration des tâches	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Gestion du pare-feu

Cette section contient des informations sur la tâche Gestion du pare-feu et sa configuration.

A propos de la tâche Gestion du pare-feu

Kaspersky Embedded Systems Security offre une solution fiable et conviviale pour la protection des connexions réseau grâce à la tâche Gestion du pare-feu.

La tâche Gestion du pare-feu ne réalise pas un filtrage indépendant du trafic réseau, mais elle permet d'administrer le pare-feu Windows via l'interface graphique de Kaspersky Embedded Systems Security. Au cours de l'exécution de la tâche Gestion du pare-feu, Kaspersky Embedded Systems Security assume l'administration des paramètres et des stratégies du pare-feu du système d'exploitation et interdit toute tentative de configuration externe du pare-feu.

Au cours de l'installation de l'application, le composant Gestion du pare-feu lit et copie l'état du pare-feu Windows, ainsi que toutes les règles définies. Par la suite, la modification de l'ensemble des règles ou de leurs paramètres, ainsi que l'arrêt ou le lancement du pare-feu seront possibles uniquement via Kaspersky Embedded Systems Security.

Si le pare-feu Windows est désactivé lors de l'installation de Kaspersky Embedded Systems Security, la tâche Gestion du pare-feu n'est pas lancée à la fin de l'installation. Si le pare-feu Windows est activé lors de l'installation de l'application, la tâche Gestion du pare-feu est exécutée à la fin de l'installation et bloque toutes les connexions de réseau sur la base des règles définies autorisées.

Le composant Gestion du pare-feu n'est pas repris dans la sélection de composants de l'installation Recommandée et n'est pas installé par défaut.

La tâche Gestion du pare-feu force l'interdiction de tous les connexions entrantes et sortantes si elles ne sont pas autorisées par les règles définies de la tâche.

La tâche interroge régulièrement le pare-feu Windows et contrôle son état. L'intervalle de sondage par défaut est de 1 minute et il n'est pas modifiable. Si Kaspersky Embedded Systems Security détecte un écart entre les paramètres du pare-feu Windows et ceux de la tâche Gestion du pare-feu, l'application impose les paramètres de la tâche au pare-feu du système d'exploitation.

En interrogeant le Pare-feu Windows toutes les minutes, Kaspersky Embedded Systems Security surveille les éléments suivants :

- état de fonctionnement du pare-feu Windows ;
- l'état de règles ajoutées par d'autres applications ou outils (par exemple, ajout d'une nouvelle règle de l'application pour un port/une application à l'aide de wf.msc) après l'installation de Kaspersky Embedded Systems Security.

Lors de l'application de nouvelles règles au Pare-feu Windows, Kaspersky Embedded Systems Security crée l'ensemble de règles Kaspersky Security Group dans le composant logiciel enfichable du Pare-feu Windows. Ce jeu de règles contient toutes les règles créées par Kaspersky Embedded Systems Security à l'aide de la tâche de Gestion du pare-feu. Les règles qui figurent dans le groupe Kaspersky Security Group ne sont pas contrôlées par l'application lors du sondage et elles ne sont pas synchronisées automatiquement avec la liste des règles définies dans les paramètres de la tâche Gestion du pare-feu. Le cas échéant, vous pouvez actualiser manuellement les règles de Kaspersky Security.

Pour mettre à jour manuellement la liste des règles Kaspersky Security Group,

redémarrez la tâche Gestion du pare-feu de Kaspersky Embedded Systems Security.

Vous pouvez également modifier les règles de Kaspersky Security Group manuellement dans le composant logiciel enfichable Pare-feu Windows.

Le lancement de la tâche Gestion du pare-feu est impossible si le pare-feu Windows est administré par une stratégie de groupe Kaspersky Security Center.

A propos des règles du pare-feu

La tâche Gestion du pare-feu contrôle le filtrage du trafic entrant et sortant à l'aide de règles d'autorisation qui sont imposées au pare-feu Windows lors de l'exécution de la tâche.

Au premier lancement de la tâche, Kaspersky Embedded Systems Security lit toutes les règles pour le trafic entrant définies dans les paramètres du pare-feu Windows et les copie dans la tâche Gestion du pare-feu. Par la suite, l'application fonctionne conformément aux algorithmes suivants :

- si une règle est créée, manuellement ou automatiquement suite à l'installation d'une nouvelle application, dans les paramètres du pare-feu Windows, Kaspersky Embedded Systems Security supprime cette règle.
- si une règle existante est supprimée dans les paramètres du pare-feu Windows, Kaspersky Embedded Systems Security restaure cette règle après le redémarrage de la tâche.
- si les paramètres d'une règle existante sont modifiés dans les paramètres du pare-feu Windows, Kaspersky Embedded Systems Security annule les modifications.
- si une règle est créée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Embedded Systems Security impose cette règle au pare-feu Windows.
- si un règle existante est supprimée dans les paramètres de la tâche Gestion du pare-feu, Kaspersky Embedded Systems Security impose la suppression de cette règle dans les paramètres du pare-feu Windows.

Vous pouvez administrer différents types de Règles du pare-feu : pour les applications et pour les ports.

Comportement des règles par défaut lors de l'installation et de la suppression de l'application

Lors de l'installation, un ensemble de règles d'autorisation est créé pour empêcher le blocage des applications installées avec Kaspersky Embedded Systems Security et pour garantir leur fonctionnement continu. Voici les détails et les limites.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau entrant lorsque vous installez l'application sur un périphérique qui exécute n'importe quelle version compatible du système d'exploitation Windows :

- Règles d'autorisation pour ouvrir la Console de Kaspersky Embedded Systems Security, situées dans le dossier d'installation de l'application. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Deux règles d'autorisation pour le port local 15000, si l'Agent d'administration de Kaspersky Security Center est installé sur le périphérique. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau sortant lorsque vous installez l'application sur un périphérique qui exécute Windows 7 ou version ultérieure :

- Règles d'autorisation pour Kaspersky Security Management, situées dans le dossier d'installation de l'application. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Règles d'autorisation pour Kaspersky Embedded Systems Security, situées dans le dossier d'installation de l'application. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.
- Deux règles d'autorisation pour le port local 13000, si l'Agent d'administration de Kaspersky Security Center est installé sur le périphérique. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UPD – une règle par protocole.

Lorsque vous désinstallez Kaspersky Embedded Systems Security, l'application supprime toutes les règles de pare-feu créées, à l'exception des règles créées par l'Agent d'administration de Kaspersky Security Center, telles que Kaspersky Security Center WDS et Kaspersky Administration Kit. De plus, l'application supprime les règles ICMPv4 et ICMPv6 pour Windows 7 et versions ultérieures.

Lorsque vous désinstallez Kaspersky Embedded Systems Security, l'application active toutes les connexions ICMP pour les systèmes d'exploitation antérieurs à Windows 7.

Règles pour les applications

Les règles de ce type autorisent au cas par cas les connexions pour les apps indiquées. Le critère de déclenchement de ces règles est le chemin d'accès au fichier exécutable.

Vous pouvez administrer les règles pour les apps :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le chemin d'accès au fichier exécutable et la zone d'application de la règle.

Règles pour les ports

Les règles de ce type autorisent les connexions réseau pour les ports et les protocoles indiqués (TCP / UDP). Les critères de déclenchement de ces règles sont le numéro du port et le type de protocole.

Vous pouvez administrer les règles pour les ports :

- ajouter de nouvelles règles ;
- supprimer des règles existantes ;
- activer ou désactiver les règles définies ;
- modifier les paramètres des règles définies : indiquer le nom de la règle, le numéro de port, le type de protocole et la zone d'application de la règle.

Les règles pour les ports impliquent une plus grande zone d'action que les règles pour les apps. En autorisant les connexions sur la base de règles pour les ports, vous abaissez le niveau de sécurité de l'appareil protégé.

Paramètres par défaut de la tâche Gestion du pare-feu

La tâche Gestion du pare-feu utilise les paramètres par défaut décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres par défaut de la tâche Gestion du pare-feu

Paramètre	Valeur par défaut	Description
Connexions entrantes	**Interdire**	Vous pouvez configurer les paramètres des règles de trafic entrant pour bloquer ou autoriser les connexions entrantes. Par défaut, le type de la règle est opposé au type de stratégie. Par exemple, pour la stratégie Interdire par défaut, la valeur par défaut de la règle est **Autoriser**. Pour la stratégie Autoriser par défaut, la valeur par défaut de la règle est **Interdire**. Le cas échéant, vous pouvez modifier le type de la règle.
Connexions sortantes	**Autoriser**	Vous pouvez configurer les paramètres des règles de trafic sortant pour bloquer ou autoriser les connexions sortantes. Par défaut, le type de la règle est opposé au type de stratégie. Par exemple, pour la stratégie Interdire par défaut, la valeur par défaut de la règle est **Autoriser**. Pour la stratégie Autoriser par défaut, la valeur par défaut de la règle est **Interdire**. Le cas échéant, vous pouvez modifier le type de la règle.
Autoriser les connexions ICMP	**Désactivée**	Cette option contrôle simultanément les connexions ICMP entrantes et sortantes via les protocoles ICMPv4 et ICMPv6. Si l'option est activée, Kaspersky Embedded Systems Security ignore la valeur **Interdire** configurée pour les paramètres de connexion entrante ou de connexion sortante. La priorité de l'option **Autoriser les connexions ICMP** sélectionnée est plus élevée.
Planification du lancement de la tâche	S/O	La tâche Gestion du pare-feu n'est pas lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez configurer la planification du lancement de la tâche.

Administration des règles du pare-feu via le plug-in d'administration

Cette section explique comment administrer les règles du pare-feu via l'interface du Plug-in d'administration.

Activation et désactivation des règles du pare-feu

Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** de la sous-section **Gestion du pare-feu**.
5. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

   La fenêtre **Règles du pare-feu entrantes** s'ouvre.
6. En fonction du type de règle dont vous souhaitez modifier l'état, cliquez sur le lient **Entrant** ou **Sortant**, puis choisissez l'onglet **Applications** ou **Ports**.
7. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :
   - Si vous voulez qu'une règle inactive soit appliquée, cochez la case à gauche du nom de la règle.

     La règle choisie sera activée.
   - Si vous voulez qu'une règle active ne soit plus appliquée, décochez la case à gauche du nom de la règle.

     La règle choisie sera désactivée.
8. Dans la fenêtre **Règles du pare-feu entrantes**, cliquez sur **OK**.
9. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la stratégie>**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Ajout manuel de règles du pare-feu

Vous pouvez ajouter ou modifier uniquement les règles pour les applications et les ports. Vous ne pouvez pas ajouter des règles de groupe ou modifier les règles de groupe existantes.

Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** de la sous-section **Gestion du pare-feu**.
5. Dans la fenêtre **Gestion du pare-feu** qui s'affiche, sous l'onglet **Général**, cliquez sur le bouton **Liste des règles** en face de la sous-section **Entrante ou sortante** selon le type de connexion que vous souhaitez configurer.

   Lorsque vous configurez les règles pour les connexions entrantes et sortantes, tenez compte des options et limitations suivantes :
   - Par défaut, le type de la règle est opposé au type de stratégie. Par exemple, pour la stratégie Interdire par défaut, la valeur par défaut de la règle est **Autoriser**. Pour la stratégie Autoriser par défaut, la valeur par défaut de la règle est **Bloquer**. Le cas échéant, vous pouvez modifier le type de la règle.
   - Vous pouvez configurer les paramètres de la tâche par défaut si vous connectez une Console de l'application locale à un périphérique distant qui exécute n'importe quel système d'exploitation ou si vous connectez une Console de l'application locale à un périphérique local qui exécute Windows 7 ou une version ultérieure.
   - La configuration des paramètres par défaut de la tâche Pare-feu n'est pas disponible si vous connectez une Console de l'application locale à un périphérique local qui exécute un système d'exploitation antérieur à Windows 7.
6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications** ou **Ports** et exécutez l'une des actions suivantes :
   - Pour modifier une règle existante, sélectionnez dans la liste des règles celle dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Modifier**.
   - Pour créer une règle, cliquez sur le bouton **Ajouter**.

     En fonction du type de la règle à configurer, la fenêtre **Configurer une règle pour un port** ou **Règle pour l'application** s'ouvre.
7. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

- Si vous travaillez avec la règle pour une app, procédez comme suit :

  a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

  b. Dans la liste **Action de la règle**, sélectionnez l'option **Autoriser** ou **Interdire**, selon le cas.

  c. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.

  Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.

  d. Saisissez dans le champ **Action de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

  Les adresses IP doivent obligatoirement être saisies au format IPv4.

- Si vous travaillez avec une règle pour un port, procédez comme suit :

  a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

  b. Dans la liste **Action de la règle**, sélectionnez l'option **Autoriser** ou **Interdire**, selon le cas.

  c. Dans la sous-section **Port local**, indiquez le **numéro de port ou la plage de ports**, selon le cas.

  Lorsque vous configurez les ports pour établir une connexion réseau, tenez compte des options et des limitations suivantes.

  Pour les connexions entrantes, vous définissez les paramètres de port pour un périphérique local. Pour les connexions sortantes, vous définissez les paramètres de port pour les périphériques distants.

  Pour l'option **Numéro de port**, les valeurs disponibles sont comprises entre 1 et 65535.

  Pour l'option **Plage de ports**, les valeurs disponibles sont 1à 10, 20 à 30 000 et 1 à 65 535.

  Les limites des paramètres du port sont les suivantes :

  - Pour configurer une connexion réseau pour un périphérique local fonctionnant sous Windows XP, vous ne pouvez indiquer qu'un seul port dans les paramètres du port, car Windows XP n'est pas compatible avec les paramètres de plage de ports.
  - Pour configurer une connexion réseau pour un périphérique distant fonctionnant sous Windows XP, vous pouvez choisir **Plage de ports**, mais la règle s'applique uniquement au premier port de la plage définie, car Windows XP n'est pas compatible avec les paramètres de plage de ports.

  d. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.

  e. Saisissez dans le champ **Action de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

  Les adresses IP doivent obligatoirement être saisies au format IPv4.

8. Dans la fenêtre **Règle pour l'application** ou **Configurer une règle pour un port**, cliquez sur le bouton **OK**.

9. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
10. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la stratégie>**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configuration** de la sous-section **Gestion du pare-feu**.
5. Cliquez sur le bouton **Liste des règles** dans la fenêtre qui s'ouvre.

   La fenêtre **Règles du pare-feu entrantes** s'ouvre.
6. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.
7. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
8. Cliquez sur le bouton **Supprimer**.

   La règle sélectionnée sera supprimée.
9. Dans la fenêtre **Règles du pare-feu entrantes**, cliquez sur **OK**.
10. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.
11. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : <Nom de la stratégie>**.

Les paramètres définis de la tâche Gestion du pare-feu sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Administration des règles du pare-feu via la Console de l'application

Cette section explique comment administrer les règles du pare-feu via l'interface de la Console de l'application.

Activation et désactivation des règles du pare-feu

Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Dans le panneau de détails du nœud **Gestion du pare-feu**, cliquez sur le lien **Règles du pare-feu**.
   La fenêtre **Règles du pare-feu** s'ouvre.
4. En fonction du type de règle dont vous souhaitez modifier l'état, cliquez sur le lient **Entrant** ou **Sortant**, puis choisissez l'onglet **Applications** ou **Ports**.
5. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :
   - Si vous voulez qu'une règle inactive soit appliquée, cochez la case à gauche du nom de la règle.
     La règle choisie sera activée.
   - Si vous voulez qu'une règle active ne soit plus appliquée, décochez la case à gauche du nom de la règle.
     La règle choisie sera désactivée.
6. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Ajout manuel de règles du pare-feu

Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Selon le type de connexion que vous souhaitez configurer, cliquez sur le lien **Connexion entrante ou sortante** dans le volet des détails du nœud **Gestion du pare-feu**.

Lorsque vous configurez les règles pour les connexions entrantes et sortantes, tenez compte des options et limitations suivantes :

- Par défaut, le type de la règle est opposé au type de stratégie. Par exemple, pour la stratégie Interdire par défaut, la valeur par défaut de la règle est **Autoriser**. Pour la stratégie Autoriser par défaut, la valeur par défaut de la règle est **Bloquer**. Le cas échéant, vous pouvez modifier le type de la règle.
- Vous pouvez configurer les paramètres de la tâche par défaut si vous connectez une Console de l'application locale à un périphérique distant qui exécute n'importe quel système d'exploitation ou si vous connectez une Console de l'application locale à un périphérique local qui exécute Windows 7 ou une version ultérieure.
- La configuration des paramètres par défaut de la tâche Pare-feu n'est pas disponible si vous connectez une Console de l'application locale à un périphérique local qui exécute un système d'exploitation antérieur à Windows 7.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications** ou **Ports** et exécutez l'une des actions suivantes :
   - Pour modifier une règle existante, sélectionnez dans la liste des règles celle dont vous souhaitez modifier les paramètres, puis cliquez sur le bouton **Modifier**.
   - Pour créer une règle, cliquez sur le bouton **Ajouter**.

     En fonction du type de la règle à configurer, la fenêtre **Configurer une règle pour un port** ou **Règle pour l'application** s'ouvre.
5. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Si vous travaillez avec la règle pour une app, procédez comme suit :
     a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.
     b. Dans la liste **Action de la règle**, sélectionnez l'option **Autoriser** ou **Interdire**, selon le cas.
     c. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.

        Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.
     d. Saisissez dans le champ **Action de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

     Les adresses IP doivent obligatoirement être saisies au format IPv4.
   - Si vous travaillez avec une règle pour un port, procédez comme suit :
     a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.
     b. Dans la liste **Action de la règle**, sélectionnez l'option **Autoriser** ou **Interdire**, selon le cas.
     c. Dans la sous-section **Port local**, attribuez une valeur au paramètre **Numéro de port** ou **Plage de ports**, selon le cas.

Lorsque vous configurez les ports pour établir une connexion réseau, tenez compte des options et des limitations suivantes.

Pour les connexions entrantes, vous définissez les paramètres de port pour un périphérique local. Pour les connexions sortantes, vous définissez les paramètres de port pour les périphériques distants.

Pour l'option **Numéro de port**, les valeurs disponibles sont comprises entre 1 et 65535.

Pour l'option **Plage de ports**, les valeurs disponibles sont 1à 10, 20 à 30 000 et 1 à 65 535.

Les limites des paramètres du port sont les suivantes :

- Pour configurer une connexion réseau pour un périphérique local fonctionnant sous Windows XP, vous ne pouvez indiquer qu'un seul port dans les paramètres du port, car Windows XP n'est pas compatible avec les paramètres de plage de ports.
- Pour configurer une connexion réseau pour un périphérique distant fonctionnant sous Windows XP, vous pouvez choisir **Plage de ports**, mais la règle s'applique uniquement au premier port de la plage définie, car Windows XP n'est pas compatible avec les paramètres de plage de ports.

d. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.

e. Saisissez dans le champ **Action de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

6. Dans la fenêtre **Règle pour l'application** ou **Configurer une règle pour un port**, cliquez sur le bouton **OK**.
7. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Contrôle de l'ordinateur**.
2. Sélectionnez le nœud enfant **Gestion du pare-feu**.
3. Dans le panneau de détails du nœud **Gestion du pare-feu**, cliquez sur le lien **Règles du pare-feu**.
   La fenêtre **Règles du pare-feu** s'ouvre.
4. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Applications** ou **Ports**.

5. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
6. Cliquez sur le bouton **Supprimer**.

   La règle sélectionnée sera supprimée.
7. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Administration des règles du pare-feu via le Plug-in Web

Pour configurer les règles du pare-feu via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôle de l'activité réseau**.
5. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **Configuration**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la tâche Gestion du pare-feu

Paramètre	Description
Règles pour l'application	Vous pouvez administrer les règles pour les apps. Les règles de ce type autorisent au cas par cas les connexions pour les apps indiquées. Le critère de déclenchement de ces règles est le chemin d'accès au fichier exécutable.
Règles pour un port	Vous pouvez administrer les règles pour les ports. Les règles de ce type autorisent les connexions réseau pour les ports et les protocoles indiqués (TCP / UDP). Les critères de déclenchement de ces règles sont le numéro du port et le type de protocole.
Administration des tâches	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Activation et désactivation des règles du pare-feu

Pour activer ou désactiver une règle existante de filtrage du trafic entrant, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôle de l'activité réseau**.

5. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **Configuration**.

6. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Règles pour l'application** ou **Règles pour un port**.

7. Dans la liste des règles, trouvez celle dont vous souhaitez modifier l'état, puis réalisez une des opérations suivantes :

   - Si vous voulez qu'une règle inactive soit appliquée, activez le bouton bascule à gauche du nom de la règle.
   - Si vous voulez qu'une règle active ne soit plus appliquée, désactivez le bouton à bascule gauche du nom de la règle.

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

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Ajout manuel de règles du pare-feu

Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.

2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité réseau**.

5. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **Configuration**.

6. En fonction du type de règle dont vous souhaitez modifier l'état, choisissez l'onglet **Règles entrantes ou sortantes** **pour les applications Règles entrantes ou sortantes pour les ports** et exécutez une des actions suivantes :

   Lorsque vous configurez les règles pour les connexions entrantes et sortantes, tenez compte des options et limitations suivantes :

   - Par défaut, le type de la règle est opposé au type de stratégie. Par exemple, pour la stratégie Interdire par défaut, la valeur par défaut de la règle est **Autoriser**. Pour la stratégie Autoriser par défaut, la valeur par défaut de la règle est **Bloquer**. Le cas échéant, vous pouvez modifier le type de la règle.
   - Vous pouvez configurer les paramètres de la tâche par défaut si vous connectez une Console de l'application locale à un périphérique distant qui exécute n'importe quel système d'exploitation ou si vous connectez une Console de l'application locale à un périphérique local qui exécute Windows 7 ou une version ultérieure.
   - La configuration des paramètres par défaut de la tâche Pare-feu n'est pas disponible si vous connectez une Console de l'application locale à un périphérique local qui exécute un système d'exploitation antérieur à Windows 7.

   - Pour modifier une règle existante, sélectionnez la règle à éditer, puis cliquez sur **Modifier**.
   - Pour créer une règle, cliquez sur le bouton **Ajouter**.

7. Dans la partie droite de l'écran, réalisez les opérations suivantes :

- Si vous travaillez avec la règle pour une app, procédez comme suit :

  a. Cochez la case **Utiliser la règle** si vous souhaitez appliquer la règle créée.

  b. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

  c. Dans la liste **Action de la règle**, sélectionnez l'option **Autoriser** ou **Interdire**, selon le cas.

  d. Saisissez dans le champ **Chemin d'accès à l'application** le chemin d'accès au fichier exécutable de l'application pour laquelle vous souhaitez autoriser la connexion en modifiant la règle.

  e. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

  Les adresses IP doivent obligatoirement être saisies au format IPv4.

- Si vous travaillez avec une règle pour un port, procédez comme suit :

  a. Cochez la case **Utiliser la règle** si vous souhaitez appliquer la règle créée.

  b. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

  c. Saisissez dans le champ **Numéro de port ou Plage de ports** le ou les ports pour lesquels l'application autorisera les connexions.

  Lorsque vous configurez les ports pour établir une connexion réseau, tenez compte des options et des limitations suivantes.

  Pour les connexions entrantes, vous définissez les paramètres de port pour un périphérique local. Pour les connexions sortantes, vous définissez les paramètres de port pour les périphériques distants.

  Pour l'option **Numéro de port**, les valeurs disponibles sont comprises entre 1 et 65535.

  Pour l'option **Plage de ports**, les valeurs disponibles sont 1à 10, 20 à 30 000 et 1 à 65 535.

  Les limites des paramètres du port sont les suivantes :

  - Pour configurer une connexion réseau pour un périphérique local fonctionnant sous Windows XP, vous ne pouvez indiquer qu'un seul port dans les paramètres du port, car Windows XP n'est pas compatible avec les paramètres de plage de ports.
  - Pour configurer une connexion réseau pour un périphérique distant fonctionnant sous Windows XP, vous pouvez choisir **Plage de ports**, mais la règle s'applique uniquement au premier port de la plage définie, car Windows XP n'est pas compatible avec les paramètres de plage de ports.

  d. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.

  e. Saisissez dans le champ **Zone d'application de la règle** les adresses réseau auxquelles la règle configurée sera appliquée.

Les adresses IP doivent obligatoirement être saisies au format IPv4.

8. Cliquez sur le bouton **OK**.
9. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **OK**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Suppression de règles du pare-feu

Vous pouvez supprimer uniquement les règles pour les apps et les ports. Vous ne pouvez pas supprimer les règles existantes pour les groupes.

Pour supprimer une règle existante du filtrage du trafic entrant, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôle de l'activité réseau**.
5. Dans la fenêtre **Gestion du pare-feu**, cliquez sur **Configuration**.
6. En fonction du type de règle que vous souhaitez supprimer, choisissez l'onglet **Règles pour l'application** ou **Règles pour un port**.
7. Dans la liste des règles, sélectionnez celle que vous voulez supprimer.
8. Cliquez sur le bouton **Supprimer**.

   La règle sélectionnée sera supprimée.
9. Cliquez sur le bouton **OK**.

Les paramètres définis de la tâche sont enregistrés. Les paramètres de la nouvelle règle sont envoyés au pare-feu Windows.

Moniteur d'intégrité des fichiers

Cette section contient des informations sur le lancement et la configuration de la tâche Moniteur d'intégrité des fichiers.

A propos de la tâche Moniteur d'intégrité des fichiers

La tâche Moniteur d'intégrité des fichiers permet de surveiller les actions exécutées sur les fichiers et les dossiers indiqués au sein des zones de surveillance définies dans les paramètres de la tâche. Vous pouvez utiliser la tâche pour détecter les modifications des fichiers afin d'identifier une violation de la sécurité sur l'appareil protégé. Il est également possible de configurer le suivi des modifications des fichiers pendant la durée d'interruption du monitoring.

L'*interruption de la surveillance* désigne une période au cours de laquelle la zone de surveillance est exclue temporairement de la zone d'action de la tâche, par exemple suite à l'arrêt de la tâche ou en l'absence physique d'un périphérique externe sur le périphérique protégé. Kaspersky Embedded Systems Security signale la détection d'opérations sur les fichiers dans la zone de surveillance dès qu'un périphérique externe est connecté.

Une suspension de l'exécution de la tâche dans la zone de surveillance définie suite à la réinstallation du composant Moniteur d'intégrité des fichiers ne constitue pas une interruption de la surveillance. Dans ce cas, la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

Exigences applicables à l'environnement

Pour permettre le lancement de la tâche Moniteur d'intégrité des fichiers sur les fichiers, les conditions suivantes doivent être remplies :

- Les systèmes de fichiers ReFS ou NTFS doivent être utilisés sur le périphérique protégé.
- Le journal USN Windows doit être activé. Le composant interroge ce journal afin d'obtenir des informations sur les opérations sur les fichiers.

  Si vous avez activé le journal USN après que vous avez créé une règle pour un volume et lancé la tâche Moniteur d'intégrité des fichiers, il faut relancer la tâche. Dans le cas contraire, cette règle n'est pas prise en compte par le monitoring.

Exclusions pour la zone de surveillance

Vous pouvez créer des zones de surveillance exclues. Les exclusions sont définies pour chaque règle distincte et fonctionnent uniquement pour la zone de surveillance indiquée. Vous pouvez définir un nombre illimité d'exclusions pour chaque règle.

Les exclusions possèdent une priorité plus grande dans la zone de surveillance et elles ne sont pas contrôlées par la tâche, même si un dossier ou fichier indiqué se trouve dans la zone de surveillance. Si les paramètres d'une des règles définissent une zone de surveillance à un niveau inférieur à celui du dossier défini dans les exclusions, la zone de surveillance n'est pas prise en compte quand la tâche est exécutée.

Pour définir les exclusions, il convient d'utiliser les mêmes masques que ceux utilisés pour déterminer la zone de surveillance.

A propos des règles de monitoring des opérations sur les fichiers

La tâche Moniteur d'intégrité des fichiers est exécutée sur la base de règles de surveillance des opérations sur les fichiers. Les critères de déclenchement de la règle permettent de configurer les conditions de déclenchement d'une tâche et de régler le niveau d'importance des événement d'opérations réalisées sur les fichiers qui ont été détectées et consignées dans le journal d'exécution de la tâche.

La règle de monitoring des opérations sur les fichiers est définie pour chaque zone de surveillance.

Vous pouvez configurer les critères de déclenchement de la règle suivants :

- Utilisateurs de confiance
- Marqueurs d'opérations sur les fichiers

Utilisateurs de confiance

L'application considère par défaut les actions de tous les utilisateurs comme des violations potentielles de la sécurité. La liste des utilisateurs de confiance est vide. Vous pouvez configurer le niveau d'importance de l'événement en dressant une liste d'utilisateurs de confiance dans les paramètres de la règle de monitoring des opérations sur les fichiers.

L'état *utilisateur douteux* est attribué à tout utilisateur qui ne figure pas dans la liste des utilisateurs de confiance définie dans les paramètres de la zone de surveillance. Si Kaspersky Embedded Systems Security détecte une opération sur un fichier réalisée par un utilisateur douteux, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance Événement critique dans le journal d'exécution de la tâche.

L'état *utilisateur de confiance* est attribué à tout utilisateur ou groupe d'utilisateurs autorisé à exécuter des opérations sur les fichiers dans la zone de surveillance indiquée. Si Kaspersky Embedded Systems Security détecte une opération sur un fichier réalisée par un utilisateur de confiance, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance Événement d'information dans le journal d'exécution de la tâche.

Kaspersky Embedded Systems Security ne peut pas identifier l'utilisateur à l'origine des opérations quand celles-ci ont lieu lors des interruptions de la surveillance. Dans ce cas, l'état de l'utilisateur est défini comme inconnu.

L'état *utilisateur inconnu* est un état attribué à un utilisateur quand Kaspersky Embedded Systems Security ne peut pas recevoir les données relatives à l'utilisateur suite à une interruption de la tâche ou à un échec du pilote de synchronisation des données et du journal USN. Si Kaspersky Embedded Systems Security détecte une opération sur un fichier réalisée par un utilisateur inconnu, la tâche Moniteur d'intégrité des fichiers consigne l'événement avec le niveau d'importance *Avertissement* dans le journal d'exécution de la tâche.

Marqueurs d'opérations sur les fichiers

Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Embedded Systems Security utilise les marqueurs d'opérations sur les fichiers pour confirmer si une action a été réalisée sur le fichier.

Le marqueur d'opération sur les fichiers est un indice unique qui permet de définir une opération réalisée sur un fichier.

Chaque opération réalisée sur un fichier peut être composée d'une seule action ou d'une série d'actions exécutées sur les fichiers. Chaque action de ce genre reçoit un marqueur d'opérations sur les fichiers. Quand un marqueur que vous avez désigné comme critère de déclenchement de la règle de monitoring est détecté dans la chaîne d'opérations réalisées sur un fichier, l'application consigne l'événement lié à la réalisation d'une telle action.

Le niveau d'importance des événements consignés ne dépend pas des marqueurs d'opérations sur les fichiers choisis, ni de leur quantité.

Par défaut, Kaspersky Embedded Systems Security tient compte de tous les marqueurs d'opérations sur les fichiers disponibles. Vous pouvez sélectionner les marqueurs d'opérations sur les fichiers manuellement dans les paramètres des règles de la tâche (cf. tableau ci-dessous).

Marqueurs d'opérations sur les fichiers

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
BASIC_INFO_CHANGE	attributs ou horodatage d'un fichier ou d'un dossier modifiés	NTFS, ReFS
COMPRESSION_CHANGE	compression d'un fichier ou d'un dossier modifiée	NTFS, ReFS
DATA_EXTEND	taille du fichier ou du dossier augmentée	NTFS, ReFS
DATA_OVERWRITE	Données dans le fichier ou me dossier écrasées	NTFS, ReFS
DATA_TRUNCATION	fichier ou dossier tronqués	NTFS, ReFS
EA_CHANGE	attributs étendus du fichier ou du dossier modifiés	NTFS uniquement
ENCRYPTION_CHANGE	état de chiffrement malveillant du fichier ou du dossier modifié	NTFS, ReFS
FILE_CREATE	fichier ou dossier créés pour la première fois	NTFS, ReFS
FILE_DELETE	Fichier ou dossier supprimé définitivement par une combinaison MAJ+SUPPR	NTFS, ReFS
HARD_LINK_CHANGE	lien physique pour le fichier ou le dossier créé ou supprimé	NTFS uniquement
INDEXABLE_CHANGE	état d'indexation du fichier ou du dossier modifié	NTFS, ReFS
INTEGRITY_CHANGE	attribut d'intégrité pour le flux de fichiers nommé modifié	ReFS uniquement
NAMED_DATA_EXTEND	taille du flux de fichiers nommé augmentée	NTFS, ReFS
NAMED_DATA_OVERWRITE	flux de fichiers nommé écrasé	NTFS, ReFS
NAMED_DATA_TRUNCATION	flux de fichiers nommé tronqué	NTFS, ReFS
OBJECT_ID_CHANGE	identifiant de fichier ou de dossier modifié	NTFS, ReFS
RENAME_NEW_NAME	nouveau nom attribué au fichier ou au dossier	NTFS, ReFS
REPARSE_POINT_CHANGE	point d'analyse répétée pour le fichier ou le dossier créé ou point d'analyse répétée existant modifié	NTFS, ReFS
SECURITY_CHANGE	autorisations d'accès au fichier ou au dossier modifiées	NTFS, ReFS
STREAM_CHANGE	flux de fichier nommé créé ou flux existant modifié	NTFS, ReFS
TRANSACTED_CHANGE	flux de fichier nommé modifié par la transaction TxF	ReFS uniquement

Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

La tâche Moniteur d'intégrité des fichiers possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs des paramètres dans les composants suivants :

- Plug-in d'administration
- Console de l'application
- Plug-in Web

Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur par défaut	Description
Zone de surveillance	Non configuré	Utilisez cette option pour définir les dossiers et les fichiers pour lesquels les opérations doivent être surveillées. Des événements de monitoring sont créés pour les dossiers et les fichiers de la zone de surveillance définie.
Liste des **Utilisateurs de confiance**	Non configuré	Utilisez cette option pour désigner des utilisateurs et/ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.
Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du contrôle	Appliquée	Utilisez cette option pour activer ou désactiver la consignation des opérations sur les fichiers exécutées dans les zones de surveillance indiquée au cours des périodes pendant lesquelles la tâche n'est pas en cours d'exécution. Par défaut, les statistiques sont compilées pour les utilisateurs et les objets douteux et inconnus.
Bloquer les tentatives de compromission du journal USN	Appliquée	Utilisez cette option pour activer et désactiver la protection du journal USN.
Appliquer la zone de confiance	Désactivée	Cochez ou décochez la case **Appliquer la zone de confiance** pour appliquer les exclusions **Zone de confiance** en plus de la zone de surveillance configurée pour une règle.
Détecter et bloquer toutes les opérations sur les fichiers dans la zone sélectionnée	Désactivée	Cochez ou décochez la case **Détecter et bloquer toutes les opérations sur les fichiers dans la zone sélectionnée** si vous souhaitez bloquer toutes les modifications pour la zone de surveillance sélectionnée.
Exclure les dossiers suivants du contrôle	Pas appliqué	Utilisez cette option pour contrôler l'application des exclusions pour les dossiers où il n'est pas nécessaire de surveiller les opérations réalisées sur les fichiers. Lors de l'exécution de la tâche Moniteur d'intégrité des fichiers, Kaspersky Embedded Systems Security ignore les zones de surveillance définies en tant qu'exclusion.
Calcul de la somme de contrôle	Pas appliqué	Utilisez cette option pour configurer le calcul de la somme de contrôle du fichier après les modifications introduites dans le fichier.

Marqueurs d'opérations sur les fichiers	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Utilisez cette option pour définir l'ensemble de marqueurs d'opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de surveillance se caractérise par au moins un des marqueurs indiqués, Kaspersky Embedded Systems Security génère un événement d'audit.
Planification du lancement de la tâche	Le premier lancement n'est pas défini	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Administrer le Moniteur d'intégrité des fichiers via le plug-in d'administration

Cette section explique comment configurer le Moniteur d'intégrité des fichiers via le Plug-in d'administration.

Configuration de la tâche Moniteur d'intégrité des fichiers

Pour configurer les paramètres de la tâche Moniteur d'intégrité des fichiers :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Diagnostic du système** de la sous-section **Moniteur d'intégrité des fichiers**, cliquez sur le bouton **Configuration**.

   La fenêtre **Moniteur d'intégrité des fichiers** s'ouvre.
5. Sous l'onglet **Paramètres de surveillance des opérations sur les fichiers** de la fenêtre qui s'ouvre, configurez les paramètres suivants :
   - Cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du contrôle**.

La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

Si la case est cochée, Kaspersky Embedded Systems Security consigne les événements survenus dans toutes les zones de surveillance quand la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

Si la case est décochée, les opérations sur les fichiers réalisées dans les zones de surveillance pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

Cette case est cochée par défaut.

- Décochez ou cochez la case **Bloquer les tentatives de compromission du journal USN**.

  La case active ou désactive la protection du journal USN.

  Si cette case est cochée, Kaspersky Embedded Systems Security bloquera les tentatives de suppression du journal USN ou de compromission du contenu du journal USN.

  Si la case est décochée, l'application ne surveillera pas les modifications apportées au journal USN.

  Cette case est cochée par défaut.

- Cochez ou décochez la case **Appliquer la zone de confiance**, le cas échéant.

  Si la case **Appliquer la zone de confiance** est cochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

  Si la case **Appliquer la zone de confiance** est décochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** ne sont pas appliqués à la zone de surveillance.

  Par défaut, la case est décochée.

- Ajoutez les zones de surveillance que la tâche doit surveiller.

6. Sous l'onglet **Administration des tâches**, configurez les paramètres de lancement de la tâche sur la base d'une planification.

7. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Pour ajouter une zone de surveillance :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

- Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
- Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

  En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** de la sous-section **Moniteur d'intégrité des fichiers**, cliquez sur le bouton **Configuration**.

   La fenêtre **Moniteur d'intégrité des fichiers** s'ouvre.

5. Dans la section **Zone de surveillance**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle de surveillance des opérations sur les fichiers** s'ouvre.

6. Ajoutez une zone de monitoring à l'aide d'une des méthodes suivantes :

   - Si vous voulez choisir les dossiers via la boîte de dialogue Microsoft Windows standard :

     a. Cliquez sur le bouton **Parcourir**.

        La fenêtre standard de Microsoft Windows **Rechercher le dossier** s'ouvre.

     b. Dans la fenêtre **Rechercher le dossier** qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations, puis cliquez sur le bouton **OK**.

   - Si vous voulez définir la zone de surveillance manuellement, ajoutez le chemin d'accès à l'aide d'un des masques pris en charge :

     - <*.ext> : tous les fichiers avec l'extension <ext>, quel que soit leur emplacement ;
     - <*\name.ext> : tous les fichiers portant le nom name et l'extension <ext>, quel que soit leur emplacement ;
     - <\dir*> : tous les fichiers du dossier <\dir> ;
     - <\dir*\name.ext> : tous les fichiers portant le nom <name> et l'extension <ext> dans le dossier <\dir> et l'ensemble de ses sous-dossiers.

   Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque> En l'absence de l'indication du volume, Kaspersky Embedded Systems Security n'ajoute pas la zone de surveillance indiquée.

7. Sous l'onglet **Utilisateurs de confiance**, cliquez sur le bouton **Ajouter**.

   La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

8. Sélectionnez les utilisateurs ou groupes d'utilisateurs autorisés à exécuter des opérations sur les fichiers dans la zone de surveillance sélectionnée, puis cliquez sur **OK**.

Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.

9. Choisissez l'onglet **Marqueurs d'opérations sur les fichiers**.

10. Réalisez les opérations suivantes pour sélectionner plusieurs marqueurs d'opération sur les fichiers, le cas échéant :

    a. Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.

    b. Dans la liste des opérations sur les fichiers disponibles, cochez les cases en regard des opérations que vous souhaitez surveiller.

Kaspersky Embedded Systems Security détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

11. Si vous souhaitez bloquer toutes les opérations sur les fichiers pour la zone sélectionnées, cochez la case **Détecter et bloquer toutes les opérations sur les fichiers dans la zone sélectionnée**.

12. Si vous souhaitez que Kaspersky Embedded Systems Security calcule la somme de contrôle d'une fichier après une opération, procédez comme suit :

    a. Cochez la case **Calculer, si possible, la somme de contrôle du fichier. La somme de contrôle est reprise dans le rapport de la tâche** de la tâche.

    b. Dans la liste déroulante **Type de somme de contrôle**, sélectionnez une des options :

    - **Hash MD5**
    - **Hash SHA256**

13. Si vous ne souhaitez contrôler que certaines opérations sur les fichiers, ouvrez la liste des opérations disponibles, puis cochez les cases en regard des opérations que vous souhaitez contrôler.

14. Ajoutez les zones de surveillance exclues en fonction des besoins :

    a. Sélectionnez l'onglet **Exclusions**.

    b. Cochez la case Exclure les dossiers suivants du contrôle.

    c. Cliquez sur **Ajouter**.

    La fenêtre **Sélectionner un dossier à ajouter** s'ouvre.

    d. Dans la fenêtre qui s'ouvre, sélectionnez le dossier que vous souhaitez exclure de la zone de monitoring.

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

    Le dossier indiqué est ajouté à la liste des zones exclues.

15. Cliquez sur **OK** dans la fenêtre **Règle de surveillance des opérations sur les fichiers**.

    Les paramètres définis pour la règle seront appliqués à la zone de surveillance sélectionnée de la tâche Moniteur d'intégrité des fichiers.

Administrer le Moniteur d'intégrité des fichiers via la Console de l'application

Cette section explique comment configurer le Moniteur d'intégrité des fichiers via la Console de l'application.

Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers

Pour configurer les paramètres de la tâche Moniteur d'intégrité des fichiers :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Moniteur d'intégrité des fichiers**.
3. Dans le volet résultats du nœud **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général** de la fenêtre qui s'ouvre, configurez les paramètres suivants :
   a. Cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du contrôle**.

      La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

      Si la case est cochée, Kaspersky Embedded Systems Security consigne les événements survenus dans toutes les zones de surveillance quand la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

      Si la case est décochée, les opérations sur les fichiers réalisées dans les zones de surveillance pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

      Cette case est cochée par défaut.

   b. Décochez ou cochez la case **Bloquer les tentatives de compromission du journal USN**.

      La case active ou désactive la protection du journal USN.

      Si cette case est cochée, Kaspersky Embedded Systems Security bloquera les tentatives de suppression du journal USN ou de compromission du contenu du journal USN.

      Si la case est décochée, l'application ne surveillera pas les modifications apportées au journal USN.

      Cette case est cochée par défaut.

   c. Cochez ou décochez la case **Appliquer la zone de confiance**, le cas échéant.

Si la case **Appliquer la zone de confiance** est cochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

Si la case **Appliquer la zone de confiance** est décochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** ne sont pas appliqués à la zone de surveillance.

Par défaut, la case est décochée.

5. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche.

6. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Pour ajouter une zone de surveillance :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.

2. Choisissez le nœud enfant **Moniteur d'intégrité des fichiers**.

3. Dans le volet résultats du nœud **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Règles de surveillance des opérations sur les fichiers**.

   La fenêtre **Surveillance des opérations sur les fichiers** s'ouvre.

4. Ajoutez une zone de monitoring à l'aide d'une des méthodes suivantes :

   - Si vous voulez choisir les dossiers via la boîte de dialogue Microsoft Windows standard :

     a. Dans la section gauche de la fenêtre, cliquez sur le bouton **Parcourir**.

        La fenêtre standard de Microsoft Windows **Rechercher le dossier** s'ouvre.

     b. Dans la fenêtre **Rechercher le dossier** qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations, puis cliquez sur le bouton **OK**.

     c. Cliquez sur le bouton **Ajouter** pour que Kaspersky Embedded Systems Security commence à contrôler les opérations sur les fichiers dans la zone de surveillance indiquée.

   - Si vous voulez définir la zone de surveillance manuellement, ajoutez le chemin d'accès à l'aide d'un des masques pris en charge :

     - <*.ext> : tous les fichiers avec l'extension <ext>, quel que soit leur emplacement ;
     - <*\name.ext> : tous les fichiers portant le nom name et l'extension <ext>, quel que soit leur emplacement ;
     - <\dir*> : tous les fichiers du dossier <\dir> ;
     - <\dir*\name.ext> : tous les fichiers portant le nom <name> et l'extension <ext> dans le dossier <\dir> et l'ensemble de ses sous-dossiers.

Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque> En l'absence de l'indication du volume, Kaspersky Embedded Systems Security n'ajoute pas la zone de surveillance indiquée.

Dans la partie droite de la fenêtre, l'onglet **Description de la règle** affiche les utilisateurs de confiance et les marqueurs d'opérations sur les fichiers sélectionnés pour cette zone de surveillance.

5. Dans la liste des zones de surveillance ajoutées, sélectionnez celle que vous souhaitez configurer.

6. Ouvrez l'onglet **Utilisateurs de confiance**.

7. Cliquez sur **Ajouter**.

   La fenêtre standard de Microsoft Windows **Sélection d'utilisateurs ou de groupes** s'ouvre.

8. Choisissez les utilisateurs ou les groupes d'utilisateurs considérés que Kaspersky Embedded Systems Security considère comme étant de confiance pour la zone de surveillance sélectionnée.

9. Cliquez sur le bouton **OK**.

   Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.

10. Choisissez l'onglet **Marqueurs d'opérations sur les fichiers**.

11. Le cas échéant, sélectionnez plusieurs marqueurs d'opération sur les fichiers en réalisant les opérations suivantes :

    a. Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.

    b. Dans la liste des opérations sur les fichiers disponibles, cochez les cases en regard des opérations que vous souhaitez surveiller.

    Kaspersky Embedded Systems Security détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

12. Si vous souhaitez bloquer toutes les opérations sur les fichiers pour la zone sélectionnées, cochez la case **Détecter et bloquer toutes les opérations sur les fichiers dans la zone sélectionnée**.

13. Si vous souhaitez que Kaspersky Embedded Systems Security calcule la somme de contrôle d'une fichier après une opération, procédez comme suit :

    a. Dans la section **Calcul de la somme de contrôle**, sélectionnez l'option **Calculer, si possible, la somme de contrôle de la version finale d'un fichier après que le fichier a été modifié. La somme de contrôle est reprise dans le journal d'exécution de la tâche**.

    b. Sélectionnez une des options de la liste déroulante **Calculer la somme de contrôle selon l'algorithme** :

    - **Hash MD5**.
    - **Hash SHA256**.

14. Ajoutez les zones de surveillance excluses en fonction des besoins :

    a. Sélectionnez l'onglet **Définir les exclusions**.

    b. Cochez la case **Tenir compte des zones de surveillance exclues**.

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

    La fenêtre standard de Microsoft Windows **Rechercher le dossier** s'ouvre.

    d. Dans la fenêtre **Rechercher le dossier**, sélectionnez le dossier que vous souhaitez exclure de la zone de surveillance.

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

    f. Cliquez sur **Ajouter**.

    Le dossier indiqué est ajouté à la liste des zones exclues.

    > Vous pouvez également ajouter des exclusions pour la zone de surveillance manuellement en utilisant les masques identiques à ceux employés pour définir les zones de surveillance.

15. Cliquez sur le bouton **Enregistrer** pour appliquer la nouvelle configuration de règle.

Les paramètres définis pour la règle sont appliqués immédiatement à la zone de surveillance définie de la tâche **Moniteur d'accès au registre**.

Administrer le Moniteur d'intégrité des fichiers via le Plug-in Web

Cette section explique comment configurer le Moniteur d'intégrité des fichiers via le Plug-in Web.

Configuration de la tâche Moniteur d'intégrité des fichiers

Pour configurer la tâche Moniteur d'intégrité des fichiers via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic du système**.
5. Cliquez sur **Configuration** dans la sous-section **Moniteur d'intégrité des fichiers**.
6. Dans la fenêtre **Moniteur d'intégrité des fichiers** qui s'ouvre, accédez à l'onglet **Paramètres de surveillance des opérations sur les fichiers** et configurez les paramètres suivants :

    a. Cochez ou décochez la case **Consigner les informations relatives aux opérations exécutées pendant la durée d'interruption du contrôle**.

La case active ou désactive le contrôle des opérations sur les fichiers sélectionnées dans les paramètres de la tâche Moniteur d'intégrité des fichiers quand la tâche est suspendue pour une raison quelconque (extraction du disque dur, arrêt de la tâche par l'utilisateur, échec du logiciel).

Si la case est cochée, Kaspersky Embedded Systems Security consigne les événements survenus dans toutes les zones de surveillance quand la tâche Moniteur d'intégrité des fichiers n'est pas exécutée.

Si la case est décochée, les opérations sur les fichiers réalisées dans les zones de surveillance pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

Cette case est cochée par défaut.

b. Décochez ou cochez la case **Bloquer les tentatives de compromission du journal USN**.

La case active ou désactive la protection du journal USN.

Si cette case est cochée, Kaspersky Embedded Systems Security bloquera les tentatives de suppression du journal USN ou de compromission du contenu du journal USN.

Si la case est décochée, l'application ne surveillera pas les modifications apportées au journal USN.

Cette case est cochée par défaut.

c. Cochez ou décochez la case **Appliquer la zone de confiance**, le cas échéant.

Si la case **Appliquer la zone de confiance** est cochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

Si la case **Appliquer la zone de confiance** est décochée, les **Exclusions** et les **Processus de confiance** configurés dans la **Zone de confiance** ne sont pas appliqués à la zone de surveillance.

Par défaut, la case est décochée.

7. Sous l'onglet **Administration des tâches**, configurez la planification du lancement de la tâche.

8. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Pour ajouter une zone de surveillance :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.

2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Diagnostic du système**.

5. Cliquez sur **Configuration** dans la sous-section **Moniteur d'intégrité des fichiers**.

6. Dans la fenêtre **Moniteur d'intégrité des fichiers** qui s'ouvre, accédez à l'onglet **Paramètres de surveillance des opérations sur les fichiers**.

7. Dans la section **Journal USN**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle de surveillance des opérations sur les fichiers** s'ouvre.

8. Dans les **Contrôler les opérations sur les fichiers dans la zone**, renseignez un chemin à l'aide d'un masque pris en charge :

   - <*.ext> : tous les fichiers avec l'extension <ext>, quel que soit leur emplacement ;
   - <*\name.ext> : tous les fichiers portant le nom name et l'extension <ext>, quel que soit leur emplacement ;
   - <\dir*> : tous les fichiers du dossier <\dir> ;
   - <\dir*\name.ext> : tous les fichiers portant le nom <name> et l'extension <ext> dans le dossier <\dir> et l'ensemble de ses sous-dossiers.

   Au moment de définir une zone de monitoring manuellement, assurez-vous que le chemin d'accès respecte le format : <lettre du volume>:\<masque> En l'absence de l'indication du volume, Kaspersky Embedded Systems Security n'ajoute pas la zone de surveillance indiquée.

9. Dans la section **Utilisateurs de confiance**, réalisez une des opérations suivantes :

   - Cliquez sur le bouton **Ajouter** et, dans la fenêtre qui s'ouvre, spécifiez l'utilisateur dans le champ **Nom d'utilisateur** en utilisant la notation SID.
   - Cliquez sur le bouton **Ajouter depuis le Serveur d'administration** et, dans la fenêtre qui s'ouvre, sélectionnez l'utilisateur dans la liste.

   Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.

10. Cliquez sur le bouton **OK**.

11. Choisissez l'onglet **Marqueurs d'opérations sur les fichiers**.

12. Réalisez les opérations suivantes pour sélectionner plusieurs marqueurs d'opération sur les fichiers, le cas échéant :

    a. Choisissez l'option **Détecter les opérations sur les fichiers à l'aide des marqueurs suivants**.

    b. Dans la liste des opérations sur les fichiers disponibles, cochez les cases en regard des opérations que vous souhaitez surveiller.

    Kaspersky Embedded Systems Security détecte par défaut tous les marqueurs d'opérations sur les fichiers, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

13. Si vous souhaitez bloquer toutes les opérations sur les fichiers pour la zone sélectionnées, cochez la case **Détecter et bloquer toutes les opérations sur les fichiers dans la zone sélectionnée**.

14. Si vous souhaitez que Kaspersky Embedded Systems Security calcule la somme de contrôle d'une fichier après une opération :

    a. Cochez la case **Calculer, si possible, la somme de contrôle du fichier. La somme de contrôle est reprise dans le rapport de la tâche** de la tâche.

    b. Dans la liste déroulante **Type de somme de contrôle**, sélectionnez une des options :

    - **Hash SHA256**
    - **Hash MD5**

15. Si vous ne souhaitez contrôler que certaines opérations sur les fichiers, ouvrez la liste des opérations disponibles, puis cochez les cases en regard des opérations que vous souhaitez contrôler.

16. Ajoutez les zones de surveillance excluses en fonction des besoins :

    a. Sélectionnez l'onglet **Exclusions**.

    b. Cochez la case Exclure les dossiers suivants du contrôle.

    c. Cliquez sur **Ajouter**.

    La fenêtre **Sélectionner un dossier à ajouter** s'ouvre.

    d. Dans la fenêtre qui s'ouvre à droite, sélectionnez le dossier que vous souhaitez exclure de la zone de surveillance.

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

    Le dossier indiqué est ajouté à la liste des zones exclues.

17. Cliquez sur **OK** dans la fenêtre **Règle de surveillance des opérations sur les fichiers**.

    Les paramètres définis pour la règle seront appliqués à la zone de surveillance sélectionnée de la tâche Moniteur d'intégrité des fichiers.

Analyseur AMSI

Cette section contient des informations sur la tâche Scanner AMSI et sa configuration.

À propos de la tâche Analyseur AMSI

Pendant l'exécution de la tâche Scanner AMSI, Kaspersky Embedded Systems Security contrôle l'exécution des scripts créés à l'aide des technologies de création de scripts Microsoft Windows (Active Scripting) telles que VBScript ou JScript®. L'application peut également traiter les scripts PowerShell™ et les scripts exécutés dans les applications Microsoft Office sur les systèmes d'exploitation dotés de l'interface de l'Antimalware Scan Interface (AMSI). Vous pouvez autoriser ou bloquer l'exécution d'un script jugé dangereux ou probablement dangereux. Si Kaspersky Embedded Systems Security identifie un script comme potentiellement dangereux, il bloque ou autorise l'exécution du script en fonction de l'action que vous avez sélectionnée. Si l'action **Interdire** est sélectionnée, l'application autorise l'exécution du script uniquement si le script est considéré comme sûr.

À partir des systèmes d'exploitation Microsoft Windows 10 et Microsoft Windows Server 2016, Kaspersky Embedded Systems Security est compatible avec l'Antimalware Scan Interface (AMSI). AMSI permet aux applications et aux services de s'intégrer à n'importe quelle application de lutte contre les applications malveillantes installée sur le périphérique afin que tous les scripts exécutés soient interceptés et analysés par la solution anti-applications malveillantes.

Vous trouverez plus d'informations sur la fonctionnalité AMSI sur le site Internet de Microsoft Windows.

Vous pouvez configurer les paramètres de la tâche Scanner AMSI.

Paramètres par défaut de la tâche Analyseur AMSI

La tâche locale du système Scanner AMSI utilise les paramètres par défaut décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres par défaut de la tâche Scanner AMSI

Paramètre	Valeur par défaut	Description
Actions à exécuter sur les scripts dangereux	**Interdire**	Vous pouvez spécifier l'action à exécuter en cas de détection de scripts probablement dangereux : bloquer ou autoriser leur exécution.
Analyse heuristique	Le niveau de sécurité **Moyenne** est appliqué.	L'analyse heuristique peut être activée ou désactivée. Le niveau d'analyse peut être configuré.
Zone de confiance	Appliquée	Liste d'exclusions générale que vous pouvez appliquer dans les tâches sélectionnées.

Configuration des paramètres de la tâche Analyseur AMSI via le plug-in d'administration

Pour configurer une tâche Scanner AMSI :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Protection en temps réel du serveur** de la fenêtre **Propriétés : <nom de la stratégie>**, cliquez sur **Configuration** pour **Scanner AMSI**.

5. Dans la section **Actions à exécuter sur les scripts dangereux** de l'onglet **Général**, effectuez l'une des actions suivantes :

   - Pour autoriser l'exécution de scripts probablement dangereux, sélectionnez **Autoriser**.
   - Pour bloquer l'exécution de scripts probablement dangereux, sélectionnez **Interdire**.

6. Dans **Analyse heuristique**, réalisez une des opérations suivantes :

   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.
   - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

7. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.

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

Les nouveaux paramètres de la tâche sont appliqués.

Configuration des paramètres de la tâche Analyseur AMSI via la Console de l'application

Pour configurer une tâche Scanner AMSI :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Scanner AMSI**.

3. Dans le volet résultats du nœud, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre sous l'onglet **Général**.

4. Dans la section **Actions à exécuter sur les scripts dangereux**, effectuez l'une des actions suivantes :

   - Pour autoriser l'exécution de scripts probablement dangereux, sélectionnez **Autoriser**.

- Pour interdire l'exécution de scripts probablement dangereux, sélectionnez **Interdire**.

5. Dans **Analyse heuristique**, réalisez une des opérations suivantes :
   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.
   - Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.
6. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.
7. Cliquez sur le bouton **OK**.

Les nouveaux paramètres de la tâche sont appliqués.

Configuration des paramètres de la tâche Analyseur AMSI via le plug-in Web

Pour configurer une tâche Scanner AMSI :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel du serveur**.
5. Cliquez sur **Configuration** de la sous-section **Scanner AMSI**.
6. Dans la section **Actions à exécuter sur les scripts dangereux** de l'onglet **Général**, effectuez l'une des actions suivantes :
   - Pour autoriser l'exécution de scripts probablement dangereux, sélectionnez **Autoriser**.
   - Pour bloquer l'exécution de scripts probablement dangereux, sélectionnez **Interdire**.
7. Dans **Analyse heuristique**, réalisez une des opérations suivantes :
   - Cochez ou décochez la case **Utiliser l'analyse heuristique**.
   - Si nécessaire, ajustez le niveau de l'analyse heuristique.
8. Dans la section **Zone de confiance**, cochez ou décochez la case **Appliquer la zone de confiance**.
9. Cliquez sur le bouton **OK**.

Les nouveaux paramètres de la tâche sont appliqués.

Statistiques de la tâche Analyseur AMSI

Pendant l'exécution de la tâche **Scanner AMSI**, vous pouvez consulter les informations relatives au nombre de scripts traités par Kaspersky Embedded Systems Security depuis le lancement de la tâche.

Pour consulter les statistiques de la tâche Scanner AMSI, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Scanner AMSI**.

Les statistiques de la tâche en cours sont affichées dans le volet des résultats du nœud dans les sections **Administration** et **Statistiques**.

Vous pouvez consulter les informations sur les objets que Kaspersky Embedded Systems Security a traités au cours de la durée de la tâche (cf. tableau ci-dessous).

Statistiques de la tâche Analyseur AMSI

Champ	Description
Scripts bloqués	Nombre de scripts bloqués par Kaspersky Embedded Systems Security.
Scripts dangereux détectés	Nombre de scripts dangereux détectés.
Scripts présumés dangereux détectés	Nombre de scripts probablement dangereux détectés.
Scripts traités	Nombre total de scripts traités.

Moniteur d'accès au registre

Cette section explique comment démarrer et configurer la tâche Moniteur d'accès au registre.

À propos de la tâche Moniteur d'accès au registre

La tâche Moniteur d'accès au registre permet de surveiller les actions exécutées sur les branches et les clés du registre indiquées au sein des zones de surveillance définies dans les paramètres de la tâche. La tâche effectue le suivi des actions dans le système d'exploitation installé sur l'appareil ou dans les conteneurs Windows Server 2016 et suivants définis dans la zone de surveillance. Vous pouvez utiliser la tâche pour détecter les modifications afin d'identifier une violation de la sécurité sur l'appareil protégé.

Pour lancer la tâche Moniteur d'accès au registre, vous devez configurer au moins une règle de surveillance.

À propos des règles de surveillance du registre système

La tâche **Moniteur d'accès au registre** est exécutée en fonction des règles de surveillance du registre système. Les critères de déclenchement de la règle permettent de configurer les conditions de déclenchement d'une tâche et de régler le niveau d'importance des événements détectés qui ont été consignés dans le journal d'exécution de la tâche.

Une règle de surveillance du registre système est définie pour chaque zone de surveillance.

Vous pouvez configurer les critères de déclenchement de la règle suivants :

- **Actions**
- **Valeurs de registre**
- **Utilisateurs de confiance**

Actions

Quand la tâche Moniteur d'accès au registre est lancée, Kaspersky Embedded Systems Security utilise une liste d'actions pour surveiller le registre (cf. tableau ci-dessous).

Si une action définie comme critère de déclenchement de la règle est détectée, l'application consigne un événement respectif.

Le niveau d'importance des événements consignés ne dépend pas des actions sélectionnées ni du nombre d'événements.

Par défaut, Kaspersky Embedded Systems Security prend en compte toutes les actions. Vous pouvez configurer la liste des actions manuellement dans les paramètres des règles de la tâche.

Actions

Action	Restrictions	Système d'exploitation
Créer une clé	• Pour Windows XP et Windows Server 2003, si vous ajoutez **Créer une clé** à la liste des **Actions**, puis sélectionnez le mode **Bloquer les opérations selon les règles**, la création de la clé n'est pas bloquée dans les systèmes d'exploitation définis en raison des restrictions du système. La clé est créée avec une notification respective envoyée au journal des événements. • Si vous souhaitez interdire la création d'une clé particulière via RegEdit, créez une règle pour une clé de registre parent et assurez-vous d'ajouter **Créer des sous-clés** à la liste des **Actions**, puis sélectionnez le mode **Bloquer les opérations selon les règles**.	Windows XP et versions ultérieures
Supprimer une clé	Si vous souhaitez supprimer une clé parent, assurez-vous d'effacer à la fois les options **Supprimer une clé** et **Supprimer des sous-clés** dans la liste des **Actions** surveillées pour une clé de registre configurée, car vous ne pouvez supprimer que la clé parent avec des sous-clés.	Windows XP et versions ultérieures
Renommer une clé	S/O	Windows XP et versions ultérieures
Modifier les paramètres de sécurité de la clé	S/O	Windows Vista et versions ultérieures
Supprimer des valeurs	S/O	Windows XP et versions ultérieures
Définir les valeurs	Si vous ajoutez **Définir les valeurs** à la liste des **Actions**, que vous définissez le **Nom de la valeur** par défaut dans la règle d'une clé, puis que vous sélectionnez le mode **Bloquer les opérations selon les règles**, la clé n'est pas créée, car une nouvelle clé peut être créée uniquement avec une valeur par défaut.	Windows XP et versions ultérieures
Créer des sous-clés	S/O	Windows XP et versions ultérieures
Supprimer des sous-clés	S/O	Windows XP et versions ultérieures
Renommer des sous-clés	S/O	Windows XP et versions ultérieures
Modifier les paramètres de sécurité des sous-clés	S/O	Windows Vista et versions ultérieures

Valeurs de registre

En plus de la surveillance des clés de registre, vous pouvez bloquer ou surveiller les modifications des valeurs de registre existantes. Les options suivantes sont disponibles :

- **Définir la valeur** : créer les nouvelles valeurs de registre ou modifier les valeurs de registre existantes.
- **Supprimer une valeur** : supprimer les valeurs de registre existantes.

Renommer et modifier les paramètres de sécurité ne s'applique pas aux valeurs de registre.

Utilisateurs de confiance

L'application considère par défaut les actions de tous les utilisateurs comme des violations potentielles de la sécurité. La liste des utilisateurs de confiance est vide. Vous pouvez configurer le niveau d'importance de l'événement en dressant une liste d'utilisateurs de confiance dans les paramètres de la règle de surveillance du registre système.

Un *utilisateur douteux* désigne n'importe quel utilisateur qui ne figure pas dans la liste des utilisateurs de confiance définie dans les paramètres de la zone de surveillance. Si Kaspersky Embedded Systems Security détecte une action réalisée par un utilisateur douteux, la tâche Moniteur d'accès au registre consigne l'événement avec le niveau d'importance Événement critique dans le journal d'exécution de la tâche.

L'*utilisateur de confiance* est un utilisateur ou un groupe d'utilisateurs autorisé à exécuter des actions dans la zone de surveillance indiquée. Si Kaspersky Embedded Systems Security détecte une action réalisée par un utilisateur de confiance, la tâche Moniteur d'accès au registre consigne l'événement avec le niveau d'importance Événement d'information dans le journal d'exécution de la tâche.

Paramètres par défaut de la tâche Moniteur d'accès au registre

Les paramètres par défaut de la tâche Moniteur d'accès au registre sont décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs des paramètres dans les composants suivants :

- Plug-in d'administration
- Console de l'application
- Plug-in Web

Paramètres par défaut de la tâche Moniteur d'accès au registre

Paramètre	Valeur par défaut	Description
Zone de surveillance	Non définie	Utilisez cette option pour définir les clés de registre parent et les sous-clés à surveiller. Le paramètre est obligatoire. Si vous ne définissez pas le paramètre, la tâche ne démarre pas. Les événements de surveillance sont générés pour les clés et les sous-clés de registre parent dans la zone de surveillance définie.
Actions	Tous les éléments de la liste des actions sont sélectionnés	Utilisez cette option pour configurer une liste d'actions selon le cas en cochant et en décochant les cases respectives.
Valeurs de	Non définie	Utilisez cette option pour ajouter, modifier et supprimer les valeurs de

registre		registre que vous souhaitez surveiller pour la zone de surveillance définie.
Utilisateurs de confiance	Non définie	Utilisez cette option pour préciser des utilisateurs et/ou des groupes d'utilisateurs autorisés à effectuer les actions définies pour les clés de registre indiquées.
Mode de tâche	Statistiques seulement	Vous pouvez sélectionner le mode de tâche pour **Bloquer les opérations selon les règles** ou vous pouvez sélectionner le mode **Statistiques seulement** pour recevoir les notifications.
Appliquer la zone de confiance	Désactivée	Vous pouvez cocher ou décocher la case **Appliquer la zone de confiance** pour appliquer les exclusions de la **Zone de confiance** en plus de celles configurées pour une règle.
Planification du lancement de la tâche	Non définie	Vous pouvez configurer les paramètres pour lancer la tâche selon une planification.

Administration du Moniteur d'accès au registre via le plug-in d'administration

Cette section explique comment configurer la tâche Moniteur d'accès au registre via le plug-in d'administration.

Configurer les paramètres de la tâche Moniteur d'accès au registre

Pour configurer les paramètres généraux de la tâche Moniteur d'accès au registre, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Diagnostic du système** de la sous-section **Moniteur d'accès au registre**, cliquez sur le bouton **Configuration**.

   La fenêtre **Moniteur d'accès au registre** s'affiche.
5. Sous l'onglet **Paramètres du moniteur d'accès au registre**, configurez les paramètres suivants :
   - Dans le groupe **Mode de tâche**, sélectionnez l'option requise dans la liste :

- **Bloquer les opérations selon les règles**

  Si vous sélectionnez le mode **Bloquer les opérations selon les règles**, Kaspersky Embedded Systems Security bloque les **actions** définies pour la zone de surveillance. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne bloque pas les processus définis sous **Zone de confiance**.

  Par défaut, le mode **Statistiques seulement** est appliqué.

- **Statistiques seulement**

  Si le mode **Statistiques seulement** est sélectionné pour la zone de surveillance, Kaspersky Embedded Systems Security compile les statistiques pour les actions de clé de registre en fonction des règles configurées. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne compile pas les statistiques des processus définis sous **Zone de confiance**.

  Par défaut, le mode **Statistiques seulement** est appliqué.

- Cochez ou décochez la case **Appliquer la zone de confiance**, le cas échéant.

  Si la case **Appliquer la zone de confiance** est cochée, les **processus de confiance** configurés dans la **zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

  Si la case **Appliquer la zone de confiance** est décochée, les **processus de confiance** configurés dans la **zone de confiance** ne sont pas appliqués à la zone de surveillance.

  Par défaut, la case est décochée.

6. Ajoutez les zones de surveillance que la tâche doit surveiller.
7. Sous l'onglet **Administration des tâches**, configurez les paramètres de planification de la tâche.
8. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Les règles de surveillance sont appliquées les unes après les autres conformément à leur position dans la liste des règles configurées.

Pour ajouter une zone de surveillance :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

- Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
- Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

  En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système** de la sous-section **Moniteur d'accès au registre**, cliquez sur le bouton **Configuration**.

   La fenêtre **Moniteur d'accès au registre** s'affiche.

5. Dans la section **Surveiller les opérations dans le registre pour la zone**, cliquez sur le bouton **Ajouter**.

6. Dans la fenêtre **Zone de surveillance de l'accès au registre**, pour ajouter une zone de surveillance, indiquez un chemin à l'aide d'un masque pris en charge.

   Vous pouvez utiliser `?` et `*` comme masque lors de la saisie d'un chemin.

   Si vous saisissez le chemin d'accès à une clé de registre racine, assurez-vous de définir le chemin complet sans masque, par exemple `HKEY_USERS`. Voici une liste de clés de registre racine valides :

   - `HKEY_LOCAL_MACHINE`
   - `HKLM`
   - `HKEY_CURRENT_USER`
   - `HKCU`
   - `HKEY_USERS`
   - `HKUS`
   - `HKU`
   - `HKEY_CURRENT_CONFIG`
   - `HKEY_CLASSES_ROOT`
   - `CRHK`

Évitez d'utiliser des masques pris en charge pour les clés racines lors de la création des règles.
Si vous précisez uniquement une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, un grand nombre de notifications sur l'adressage des clés enfants indiquées est générée, ce qui entraîne des problèmes relatifs aux performances du système. Si vous précisez une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, et sélectionnez le mode **Bloquer les opérations selon les règles**, le système n'est pas en mesure de lire ni de modifier les clés nécessaires au fonctionnement du système d'exploitation et il ne répond pas.

7. Sous l'onglet **Ajouter**, configurez la liste des actions selon le cas.
8. Si vous souhaitez surveiller certaines **Valeurs de registre**, procédez comme suit :
   - Sous l'onglet **Valeurs de registre**, cliquez sur le bouton **Ajouter**.
   - Dans la fenêtre **Règle de valeur de registre**, saisissez le **Opérations contrôlées** et configurez les **Opérations contrôlées**.
   - Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
9. Si vous voulez définir les **Utilisateurs de confiance**, procédez comme suit :
   - Sous l'onglet **Utilisateurs de confiance**, cliquez sur le bouton **Ajouter**.
   - Dans la fenêtre **Sélection d'utilisateurs ou de groupes**, sélectionnez les utilisateurs ou les groupes d'utilisateurs autorisés à effectuer les actions définies.
   - Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

   Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.
10. Cliquez sur **OK** dans la fenêtre **Zone de surveillance de l'accès au registre**.

    Les paramètres définis pour la règle sont appliqués à la zone de surveillance définie de la tâche **Moniteur d'accès au registre**.

Administration du Moniteur d'accès au registre via la Console d'administration

Cette section explique comment configurer la tâche Moniteur d'accès au registre via la Console de l'application.

Configuration des paramètres de la tâche Moniteur d'accès au registre

Pour configurer les paramètres généraux de la tâche Moniteur d'accès au registre, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Moniteur d'accès au registre**.
3. Dans le volet résultats du nœud **Moniteur d'accès au registre**, cliquez sur le lien **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet **Général** de la fenêtre **Paramètres de la tâche**, configurez les paramètres suivants :
   - Dans le groupe **Mode de tâche**, sélectionnez l'option requise dans la liste :
     - Bloquer les opérations selon les règles

       Si vous sélectionnez le mode **Bloquer les opérations selon les règles**, Kaspersky Embedded Systems Security bloque les **actions** définies pour la zone de surveillance. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne bloque pas les processus définis sous **Zone de confiance**.

       Par défaut, le mode **Statistiques seulement** est appliqué.

     - Statistiques seulement

       Si le mode **Statistiques seulement** est sélectionné pour la zone de surveillance, Kaspersky Embedded Systems Security compile les statistiques pour les actions de clé de registre en fonction des règles configurées. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne compile pas les statistiques des processus définis sous **Zone de confiance**.

       Par défaut, le mode **Statistiques seulement** est appliqué.

   - Cochez ou décochez la case Appliquer la zone de confiance, le cas échéant.

     Si la case **Appliquer la zone de confiance** est cochée, les **processus de confiance** configurés dans la **zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

     Si la case **Appliquer la zone de confiance** est décochée, les **processus de confiance** configurés dans la **zone de confiance** ne sont pas appliqués à la zone de surveillance.

     Par défaut, la case est décochée.
5. Sous les onglets **Planification** et **Avancé**, configurez la planification du lancement de la tâche.
6. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Les règles de surveillance sont appliquées les unes après les autres conformément à leur position dans la liste des règles configurées.

Pour ajouter une zone de surveillance :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Moniteur d'accès au registre**.
3. Dans le volet résultats du nœud **Moniteur d'accès au registre**, cliquez sur le lien **Règles de surveillance de l'accès au registre**.

   La fenêtre **Surveillance de l'accès au registre** s'affiche.
4. Dans la fenêtre **Surveillance de l'accès au registre**, indiquez un chemin à l'aide d'un masque pris en charge pour **Ajouter une clé de registre à surveiller** et cliquez sur le bouton **Ajouter**.

   Évitez d'utiliser des masques pris en charge pour les clés racines lors de la création des règles.
   Si vous précisez uniquement une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, un grand nombre de notifications sur l'adressage des clés enfants indiquées est générée, ce qui entraîne des problèmes relatifs aux performances du système.
   Si vous précisez une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, et sélectionnez le mode **Bloquer les opérations selon les règles**, le système n'est pas en mesure de lire ni de modifier les clés nécessaires au fonctionnement du système d'exploitation et il ne répond pas.
5. Sous l'onglet **Actions** pour la zone de surveillance sélectionné, configurez la liste des actions selon le cas.
6. Si vous souhaitez surveiller certaines **Valeurs de registre**, procédez comme suit :

   a. Sous l'onglet **Valeurs de registre**, cliquez sur le bouton **Ajouter**.

   b. Dans la fenêtre **Règle de valeur de registre**, saisissez le **Opérations contrôlées** et configurez les **Opérations contrôlées** requises.

   c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
7. Si vous voulez définir les **Utilisateurs de confiance**, procédez comme suit :

   a. Sous l'onglet **Utilisateurs de confiance**, cliquez sur le bouton **Ajouter**.

   b. Dans la fenêtre **Sélection d'utilisateurs ou de groupes**, sélectionnez les utilisateurs ou les groupes d'utilisateurs autorisés à effectuer les actions définies.

   c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

   Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.
8. Cliquez sur **Enregistrer** dans la fenêtre **Zone de surveillance de l'accès au registre**.

Les paramètres définis pour la règle sont appliqués à la zone de surveillance définie de la tâche **Moniteur d'accès au registre**.

Administration du Contrôle d'accès au registre via le Plug-in Web

Cette section explique comment configurer la tâche Moniteur d'accès au registre via le Plug-in Web.

Configuration de la tâche Moniteur d'accès au registre

Pour configurer la tâche Moniteur d'accès au registre via le Plug-in Web, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic du système**.
5. Cliquez sur **Configuration** dans la sous-section **Moniteur d'accès au registre**.
6. Dans la fenêtre **Moniteur d'accès au registre**, sous l'onglet **Paramètres du moniteur d'accès au registre**, configurez les paramètres suivants :
   - Dans le groupe **Mode de tâche**, sélectionnez l'option requise dans la liste :
     - Bloquer les opérations selon les règles

       Si vous sélectionnez le mode **Bloquer les opérations selon les règles**, Kaspersky Embedded Systems Security bloque les **actions** définies pour la zone de surveillance. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne bloque pas les processus définis sous **Zone de confiance**.

       Par défaut, le mode **Statistiques seulement** est appliqué.

     - Statistiques seulement

       Si le mode **Statistiques seulement** est sélectionné pour la zone de surveillance, Kaspersky Embedded Systems Security compile les statistiques pour les actions de clé de registre en fonction des règles configurées. En outre, si la case **Appliquer la zone de confiance** est cochée, Kaspersky Embedded Systems Security ne compile pas les statistiques des processus définis sous **Zone de confiance**.

       Par défaut, le mode **Statistiques seulement** est appliqué.

   - Cochez ou décochez la case Appliquer la zone de confiance, le cas échéant.

Si la case **Appliquer la zone de confiance** est cochée, les **processus de confiance** configurés dans la **zone de confiance** sont appliqués à la zone de surveillance en plus de la règle configurée.

Si la case **Appliquer la zone de confiance** est décochée, les **processus de confiance** configurés dans la **zone de confiance** ne sont pas appliqués à la zone de surveillance.

Par défaut, la case est décochée.

7. Sous l'onglet **Administration des tâches**, configurez la planification du lancement de la tâche.
8. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security applique immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations relatives à la date et à l'heure des modifications des paramètres sont consignées dans le journal d'audit système.

Configuration des règles de monitoring

Les règles de surveillance sont appliquées les unes après les autres conformément à leur position dans la liste des règles configurées.

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic du système**.
5. Cliquez sur **Configuration** dans la sous-section **Moniteur d'accès au registre**.
6. Dans la fenêtre **Moniteur d'accès au registre** qui s'ouvre, accédez à l'onglet **Paramètres du moniteur d'accès au registre**.
7. Dans la section **Règles de surveillance de l'accès au registre**, cliquez sur le bouton **Ajouter**.
8. Dans la fenêtre **Zone de surveillance de l'accès au registre**, indiquez un chemin à l'aide d'un masque pris en charge pour **Surveiller les opérations dans le registre pour la zone**.

Vous pouvez utiliser `?` et `*` comme masque lors de la saisie d'un chemin.

Si vous saisissez le chemin d'accès à une clé de registre racine, assurez-vous de définir le chemin complet sans masque, par exemple `HKEY_USERS`. Voici une liste de clés de registre racine valides :

- `HKEY_LOCAL_MACHINE`
- `HKLM`
- `HKEY_CURRENT_USER`
- `HKCU`
- `HKEY_USERS`
- `HKUS`
- `HKU`
- `HKEY_CURRENT_CONFIG`
- `HKEY_CLASSES_ROOT`
- `CRHK`

Évitez d'utiliser des masques pris en charge pour les clés racines lors de la création des règles.
Si vous précisez uniquement une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, un grand nombre de notifications sur l'adressage des clés enfants indiquées est générée, ce qui entraîne des problèmes relatifs aux performances du système.
Si vous précisez une clé racine, comme HKEY_CURRENT_USER, ou une clé racine avec un masque pour toutes les clés enfants, comme HKEY_CURRENT_USER*, et sélectionnez le mode **Bloquer les opérations selon les règles**, le système n'est pas en mesure de lire ni de modifier les clés nécessaires au fonctionnement du système d'exploitation et il ne répond pas.

9. Sous l'onglet **Actions** pour la zone de surveillance sélectionné, configurez la liste des actions selon le cas.
10. Si vous souhaitez surveiller certaines **Valeurs de registre**, procédez comme suit :
    a. Sous l'onglet **Valeurs de registre**, cliquez sur le bouton **Ajouter**.
    b. Dans la fenêtre **Règle de valeur de registre**, saisissez le **Masque de valeur** et configurez la **Liste des opérations** requise.
    c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.
11. Si vous voulez définir les **Utilisateurs de confiance**, procédez comme suit :
    a. Sous l'onglet **Utilisateurs de confiance**, cliquez sur le bouton **Ajouter**.
    b. Saisissez le **Nom d'utilisateur** ou cliquez sur **Définir SID Tout le monde** pour définir les utilisateurs autorisés à effectuer les actions sélectionnées.

c. Cliquez sur le bouton **OK** afin d'enregistrer les modifications.

Kaspersky Embedded Systems Security considère par défaut tous les utilisateurs qui ne figurent pas dans la liste des utilisateurs de confiance comme des utilisateurs douteux et génère pour ceux-ci des événements de niveau Critique. Pour les utilisateurs de confiance, les statistiques sont compilées.

12. Cliquez sur **OK** dans la fenêtre **Zone de surveillance de l'accès au registre** pour enregistrer les modifications.

    Les paramètres définis pour la règle sont appliqués à la zone de surveillance définie de la tâche **Moniteur d'accès au registre**.

Inspection des journaux

Cette section contient des informations sur la tâche Inspection des journaux et la configuration de ses paramètres.

A propos de la tâche Inspection des journaux

Au cours de l'exécution de la tâche Inspection des journaux, Kaspersky Embedded Systems Security contrôle l'intégrité de l'environnement protégé d'après les résultats de l'inspection des journaux des événements Windows. L'application prévient l'administrateur en cas de détection d'un comportement anormale qui pourrait indiquer une tentative de cyberattaques.

Kaspersky Embedded Systems Security analyse les journaux des événements Windows et définit les violations conformément aux règles précisées par l'utilisateur ou par les paramètres de l'analyse heuristique que la tâche utilise pour inspecter les journaux.

Règles prédéfinie et analyse heuristique

Vous pouvez utiliser la tâche Inspection des journaux pour contrôler l'état du système protégé en appliquant les règles prédéfinies sur la base des heuristiques prédéterminées. L'analyseur heuristique identifie une activité anormale sur l'appareil protégé, ce qui peut être le signe d'une tentative d'attaque. Les modèles de définition d'une activité anormale sont repris dans les règles disponibles dans les paramètres de règles prédéfinies.

La liste des règles de la tâche Inspection des journaux répertorie sept règles. Vous pouvez activer et désactiver n'importe quelle règle. Vous ne pouvez pas supprimer des règles existantes ou en créer de nouvelles.

Vous pouvez configurer les critères de déclenchement des règles qui contrôlent les événements pour les opérations suivantes :

- Détection des attaques brute-force contre les mots de passe
- Traitement de la connexion au réseau

Dans les paramètres de la tâche, vous pouvez configurer également les exclusions. L'analyseur heuristique ne fonctionne pas si l'accès au système est exécuté par un utilisateur de confiance ou via une adresse IP de confiance.

Kaspersky Embedded Systems Security n'applique pas l'heuristique à l'inspection des journaux Windows si l'analyseur heuristique n'est pas utilisé par la tâche. Par défaut, l'analyseur heuristique est activé.

Lors de l'application des règles, l'application consigne un événement avec le niveau d'importance *Critique* dans le journal d'exécution de la tâche Inspection des journaux.

Règles personnalisées de la tâche Inspection des journaux

A l'aide des paramètres des règles, vous pouvez préciser et modifier les critères de déclenchement de la règle en cas de détection des événements choisis dans le journal Windows indiqué. Par défaut, la liste des règles d'inspection des journaux contient quatre règles. Vous pouvez activer et désactiver ces règles, supprimer les règles et en modifier les paramètres.

Vous pouvez configurer les critères suivants de déclenchement de chaque règle :

- Liste des identificateurs des enregistrements dans le journal des événements Windows.

  La règle se déclenche à l'apparition d'un nouvel enregistrement dans le journal des événements Windows, si les propriétés de l'événement incluent un identificateur d'événement indiqué dans la règle. Vous pouvez ajouter et supprimer aussi des identificateurs pour chaque règle précisée.

- Source des événements.

  Pour chaque règle, vous pouvez préciser un journal dans le journal des événements Windows. L'application exécutera la recherche des enregistrements avec les identificateurs d'événements indiqués seulement dans ce journal. Vous pouvez sélectionner un des journaux standard (Application, Sécurité ou Système) ou définir un journal personnalisé en saisissant le nom dans le champ de sélection de la source.

  L'application ne contrôle pas la présence réelle du journal indiqué dans le journal des événements Windows.

Quand la règle est déclenchée, Kaspersky Embedded Systems Security enregistre un événement Critique dans le journal d'exécution de la tâche d'inspection des journaux.

Par défaut, la tâche Inspection des journaux ne prend pas en charge les règles personnalisées.

Avant de démarrer la tâche Inspection des journaux, assurez-vous que la stratégie d'audit système est correctement configurée. Consultez l'article de Microsoft pour plus de détails.

Paramètres de la tâche Inspection des journaux par défaut

La tâche Inspection des journaux possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Paramètres de la tâche Inspection des journaux par défaut

Paramètre	Valeur par défaut	Description
Inspecter les journaux selon les règles personnalisées	Pas appliqué.	Vous pouvez activer, désactiver, ajouter ou modifier des règles personnalisées.
Inspecter les journaux selon les règles prédéfinies	Appliquée.	Vous pouvez activer ou désactiver l'analyse heuristique qui détecte l'activité anormale sur l'appareil protégé.
Détection des attaques brute-force	10 échecs de connexion toutes les 300 secondes.	Vous pouvez définir le nombre de tentatives et l'intervalle utilisé qui vont servir de critères de déclenchement de l'analyse heuristique.
Connexion au réseau	00:00:00	Vous pouvez indiquer le début et la fin de l'intervalle de temps pendant lequel Kaspersky Embedded Systems Security traite les tentatives d'ouverture de session comme une activité anormale.
Exclusions	Pas appliqué.	Vous pouvez spécifier les utilisateurs et les adresses IP qui ne déclencheront pas l'analyse heuristique.

Planification du lancement de la tâche	Le premier lancement n'est pas défini.	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Administration des règles d'inspection des journaux via le plug-in d'administration

Cette section explique comment ajouter des règles d'inspection des journaux et les configurer via le plug-in d'administration.

Configuration des règles prédéfinies d'une tâche

Pour configurer les règles prédéfinies de la tâche Inspection des journaux, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

     En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.
4. Dans la section **Diagnostic du système**, cliquez sur le bouton **Configuration** de la sous-section **Inspection des journaux**.

   La fenêtre **Inspection des journaux** s'ouvre.
5. Sélectionnez l'onglet **Règles prédéfinies**.
6. Cochez ou décochez la case **Inspecter les journaux selon les règles prédéfinies**.

   Pour que la tâche fonctionne, il faut sélectionner au moins une règle d'inspection des journaux.
7. Sélectionnez les règles que vous souhaitez appliquer dans la liste des règles prédéfinies :
   - Tentative d'attaque brute-force dans le système.
   - Des signes d'abus potentiel du journal des événements Windows ont été détectés.
   - Des actions suspectes émanant d'un nouveau service installé ont été détectées.

- Une authentification suspecte avec des identifiants explicites a été détectée.
- Le système affiche les signes d'une éventuelle attaque Kerberos forged PAC (MS14-068).
- Des actions suspectes contre un groupe Administrateurs privilégié intégré ont été détectées.
- Une activité suspecte a été détectée lors d'une session de connexion au réseau.

8. Pour configurer les règles sélectionnées, cliquez sur le bouton **Paramètres avancés**.
   La fenêtre **Inspection des journaux** s'ouvre.
9. Dans la section **Détection des attaques brute-force**, définissez le nombre de tentatives et la plage temporelle que l'analyse heuristique va utiliser comme déclencheurs.
10. Dans la section **Détection de la connexion au réseau**, définissez le début et la fin de l'intervalle de temps pendant lequel Kaspersky Embedded Systems Security considère les tentatives de connexion comme une activité anormale.
11. Sélectionnez l'onglet **Exclusions**.
12. Pour ajouter des utilisateurs considérés comme des utilisateurs de confiance, procédez comme suit :
    a. Cliquez sur le bouton **Parcourir**.
    b. Choisissez l'utilisateur.
    c. Cliquez sur le bouton **OK**.
       L'utilisateur sélectionné est ajouté à la liste des utilisateurs de confiance.
13. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :
    a. Saisissez l'adresse IP.
    b. Cliquez sur **Ajouter**.
14. L'adresse IP indiquée est ajoutée à la liste des adresses IP de confiance.
15. Sous l'onglet **Administration des tâches**, configurez la planification du lancement de la tâche.
16. Dans la fenêtre **Inspection des journaux**, cliquez sur le bouton **OK**.

Les paramètres de la tâche Inspection des journaux sont enregistrés.

Ajout de règles d'inspection des journaux via le plug-in d'administration

Pour ajouter et configurer une nouvelle règle d'inspection des journaux définie par l'utilisateur, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

- Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
- Pour configurer l'application pour un seul appareil protégé, sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.

  En cas d'application d'une stratégie active de Kaspersky Security Center à un appareil qui interdit la modification des paramètres de l'application, il est impossible d'éditer ces paramètres dans la fenêtre **Paramètres de l'application**.

4. Dans la section **Diagnostic du système**, cliquez sur le bouton **Configuration** de la sous-section **Inspection des journaux**.

   La fenêtre **Inspection des journaux** s'ouvre.

5. Sous l'onglet **Règles personnalisées**, décochez ou cochez la case Inspecter les journaux selon les règles personnalisées.

   Vous pouvez contrôler l'application des règles prédéfinies à l'inspection des journaux. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

6. Pour créer une nouvelle règle définie par l'utilisateur, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle d'inspection des journaux personnalisée** s'ouvre.

7. Dans la section **Général**, saisissez les informations suivantes au sujet de la nouvelle règle :

   - **Nom de la règle**
   - **L'apparition de nouveaux enregistrements dans le journal des événements Windows déclenche l'application de la règle si l'identifiant indiqué figure dans les paramètres de l'événement**

8. Dans la section **Critère de déclenchement**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

   a. Saisissez un identifiant.

   b. Cliquez sur **Ajouter**.

      L'identifiant de l'événement saisi est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

9. Cliquez sur le bouton **OK**.

   La règle d'inspection des journaux est ajoutée à la liste des règles.

Administration des règles d'inspection des journaux via la Console de l'application

Cette section explique comment ajouter des règles d'inspection des journaux et les configurer via la Console de l'application.

Configuration des règles prédéfinies d'une tâche

Pour configurer les paramètres de fonctionnement de l'analyse heuristique pour la tâche Inspection des journaux, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Inspection des journaux**.
3. Dans le volet résultats du nœud **Inspection des journaux**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sélectionnez l'onglet **Règles prédéfinies**.
5. Cochez ou décochez la case **Inspecter les journaux selon les règles prédéfinies**.

   Pour que la tâche fonctionne, il faut sélectionner au moins une règle d'inspection des journaux.
6. Sélectionnez les règles que vous souhaitez appliquer dans la liste des règles prédéfinies :
   - Tentative d'attaque brute-force dans le système.
   - Des signes d'abus potentiel du journal des événements Windows ont été détectés.
   - Des actions suspectes émanant d'un nouveau service installé ont été détectées.
   - Une authentification suspecte avec des identifiants explicites a été détectée.
   - Le système affiche les signes d'une éventuelle attaque Kerberos forged PAC (MS14-068).
   - Des actions suspectes contre un groupe Administrateurs privilégié intégré ont été détectées.
   - Une activité suspecte a été détectée lors d'une session de connexion au réseau.
7. Pour configurer les règles sélectionnées, accédez à l'onglet **Étendue**.
8. Dans la section **Détection des attaques brute-force**, définissez le nombre de tentatives et la plage temporelle que l'analyse heuristique va utiliser comme déclencheurs.
9. Dans la section **Connexion au réseau**, définissez le début et la fin de l'intervalle de temps pendant lequel Kaspersky Embedded Systems Security considère une tentative d'ouverture de session comme une activité anormale.
10. Sélectionnez l'onglet **Exclusions**.
11. Pour ajouter des utilisateurs considérés comme des utilisateurs de confiance, procédez comme suit :
    a. Cliquez sur le bouton **Parcourir**.
    b. Choisissez l'utilisateur.
    c. Cliquez sur le bouton **OK**.

L'utilisateur sélectionné est ajouté à la liste des utilisateurs de confiance.

12. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :

    a. Saisissez l'adresse IP.

    b. Cliquez sur **Ajouter**.

    L'adresse IP indiquée est ajoutée à la liste des adresses IP de confiance.

13. Sous les onglets **Planification** et **Avancé**, configurez les paramètres de planification du lancement de la tâche.

14. Dans la fenêtre **Paramètres de la tâche**, cliquez sur le bouton **OK**.

    Les paramètres de la tâche Inspection des journaux sont enregistrés.

Ajout de règles d'inspection des journaux via la Console de l'application

Pour ajouter et configurer une nouvelle règle d'inspection des journaux définie par l'utilisateur :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.
2. Choisissez le nœud enfant **Inspection des journaux**.
3. Dans le volet résultats du nœud **Inspection des journaux**, cliquez sur le lien **Règles d'inspection des journaux**.
4. La fenêtre **Règles d'inspection des journaux** s'ouvre.
5. Sélectionnez ou désélectionnez l'option **Inspecter les journaux selon les règles définies par l'utilisateur. Les règles configurées ne sont pas appliqués tant que la case n'est pas cochée**.

   Vous pouvez contrôler l'application des règles prédéfinies à la tâche d'inspection des journaux. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

6. Pour créer une règle définie par l'utilisateur :

   a. Saisissez le nom de la nouvelle règle.

   b. Cliquez sur **Ajouter**.

   La règle créée est ajoutée à la liste générale des règles.

7. Pour configurer une règle :

   a. Sélectionnez une règle dans la liste.

   Dans la partie droite de la fenêtre, les informations générales relatives à la règle s'affiche sous l'onglet **Description**.

   La description de la nouvelle règle est vide.

   b. Sélectionnez l'onglet **Description de la règle**.

8. Dans la section **Général**, saisissez les informations suivantes au sujet de la nouvelle règle :

   - **Nom de la règle**
   - **Nom du journal**
   - **L'apparition de nouveaux enregistrements dans le journal des événements Windows déclenche l'application de la règle si l'identifiant indiqué figure dans les paramètres de l'événement**

9. Dans la section **Identificateurs des événements**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

   a. Saisissez un identifiant d'événement.

   b. Cliquez sur **Ajouter**.

   L'identifiant de l'événement saisi est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

10. Cliquez sur le bouton **Enregistrer**.

    Les paramètres configurés des règles d'inspection des journaux sont appliqués.

Administration des règles d'inspection des journaux via le Plug-in Web

Pour ajouter et configurer des règles d'inspection des journaux via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic du système**.
5. Dans la fenêtre **Inspection des journaux**, cliquez sur le bouton **Configuration**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la tâche Inspection des journaux

Paramètre	Description
Inspecter les journaux selon les règles personnalisées	Vous pouvez activer, désactiver, ajouter ou modifier des règles personnalisées. Le paramètre est disponible dans le tableau avec la liste des règles personnalisées.
Inspecter les journaux selon les règles prédéfinies	Vous pouvez activer ou désactiver l'analyse heuristique qui détecte l'activité anormale sur l'appareil protégé. Le paramètre est disponible dans le tableau avec la liste des règles personnalisées.
Détecter une attaque brute-force si un mot de passe incorrect est saisi à une fréquence définie	Vous pouvez définir le nombre de tentatives et l'intervalle utilisé qui vont servir de critères de déclenchement de l'analyse heuristique.

Détecter une connexion réseau si la connexion a lieu au bout d'un laps de temps défini	Vous pouvez indiquer le début et la fin de l'intervalle de temps pendant lequel Kaspersky Embedded Systems Security traite les tentatives d'ouverture de session comme une activité anormale.
Définir les exclusions	Vous pouvez spécifier les utilisateurs qui ne déclencheront pas l'analyse heuristique.
Adresse IP exclues	Vous pouvez spécifier les adresses IP qui ne déclencheront pas l'analyse heuristique.
Administration des tâches	Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande et explique la configuration des paramètres de ces tâches ainsi que la configuration des paramètres de la sécurité de l'appareil protégé.

A propos des tâches d'analyse à la demande

Kaspersky Embedded Systems Security recherche des virus et autres menaces informatique dans la zone indiquée. Kaspersky Embedded Systems Security analyse les fichiers, la mémoire vive de l'appareil protégé et les objets de démarrage.

Kaspersky Embedded Systems Security propose les tâches Analyse à la demande suivantes :

- La tâche Analyse au démarrage du système d'exploitation est exécutée à chaque démarrage de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security analyse les secteurs principaux de démarrage et les zones d'amorce des disques durs et des disques amovibles, la mémoire système et la mémoire du processus. Chaque fois que Kaspersky Embedded Systems Security exécute la tâche, il crée une copie des secteurs d'amorce non infectés. Même s'il détecte une menace dans ces secteurs, il les remplace au prochain démarrage par une copie de sauvegarde.

  La tâche Analyse au démarrage du système d'exploitation est créée automatiquement après l'installation. Par défaut, le mode Informer uniquement est appliqué. Dans ce cas, après avoir déployé Kaspersky Embedded Systems Security sur les périphériques, vous pouvez activer la tâche Analyse au démarrage du système d'exploitation si aucun problème avec les services système n'a été détecté lors de l'analyse. Si l'application détecte des services système critiques comme des objets infectés ou probablement infectés, le mode Informer uniquement vous donne le temps d'en découvrir la raison et de résoudre le problème. Si l'application applique l'action Exécuter l'action recommandée qui invoque l'action Désinfecter. Supprimer si la désinfection est impossible, la désinfection ou la suppression des fichiers système peut entraîner des problèmes critiques au démarrage du système d'exploitation.

  > La tâche Analyse au démarrage du système d'exploitation peut ne pas être effectuée si un appareil protégé se réveille après le mode veille ou veille prolongée. La tâche est effectuée uniquement au redémarrage de l'appareil protégé ou au démarrage après un arrêt complet.

- La tâche Analyse rapide est exécutée par défaut chaque semaine selon une planification. Kaspersky Embedded Systems Security analyse les objets situés dans les zones critiques du système d'exploitation : objets de démarrage, secteurs et zones d'amorce des disques durs et des disques amovibles, mémoire système et mémoire du processus. L'application analyse les fichiers qui se trouvent dans les répertoires système, par exemple dans le dossier %windir%\system32. Kaspersky Embedded Systems Security applique les paramètres de sécurité qui correspondent au niveau Recommandé. Vous pouvez modifier les paramètres la tâche Analyse rapide.

- La tâche Analyse de la quarantaine est exécutée par défaut selon la planification après chaque mise à jour des bases de l'application. Vous ne pouvez pas modifier la zone de la tâche Analyse de la quarantaine.

- La tâche Vérification de l'intégrité de l'application est exécutée tous les jours. Elle permet de vérifier si les modules de Kaspersky Embedded Systems Security ont été endommagés ou modifiés. Le dossier d'installation de l'application est analysé. Les statistiques de l'exécution de la tâche indique le nombre de modules analysés et le nombre de modules endommagés. Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. Les paramètres de la planification du lancement de la tâche peuvent être modifiés.

Vous pouvez également créer des tâches d'analyse à la demande définie par l'utilisateur, par exemple, une tâche pour l'analyse des dossiers partagés sur l'appareil protégé.

Kaspersky Embedded Systems Security peut exécuter simultanément plusieurs tâches d'analyse à la demande.

A propos de la zone d'analyse de la tâche et des paramètres de sécurité

Dans la console de l'application, la zone d'analyse de la tâche d'analyse à la demande sélectionnée se présente sous la forme d'une arborescence ou d'une liste ressources de fichiers du périphérique protégé que Kaspersky Embedded Systems Security peut contrôler. Par défaut les ressources de fichier réseau de l'appareil protégé s'affichent sous la forme d'une liste.

Seul l'affichage sous forme de liste est disponible dans le plug-in d'administration.

Pour activer l'affichage des ressources de fichier réseau sous la forme d'une arborescence dans la Console de l'application,

dans la liste déroulante du coin supérieur gauche de la fenêtre **Configuration de la zone d'analyse**, choisissez l'option **Afficher sous forme d'arborescence**.

Les éléments ou les nœuds sont présentés dans une liste ou dans une arborescence des ressources de fichiers de l'appareil protégé de la manière suivante :

☑ Nœud repris dans la zone d'analyse.

☐ Nœud exclu de la zone d'analyse.

☑ Au moins un des nœuds enfants intégrés de nœud est exclu de la zone d'analyse ou les paramètres de sécurité de ces nœuds enfant diffèrent des paramètres de sécurité d'un nœud parent (uniquement pour un mode d'affichage en arborescence).

L'icône ☑ s'affiche si tous les nœuds enfants ont été sélectionnés, mais pas le nœud parent. Le cas échéant, les modifications du contenu des fichiers et dossiers du nœud parent ne sont pas automatiquement prises en compte lors de la constitution de la zone d'analyse du nœud enfant sélectionnée.

La Console de l'application permet également d'ajouter des disques virtuels à la zone d'analyse. Le nom des entrées virtuelles apparaît en bleu.

Paramètres de sécurité

Dans la tâche à la demande sélectionnée, vous pouvez modifier les valeurs des paramètres de sécurité par défaut de la même manière pour toute la zone de protection ou d'analyse ou avec des variations pour différentes entrées ou éléments dans l'arborescence ou la liste des ressources de fichiers de l'appareil.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Vous pouvez configurer les paramètres de la zone d'analyse ou de la zone de protection sélectionnée de l'une des manières suivantes :

- Sélectionner un des trois niveaux de sécurité prédéfinis (**Performance maximale**, **Recommandé** ou **Protection maximale**) ;

- Modifier manuellement les paramètres de sécurité pour les entrées sélectionnées de l'arborescence des ressources fichier de l'appareil protégé (le niveau de sécurité prend alors la valeur **Personnalisé**).

Vous pouvez enregistrer la sélection de paramètres du nœud dans un modèle afin de l'appliquer à d'autres nœuds.

Zones d'analyse prédéfinies

L'arborescence ou la liste des ressources fichier du périphérique protégé s'affiche dans le panneau de détails de l'entrée de la tâche d'analyse à la demande sélectionnée dans la fenêtre **Configuration de la zone d'analyse**.

L'arborescence ou la liste des ressources fichiers affiche les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security propose les zones d'analyse prédéfinies suivantes :

- **Poste de travail**. Kaspersky Embedded Systems Security analyse l'ensemble du périphérique protégé.
- **Disques durs locaux**. Kaspersky Embedded Systems Security analyse les objets des disques durs d'un périphérique protégé. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.
- **Disques amovibles**. Kaspersky Embedded Systems Security analyse les fichiers sur les périphériques externes tels que les lecteurs de disques compacts ou les disques amovibles. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Réseau**. Vous pouvez ajouter à la zone d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux dossiers réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte système.

  Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier de l'appareil protégé. Pour inclure les objets d'un disque réseau dans la zone d'analyse, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

- **Mémoire système**. Kaspersky Embedded Systems Security analyse les fichiers exécutables et les modules des processus exécutés dans le système d'exploitation au moment de l'analyse.
- **Objets de démarrage**. Kaspersky Embedded Systems Security analyse les objets auxquels les clés du registre et les fichiers de configuration font référence, par exemple WIN.INI ou SYSTEM.INI, ainsi que les modules de l'application qui sont lancés automatiquement au démarrage de l'appareil protégé.
- **Dossiers partagés**. Vous pouvez ajouter les dossiers partagés de l'appareil protégé à la zone d'analyse.
- **Disques virtuels**. Vous pouvez inclure dans la zone d'analyse les disques, les dossiers et les fichiers virtuels connectés à l'appareil protégé, par exemple les disques partagés d'un cluster.

  Les disques virtuels créés à l'aide de la commande SUBST ne figurent pas dans l'arborescence des ressources fichier de l'appareil protégé dans la console de l'application. Pour analyser les objets d'un disque virtuel, il faut inclure dans la zone d'analyse le répertoire de l'appareil protégé associé au disque virtuel.

Les zones d'analyse prédéfinies s'affichent par défaut dans l'arborescence des ressources de fichiers réseau et acceptent l'ajout à la liste des ressources de fichiers réseau au moment de sa création dans les paramètres de la zone d'analyse.

Par défaut, les tâches d'analyse à la demande sont exécutées dans les secteurs suivants :

- Tâche Analyse au démarrage du système d'exploitation :
  - **Disques durs locaux**
  - **Disques amovibles**
  - **Mémoire système**
- Analyse rapide :
  - **Disques durs locaux** (sauf dossier Windows)
  - **Disques amovibles**
  - **Mémoire système**
  - **Objets de démarrage**
- Autres tâches :
  - **Disques durs locaux** (sauf dossier Windows)
  - **Disques amovibles**
  - **Mémoire système**
  - **Objets de démarrage**
  - **Dossiers partagés**

Analyse des fichiers dans le stockage en ligne

A propos des fichiers cloud

Kaspersky Embedded Systems Security peut interagir avec les fichiers sur le cloud Microsoft OneDrive. L'application prend en charge la nouvelle fonction OneDrive Files On-Demand.

Kaspersky Embedded Systems Security ne prend pas en charge d'autres stockages en ligne.

OneDrive Files On-Demand permet d'accéder à tous les fichiers de OneDrive sans avoir à les télécharger tous et à utiliser de l'espace de stockage sur votre appareil. Vous pouvez télécharger des fichiers sur votre disque dur lorsque vous en avez besoin.

Lorsque la fonction OneDrive Files On-Demand est activée, des icônes d'état apparaissent en regard de chaque fichier dans la colonne **État** de l'Explorateur de fichiers. Chaque fichier peut prendre un des états suivants :

Cette icône d'état indique que le fichier est *uniquement disponible en ligne*. Les fichiers uniquement disponibles en ligne ne sont pas stockés sur le disque dur. Vous ne pouvez pas les ouvrir lorsque votre périphérique n'est pas connecté à Internet.

Cette icône d'état indique qu'un fichier est *disponible en local*. Ce cas se produit lorsque vous ouvrez un fichier uniquement disponible en ligne et qu'il se télécharge sur votre appareil. Vous pouvez ouvrir un fichier disponible en local à tout moment même sans accès Internet. Pour gagner de l'espace, vous pouvez redéfinir l'état du fichier sur uniquement en ligne.

Cette icône d'état indique qu'un fichier est *stocké sur le disque dur et toujours disponible*.

Analyse des fichiers de stockage dans le cloud

Kaspersky Embedded Systems Security analyse uniquement les fichiers du cloud lorsqu'ils sont stockés localement sur un périphérique protégé. Ces fichiers OneDrive ont les états et . Les fichiers sont ignorés pendant l'analyse car ils ne sont pas physiquement situés sur l'appareil protégé.

Kaspersky Embedded Systems Security ne télécharge pas automatiquement les fichiers du Cloud lors de l'analyse, même s'ils figurent dan la zone d'analyse.

Les fichiers du Cloud sont traités par plusieurs tâches de Kaspersky Embedded Systems Security dans différents scénario en fonction du type de tâche :

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone de protection de la tâche Protection des fichiers en temps réel. Un fichier est analysé quand l'utilisateur y accède. Si l'utilisateur accède à un fichier , celui-ci est téléchargé, devient disponible en local et a désormais l'état . Cela permet à la tâche Protection des fichiers en temps réel de traiter le fichier :

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone d'analyse de la tâche Analyse à la demande. La tâche analyse les fichiers avec les états et . Si des fichiers sont trouvés dans la zone, ils seront ignorés pendant l'analyse et un événement d'information sera enregistré dans le journal d'exécution de la tâche. Il indiquera que le fichier analysé n'est qu'une marque de réservation pour un fichier cloud et n'existe pas sur un disque local.

- Création de règles de contrôle des applications et utilisation : vous pouvez créer des règles d'autorisation et d'interdiction pour les fichiers et à l'aide de la tâche Génération des règles du Contrôle du lancement des applications. La tâche Contrôle du lancement des applications applique le principe Interdire par défaut et des règles créées pour traiter et interdire les fichiers cloud.

  La tâche Contrôle du lancement des applications bloque le lancement de tous les fichiers dans le Cloud, peu importe leur état. Les fichiers ne sont pas inclus dans la zone de génération de règles par l'application car ils ne sont pas physiquement stockés sur votre disque dur. Vu que les règles d'autorisation ne peuvent être créées pour ces fichiers. Par conséquent, ils sont soumis au principe Interdiction par défaut.

Lorsqu'une menace est détectée sur un fichier cloud OneDrive, l'application exécute l'action spécifiée dans les paramètres de la tâche effectuant l'analyse. Ainsi, le fichier peut être supprimé, désinfecté, placé en quarantaine ou sauvegardé.

Les modifications apportées aux fichiers locaux sont synchronisées avec les copies stockées sur OneDrive conformément aux principes exposés dans la documentation Microsoft OneDrive correspondante.

A propos des niveaux de sécurité prédéfinis

Les paramètres de sécurité **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique** et **Vérifier la signature Microsoft des fichiers** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si vous modifiez la valeur des paramètres **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique** ou **Vérifier la signature Microsoft des fichiers**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

Pour un nœud sélectionné dans l'arborescence des ressources de fichiers du périphérique, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** ou **Protection maximale**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité prédéfinie (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si votre réseau a adopté des mesures de sécurité pour le périphérique protégé additionnelles comme des pare-feu ou des stratégies de sécurité existantes, en plus de l'installation de Kaspersky Embedded Systems Security sur les périphériques protégés et les postes de travail.

Recommandé

Le niveau de sécurité **Recommandé** offre le meilleur équilibre entre la protection et l'impact sur les performances des appareils protégés. Les experts de Kaspersky recommandent ce niveau pour protéger les périphériques sur la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité élevé pour les périphériques.

Niveaux de sécurité prédéfinis et valeurs des paramètres correspondants

Options	Niveau de sécurité		
	Performance maximale	**Recommandé**	**Protection maximale**
Analyser les objets	En fonction du format	Tous les objets	Tous les objets
Analyser uniquement les nouveaux fichiers et les fichiers modifiés	Activée	Désactivée	Désactivée
Actions à exécuter sur les objets infectés et autres	Désinfecter. Supprimer si la désinfection est impossible	Exécuter l'action recommandée (Désinfecter. Supprimer si la désinfection est impossible	Désinfecter. Supprimer si la désinfection est impossible
Actions à exécuter sur les objets probablement infectés	Quarantaine	Exécuter l'action recommandée (quarantaine)	Quarantaine

Exclure les fichiers	non	non	non
Ne pas détecter	non	non	non
Arrêter si l'analyse dure plus de (s.)	60 s	non	non
Ne pas analyser les objets composés de plus de (Mo)	8 Mo	non	non
Analyser les flux NTFS alternatifs	Oui	Oui	Oui
Analyser les secteurs d'amorçage et la partition MBR	Oui	Oui	Oui
Analyse des objets composés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* * uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* * Tous les objets	• Archives* • Archives SFX* • Bases de données d'emails* • Message de texte plat* • Objets compactés* • Objets OLE intégrés* * Tous les objets

A propos de l'analyse des disques amovibles

Vous pouvez configurer l'analyse des disques amovibles connectés via USB à l'appareil protégé.

Kaspersky Embedded Systems Security analyse le disque amovible à l'aide de la tâche Analyse à la demande. L'application crée automatiquement une tâche Analyse à la demande lors de la connexion du disque amovible et supprime cette tâche à la fin de l'analyse. La tâche créée est exécutée selon le niveau de sécurité prédéfini pour l'analyse des disques amovibles. Vous ne pouvez pas configurer les paramètres de la tâche temporaire Analyse à la demande.

Si vous avez installé Kaspersky Embedded Systems Security sans bases antivirus, l'analyse des disques amovibles n'est pas disponible.

Kaspersky Embedded Systems Security lance l'analyse des disques amovibles lorsque ces derniers sont enregistrés dans le système d'exploitation en tant que périphérique externe USB. L'application n'analyse pas le disque amovible si la tâche Contrôle des périphériques a bloqué la connexion de ce dernier. L'application ne lance pas l'analyse des périphériques mobiles MTP.

Kaspersky Embedded Systems Security autorise l'accès aux disques amovibles durant l'analyse.

Les résultats de l'analyse de chaque disque amovible peuvent être consultés dans le journal d'exécution de la tâche Analyse à la demande créée lors de la connexion du disque amovible.

Vous pouvez modifier les valeurs des paramètres du composant Analyse des périphériques amovibles (cf. tableau ci-dessous).

Paramètres d'analyse des disques amovibles

Paramètre	Valeur par défaut	Description
Analyser les disques amovibles à la connexion via USB	Case décochée	Vous pouvez activer ou désactiver l'analyse du disque amovible lors de la connexion à l'appareil protégé via USB.
Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)	8192 Mo	Vous pouvez réduire la plage de déclenchement du composant en indiquant le volume de données maximum sur le disque amovible. Kaspersky Embedded Systems Security ne lance pas l'analyse du disque amovible si le volume des données qu'il contient est supérieur à la valeur indiquée.
Analyser avec le niveau de sécurité	Protection maximale	Vous pouvez configurer les paramètres des tâches d'analyse à la demande créées en choisissant un de trois niveaux de sécurité suivants : • **Protection maximale** • **Recommandé** • **Performance maximale** L'algorithme des actions à effectuer lors de la détection d'objets infectés, probablement infectés et autres, ainsi que d'autres paramètres d'analyse pour chaque niveau de sécurité correspondent aux niveaux de sécurité préétablis dans les tâches d'analyse à la demande.

À propos de la tâche Surveillance de l'intégrité des fichiers

Pendant la tâche Surveillance de l'intégrité des fichiers, Kaspersky Embedded Systems Security n'analyse pas les fichiers, les dossiers, les raccourcis de fichiers et les fichiers cloud verrouillés.

La tâche Surveillance de l'intégrité des fichiers surveille l'intégrité des fichiers dans la zone de surveillance en comparant le hash des fichiers (hash MD5 ou SHA256) à une ligne de référence.

Lors de la première exécution de la tâche Surveillance de l'intégrité des fichiers, Kaspersky Embedded Systems Security crée une ligne de référence en calculant et en stockant le hash des fichiers dans la zone de surveillance de la tâche. Si une zone de surveillance de la tâche Surveillance de l'intégrité des fichiers a été modifiée, Kaspersky Embedded Systems Security met à jour la ligne de référence lors de la prochaine exécution de la tâche Surveillance de l'intégrité des fichiers en calculant et en stockant le hash des fichiers dans la zone de surveillance de la tâche. Si une tâche Surveillance de l'intégrité des fichiers a été supprimée, Kaspersky Embedded Systems Security supprime la ligne de référence de cette tâche Surveillance de l'intégrité des fichiers.

Vous pouvez supprimer une ligne de référence sans supprimer la tâche du Surveillance de l'intégrité des fichiers à l'aide de la ligne de commande.

La tâche Surveillance de l'intégrité des fichiers suit les modifications de fichiers suivantes dans la zone de surveillance :

- la zone de surveillance contient un fichier qui n'est pas présent dans la ligne de référence
- la zone de surveillance ne contient pas de fichier présent dans la ligne de référence
- le hash d'un fichier dans la zone de surveillance diffère du hash de ce fichier dans une ligne de référence

La tâche Surveillance de l'intégrité des fichiers ne suit pas les modifications apportées aux attributs du fichier et aux autres flux.

Si un fichier ou un dossier est inaccessible, Kaspersky Embedded Systems Security n'ajoutera pas ce fichier ou ce dossier à la ligne de référence lors de la création de la ligne de référence et créera un événement d'échec du calcul de la somme de contrôle du fichier lors de l'exécution de la tâche Surveillance de l'intégrité des fichiers.

Un fichier ou un dossier peut être inaccessible pour les raisons suivantes :

- le chemin désigné n'existe pas
- un type de fichiers désigné par le masque n'est pas présent sous le chemin désigné
- le fichier désigné est verrouillé
- le fichier désigné est vide

Activation du lancement de la tâche Analyse à la demande à partir du menu contextuel

Vous pouvez activer le lancement de la tâche Analyse à la demande pour un ou plusieurs fichiers à partir d'un menu contextuel dans l'Explorateur Microsoft Windows.

Pour activer le lancement de la tâche Analyse à la demande à partir d'un menu contextuel :

1. Créez les fichiers REG suivants :

```
Windows Registry Editor Version 5.0.0
[HKEY_CLASSES_ROOT\Directory\shell\kess\command]
@="C:\\Temp\\scan.cmd \"%1\""
[HKEY_CLASSES_ROOT\*\shell\kess\command]
@="C:\\Temp\\scan.cmd \"%1\""
[HKEY_CLASSES_ROOT\Directory\shell\kess]
@="Scan with Kaspersky Embedded Systems Security\"
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"
```

```
[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"
[HKEY_CLASSES_ROOT\*\shell\kess]
@="Scan with Kaspersky Embedded Systems Security\"
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"
[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers]
"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavshell.exe"="~ RUNASADMIN"
```

Vous devez renseigner l'emplacement actuel du dossier d'installation de Kaspersky Embedded Systems Security.

2. Créez le fichier `scan.cmd` avec le contenu suivant :

```
@echo off
set LOGNAME=%RANDOM%
"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt
echo Scanning is in progress...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt
timeout /t -1
```

Le fichier `scan.cmd` doit contenir les informations suivantes :

- L'emplacement du fichier `kavshell.exe`.
- L'emplacement du fichier temporaire contenant les résultats de l'analyse.
- Les paramètres de la commande `KAVSHELL SCAN`.
- La valeur du délai d'attente pour la fermeture de la fenêtre de la console lorsque la tâche est terminée.

3. Copiez le fichier `scan.cmd` dans le dossier spécifié dans le fichier REG `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]`.

Le dossier `C:\Temp` est utilisé dans l'exemple.

Il n'est pas nécessaire de redémarrer le système d'exploitation.

Paramètres par défaut de la tâche d'analyse à la demande

Par défaut, les tâches d'analyse à la demande possèdent les paramètres décrits dans le tableau ci-dessous. Vous pouvez configurer les tâches d'analyse à la demande locales du système et définies par l'utilisateur.

Paramètres par défaut de la tâche d'analyse à la demande

Paramètre	Valeur par défaut	Description
Zone d'analyse	S'applique aux tâches locales du système et définies par l'utilisateur : • **Analyse au démarrage du système d'exploitation** : tout l'appareil protégé, à l'exception des dossiers partagés et des objets de démarrage ; • **Analyse rapide** : tout l'appareil protégé, à l'exception des dossiers partagés et de certains fichiers du système d'exploitation ; • Tâches d'**Analyse à la demande** définie par l'utilisateur : tout l'appareil protégé.	Vous pouvez modifier la zone d'analyse. Il est impossible de configurer la zone d'analyse pour les tâches locales du système **Analyse de la quarantaine** et **Vérification de l'intégrité de l'application**. La tâche **Analyse au démarrage du système d'exploitation** est créée automatiquement après l'installation. Par défaut, le mode **Informer uniquement** est appliqué. Dans ce cas, après avoir déployé Kaspersky Embedded Systems Security sur les périphériques, vous pouvez activer la tâche **Analyse au démarrage du système d'exploitation** si aucun problème avec les services système n'a été détecté lors de l'analyse. Si l'application détecte des services système critiques infectés ou des objets probablement infectés, le mode **Informer uniquement** vous donne le temps d'en trouver la raison et de résoudre le problème. Si l'application applique le mode **Exécuter l'action recommandée**, qui évoque l'action **Désinfecter. Supprimer si la désinfection est impossible**, la désinfection ou la suppression des fichiers système peut entraîner des problèmes critiques au démarrage du système d'exploitation.
Paramètres de sécurité	Identique pour toute la zone d'analyse ; correspond au niveau de sécurité **Recommandé**.	Pour les nœuds sélectionnés dans l'arborescence ou dans la liste des ressources de fichiers de l'appareil protégé, vous pouvez exécuter les actions suivantes : • Sélectionner un autre niveau de sécurité prédéfini ; • Modifier manuellement les paramètres de sécurité. Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à un autre nœud.
Utiliser l'analyse heuristique	Les tâches Analyse rapide et Analyse au	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse. Vous ne pouvez pas configurer le niveau d'analyse pour la tâche Analyse de la quarantaine.

	démarrage du système d'exploitation, aussi que les tâches d'analyse définies par l'utilisateur, sont exécutées selon la valeur **Moyenne**. La tâche Analyse de la quarantaine est réalisée selon la valeur **Minutieuse**.	L'analyse heuristique n'est pas utilisé dans les tâches Vérification de l'intégrité de l'application et Surveillance de l'intégrité des fichiers.
Appliquer la zone de confiance	Appliqué (pas appliquée pour la tâche Analyse de la quarantaine)	Liste d'exclusions générale que vous pouvez appliquer dans les tâches sélectionnées.
Utiliser KSN pour l'analyse	Appliquée.	Vous pouvez améliorer l'efficacité de la protection de l'appareil en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Paramètres pour lancer une tâche avec des autorisations spécifiques	La tâche est lancée sous le compte système.	Vous pouvez modifier les paramètres de lancement sous des autorisations spécifiques pour toutes les tâches d'analyse à la demande système ou définies par l'utilisateur, sauf pour les tâches Analyse de la quarantaine et Vérification de l'intégrité de l'application.
Exécuter la tâche en arrière-plan (priorité basse)	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.
Planification du lancement de la tâche	S'applique aux tâches locales du système : • Analyse au démarrage du système d'exploitation : **Au lancement de l'application** ; • Analyse rapide : **Toutes les semaines** ; • Analyse de la quarantaine : **À la mise à jour des bases de l'application** ;	Vous pouvez configurer les paramètres du lancement programmé de la tâche.

	• Vérification de l'intégrité de l'application - **Tous les jours** Pas appliqué dans les tâches définies par l'utilisateur recréées.	
Enregistrement de l'exécution de l'analyse et de la mise à jour de l'état de la protection de l'appareil	L'état de la protection de l'appareil est actualisé chaque semaine après l'exécution de la tâche Analyse rapide.	Vous pouvez configurer les paramètres d'enregistrement de l'exécution de l'analyse rapide d'une des manières suivantes : • En modifiant les paramètres de la planification du lancement de la tâche Analyse rapide. • En modifiant la zone d'analyse de la tâche Analyse rapide. • En créant des tâches d'analyse à la demande définies par l'utilisateur.

Administration des tâches d'analyse à la demande via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres de la tâche pour un seul ou pour l'ensemble des appareils protégés du réseau.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Ouverture de l'assistant de tâche d'analyse à la demande

Pour commencer à créer une tâche d'analyse à la demande définie par l'utilisateur, procédez comme suit :

1. Pour créer une tâche locale :
   a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
   b. Sélectionnez le groupe d'administration auquel appartient l'appareil protégé.
   c. Dans le volet résultats, sous l'onglet **Périphériques**, ouvrez le menu contextuel du périphérique protégé.
   d. Sélectionnez l'option de menu **Propriétés**.

e. Dans la section **Tâches** de la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

La fenêtre **Assistant de nouvelle tâche** s'ouvre.

2. Pour créer une tâche de groupe :

   a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

   b. Sélectionnez le groupe d'administration pour lequel vous souhaitez créer une tâche.

   c. Ouvrez l'onglet **Tâches**.

   d. Cliquez sur le bouton **Créer une tâche**.

   La fenêtre **Assistant de nouvelle tâche** s'ouvre.

3. Pour créer une tâche pour un ensemble d'appareils protégés défini par l'utilisateur :

   a. Dans le nœud **Sélections de périphériques** de l'arborescence de la Console d'administration de Kaspersky Security Center, cliquez sur le bouton **Exécuter une sélection** pour sélectionner un périphérique.

   b. Ouvrez l'onglet **Résultats de la sélection pour "nom de la sélection"**.

   c. Dans la liste déroulante **Réaliser une sélection**, sélectionnez l'option **Créer une tâche pour un résultat de sélection**.

   La fenêtre **Assistant de nouvelle tâche** s'ouvre.

4. Sélectionnez la tâche **Analyse à la demande** dans la liste des tâches disponibles pour Kaspersky Embedded Systems Security.

5. Cliquez sur **Suivant**.

   La fenêtre **Configuration** s'ouvre.

Configurez les paramètres de la tâche en fonction des besoins.

Pour configurer une tâche Analyse à la demande existante :

Double-cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

La fenêtre **Propriétés : Analyse à la demande** s'ouvre.

Accès aux propriétés de la tâche d'analyse à la demande

Pour accéder aux propriétés de l'application pour la tâche Analyse à la demande pour un appareil protégé unique :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration auquel appartient l'appareil protégé.

3. Sélectionnez l'onglet **Périphériques**.

4. Double-cliquez sur le nom de l'appareil protégé pour lequel vous souhaitez configurer une zone d'analyse.

La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.

5. Sélectionnez la section **Tâches**.
6. Dans la liste des tâches créées pour le périphérique, sélectionnez la tâche Analyse à la demande que vous avez créée.
7. Cliquez sur le bouton **Propriétés**.
   La fenêtre **Propriétés : Analyse à la demande** s'ouvre.

Configurez les paramètres de la tâche en fonction des besoins.

Création d'une tâche d'analyse à la demande

Pour créer une tâche d'analyse à la demande définie par l'utilisateur, procédez comme suit :

1. Ouvrez la fenêtre **Configuration** dans l'Assistant Nouvelle tâche.
2. Sélectionnez le **Mode de création de la tâche** requis.
3. Cliquez sur **Suivant**.
4. Dans la fenêtre **Zone d'analyse**, définissez la zone d'analyse.

   La zone d'analyse reprend par défaut les secteurs critiques de l'appareil protégé. Les zones d'analyse sont accompagnées de l'icône ☑ dans le tableau. Les zones d'analyse exclues sont accompagnées de l'icône ☐ dans le tableau.

   Vous pouvez modifier la zone d'analyse, y inclure des zones distinctes prédéfinies, des disques, des dossiers, des objets de réseaux et des fichiers et définir les paramètres particuliers de la protection pour chaque zone ajoutée.

   - Pour exclure de l'analyse toutes les zones d'analyse critiques, ouvrez le menu contextuel de chaque ligne, puis choisissez **Supprimer une zone**.
   - Pour inclure une zone d'analyse, un disque, un dossier, un objet réseau ou un fichier prédéfini dans la zone d'analyse :
     a. Cliquez avec le bouton droit de la souris dans le tableau **Zone d'analyse** et choisissez l'option **Ajouter une zone** ou cliquez sur le bouton **Ajouter**.
     b. Dans la fenêtre **Ajouter des objets à la zone d'analyse**, sélectionnez la zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque de l'appareil protégé, le dossier, l'objet réseau ou le fichier sur l'appareil protégé ou sur un autre appareil protégé du réseau, puis cliquez sur le bouton **OK**.
   - Pour exclure des sous-dossiers ou des fichiers de l'analyse, sélectionnez le dossier (le disque) ajouté dans la fenêtre **Zone d'analyse** de l'assistant :
     a. Ouvrez le menu contextuel et sélectionnez l'option **Configurer**.
     b. Cliquez sur le bouton **Configuration** afin d'ouvrir la fenêtre **Niveau de sécurité**.

c. Sous l'onglet **Général** de la fenêtre **Paramètres de l'analyse à la demande**, décochez les cases **Sous-dossiers** et **Sous-fichiers**.

- Pour modifier les paramètres de sécurité de la zone d'analyse :

  a. Ouvrez le menu contextuel de la zone dont vous souhaitez modifier les paramètres et choisissez l'option **Configurer**.

  b. Dans la fenêtre **Paramètres de l'analyse à la demande**, sélectionnez un des niveaux de sécurité prédéfinis ou cliquez sur le bouton **Configuration** afin de configurer manuellement les paramètres de sécurité.

  Les paramètres de sécurité sont configurés de la même manière que pour la tâche Protection des fichiers en temps réel.

- Pour ignorer les objets joints dans la zone d'analyse ajoutée :

  a. Ouvrez le menu contextuel du tableau **Zone d'analyse** et sélectionnez **Ajouter une exclusion** une exclusion.

  b. Désignez les objets à exclure : sélectionnez une zone prédéfinie dans la liste **Zone prédéfinie**, désignez le disque du périphérique protégé, le dossier, l'objet réseau ou le dossier sur le périphérique protégé ou tout autre périphérique protégé du réseau.

  c. Cliquez sur le bouton **OK**.

5. Dans la section **Options**, configurez l'analyse heuristique et l'intégration aux autres modules :

   - Configurez l'utilisation de l'analyse heuristique.
   - Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure de la zone d'analyse de la tâche les objets ajoutés à la liste Zone de confiance.
   - Cochez la case **Utiliser KSN pour l'analyse** si vous souhaitez utiliser les services cloud de Kaspersky Security Network pour la tâche.
   - Pour attribuer la priorité de référence *faible* (Low) au processus de travail dans lequel la tâche va être exécutée, cochez la case **Exécuter la tâche en arrière-plan** dans la fenêtre **Options**.

     Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

   - Pour utiliser la tâche créée en tant que tâche d'analyse rapide, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide** dans la fenêtre **Options**.

6. Cliquez sur **Suivant**.

7. Dans la fenêtre **Planification**, définissez la planification du lancement de la tâche.

8. Cliquez sur **Suivant**.

9. Dans la fenêtre **Sélection du compte pour le lancement de la tâche**, désignez le compte que vous souhaitez utiliser.

10. Cliquez sur **Suivant**.

11. Définissez un nom de tâche.

12. Cliquez sur **Suivant**.

    Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants : " * < > & \ : |

    La fenêtre **Terminer la création de la tâche** s'ouvre.

13. Il est possible également de lancer la tâche à la fin de l'Assistant en cochant la case **Exécuter la tâche à la fin de l'Assistant**.

14. Cliquez sur **Terminer** pour terminer la création de la tâche.

    Une tâche Analyse à la demande est créée pour un appareil protégé ou un groupe d'appareils protégés sélectionnés.

Attribution de l'état "Analyse rapide" à une tâche d'analyse à la demande

Kaspersky Security Center attribue par défaut l'état *Avertissement* à l'appareil protégé si la tâche Analyse rapide est exécutée moins souvent que ne l'indique le paramètre du seuil de génération d'événement dans Kaspersky Embedded Systems Security *Analyse rapide non réalisée depuis longtemps*.

Pour configurer l'analyse de tous les appareils protégés appartenant à un groupe d'administration unique, procédez comme suit :

1. Créez une tâche d'analyse à la demande de groupe.

2. Dans la fenêtre **Options** de l'Assistant de création de tâches, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide**. Les paramètres que vous aurez définis (zone d'analyse et paramètres de sécurité) seront identiques pour tous les appareils protégés du groupe. Programmez l'exécution de la tâche.

   Vous pouvez cocher la case **Considérer l'exécution de la tâche comme une analyse rapide** lors de la création d'une tâche d'analyse à la demande pour un groupe d'appareils protégés ou plus tard dans la fenêtre **Propriétés : <Nom de la tâche>**.

3. À l'aide d'une nouvelle stratégie ou d'une stratégie existante, désactivez le lancement planifié des tâches locales du système Analyse à la demande sur les appareils protégés du groupe.

Dès ce moment, le Serveur d'administration de Kaspersky Security Center évalue la protection de l'appareil protégé et vous en informe sur la base de la dernière exécution de la tâche portant l'état de l'Analyse rapide et non sur la base des résultats de la tâche locale du système Analyse rapide.

Vous pouvez attribuer l'état *Tâche d'analyse rapide* à des tâches de groupe d'analyse à la demande ou à des tâches pour des groupes d'appareils protégés.

La console de l'application permet de voir si la tâche d'analyse à la demande est une tâche d'analyse rapide.

Dans la console de l'application, la case **Considérer l'exécution de la tâche comme une analyse rapide** apparaît dans la propriété des tâches mais elle ne peut pas être modifiée.

Exécution d'une tâche d'analyse à la demande en arrière-plan

Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité de base *Moyenne* (Normal).

Vous pouvez attribuer la priorité *faible* (Low) au processus dans lequel la tâche d'analyse à la demande va être exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur les performances des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter plusieurs tâches en arrière-plan. Vous pouvez définir le nombre maximum de processus pour les tâches d'analyse à la demande en arrière-plan.

Pour modifier la priorité d'une tâche d'analyse à la demande existante, procédez comme suit !

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande**.
2. Cochez ou décochez la case **Exécuter la tâche en arrière-plan**.
3. Cliquez sur le bouton **OK**.

   Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Enregistrement de l'exécution d'une analyse rapide

Par défaut, l'état de la protection du périphérique apparaît dans le panneau des résultats du nœud **Kaspersky Embedded Systems Security** et il est actualisé chaque semaine après la fin de la tâche Analyse rapide.

L'heure de l'actualisation de l'état de la protection de l'appareil est liée à la planification de la tâche d'analyse à la demande où la case **Considérer l'exécution de la tâche comme une analyse rapide** a été cochée dans les paramètres. Par défaut, la case est cochée uniquement pour la tâche Analyse rapide et ne peut être modifiée pour cette tâche.

Vous pouvez sélectionner la tâche d'analyse à la demande associée à l'état de la protection de l'appareil uniquement au départ de Kaspersky Security Center.

Configuration de la zone d'analyse de la tâche

Si vous modifiez la zone d'analyse dans les tâches Analyse au démarrage du système d'exploitation et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la réparation de Kaspersky Embedded Systems Security (**Démarrer** > **Programmes** > **Kaspersky Embedded Systems Security** > **Modification ou suppression de Kaspersky Embedded Systems Security**). Dans l'assistant de configuration, sélectionnez **Réparation des composants installés**, puis cliquez sur **Suivant**. Cochez ensuite la case **Rétablir les paramètres recommandés de l'application**.

Pour configurer une zone d'analyse pour une tâche d'analyse à la demande existante :

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande**.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Pour inclure des éléments dans la zone d'analyse, procédez comme suit :
   a. Ouvrez le menu contextuel dans l'espace vide de la liste de zone d'analyse.
   b. Sélectionnez l'option **Ajouter une zone** dans le menu contextuel.
   c. Dans la fenêtre **Ajouter des objets à la zone d'analyse** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter à la zone d'analyse :
      - **Zone prédéfinie**, si vous voulez ajouter une des zones prédéfinies sur un appareil protégé. Puis, dans la liste déroulante, choisissez la zone d'analyse souhaitée.
      - **Disque, dossier ou objet réseau**, si vous voulez ajouter à la zone d'analyse un disque, un dossier ou un objet réseau distinct. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.
      - **Fichier**, si vous voulez insérer dans la zone d'analyse uniquement un fichier distinct. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.

   Vous ne pouvez pas ajouter un objet à une zone d'analyse s'il est déjà ajouté en tant qu'exclusion d'une zone d'analyse.
4. Pour exclure certaines entrées de la zone d'analyse, décochez les cases en regard des noms de ces entrées ou réalisez les opérations suivantes :
   a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.
   b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.
   c. Dans la fenêtre **Ajouter une exclusion**, choisissez un type d'objet que vous voulez ajouter à titre d'exclusion de la zone d'analyse en suivant la procédure utilisée pour ajouter un objet à la zone d'analyse.
5. Pour modifier la zone d'analyse ou une exclusion ajoutée, dans le menu contextuel de la zone d'analyse correspondante, choisissez l'option **Modifier la zone**.
6. Pour masquer une zone d'analyse ou une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Supprimer une zone**.

   La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.
7. Cliquez sur le bouton **OK**.

La fenêtre Configuration de la zone d'analyse s'ouvre. Les paramètres de la tâche définis seront enregistrés.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour un nœud sélectionné dans la liste des ressources de fichiers du périphérique protégé, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**.

Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande**.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Dans la liste de l'appareil protégé, sélectionnez un élément repris dans la zone d'analyse afin de définir un niveau de sécurité prédéfini.
4. Cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.
5. Sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité que vous souhaitez appliquer.

   La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau de sécurité que vous avez sélectionné.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : Analyse à la demande**.

   Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à une tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Configuration manuelle des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse.

Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone d'analyse ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil protégé.

Pour configurer manuellement les paramètres de sécurité :

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande**.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Sélectionnez les éléments dans la liste de zone d'analyse pour lesquels vous souhaitez configurer les paramètres de sécurité.

Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité à un nœud ou élément sélectionné dans la zone d'analyse.

4. Cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

5. Configurez les paramètres de sécurité pour le nœud ou l'élément sélectionné en fonction de vos exigences :

   - Général
   - Actions
   - Optimisation
   - **Stockage hiérarchique**

6. Cliquez sur **OK** dans la fenêtre **Paramètres de l'analyse à la demande**.

7. Dans la fenêtre **Zone d'analyse**, cliquez sur **OK**.

Les paramètres de la nouvelle zone d'analyse sont enregistrés.

Configuration des paramètres de tâche généraux

Pour configurer les paramètres généraux de la tâche Analyse à la demande, procédez comme suit :

1. Ouvrez la fenêtre Propriétés : Analyse à la demande.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.

4. Cliquez sur le bouton **Configuration**.
5. Dans le groupe **Analyser les objets** de l'onglet **Général**, indiquez les types d'objets que vous souhaitez inclure dans la zone d'analyse :

   - **Objets à analyser** :
     - Tous les objets
     - Objets analysés en fonction du format
     - Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus
     - Objets analysés en fonction de la liste d'extensions indiquée
   - **Sous-dossiers**
   - **Sous-fichiers**

- Analyser les secteurs d'amorçage et la partition MBR
- Analyser les flux NTFS alternatifs

6. Dans le groupe **Optimisation**, cochez ou décochez la case Analyser uniquement les nouveaux fichiers et les fichiers modifiés.

   Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.

7. Dans le groupe **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

   - **Toutes les / Les nouvelles archives**
   - **Toutes les / Les nouvelles archives SFX**
   - **Toutes les / Les nouvelles bases de données d'emails**
   - **Tous les / Les nouveaux objets compactés**
   - **Tous les / Les nouveaux messages de texte brut**
   - **Tous les / Les nouveaux objets OLE incorporés**

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

La configuration de la nouvelle tâche sera enregistrée.

Configuration des actions

Pour configurer les actions sur les objets infectés et les autres objets détectés lors de la tâche Analyse à la demande, procédez comme suit :

1. Ouvrez la fenêtre **Propriétés : Analyse à la demande**.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Cliquez sur le bouton **Configurer**.
   La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.
4. Cliquez sur le bouton **Configuration**.
5. Sélectionnez l'onglet **Actions**.
6. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

   - **Informer uniquement**
   - **Désinfecter**.
   - **Désinfecter. Supprimer si la désinfection est impossible**.

- Supprimer.
- **Exécuter l'action recommandée**.

7. Sélectionnez l'action à exécuter sur les objets probablement infectés :
   - Informer uniquement.
   - **Quarantaine**.
   - Supprimer.
   - Exécuter l'action recommandée.
8. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
   a. Cochez ou décochez la case Exécuter les actions en fonction du type d'objet détecté.
   b. Cliquez sur le bouton **Configuration**.
   c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (à exécuter si la première échoue) pour chaque type d'objet détecté.
   d. Cliquez sur le bouton **OK**.
9. Choisissez l'action à exécuter sur les objets composés qui ne peuvent être désinfectés : cochez ou décochez la case Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré.
10. Cliquez sur le bouton **OK**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'optimisation

Pour configurer la performance de la tâche Analyse à la demande :

1. Ouvrez la fenêtre Propriétés : Analyse à la demande.
2. Ouvrez l'onglet **Zone d'analyse**.
3. Cliquez sur le bouton **Configurer**.
   La fenêtre **Paramètres de l'analyse à la demande** s'ouvre.
4. Cliquez sur le bouton **Configuration**.
5. Sélectionnez l'onglet **Optimisation**.
6. Dans la section **Exclusions** :
   - Cochez ou décochez la case Exclure les fichiers.
   - Cochez ou décochez la case Ne pas détecter.

- Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

7. Dans la section **Paramètres avancés** :
   - **Arrêter si l'analyse dure plus de (s.)**
   - **Ne pas analyser les objets composés de plus de (Mo)**
   - **Utiliser la technologie iSwift**
   - **Utiliser la technologie iChecker**
8. Cliquez sur le bouton **OK**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'analyse des disques amovibles

Pour configurer l'analyse des disques amovibles lorsqu'ils sont connectés à l'appareil protégé, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.

   Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Complémentaire**.
5. Cliquez sur le bouton **Configuration** dans la sous-section **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.
6. Dans la section **Analyse à la connexion**, procédez comme suit :
   - Cochez la case **Analyser les disques amovibles à la connexion via USB** si vous souhaitez que Kaspersky Embedded Systems Security lance automatiquement l'analyse des disques amovibles à la connexion.
   - Le cas échéant, cochez la case **Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.
7. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés et appliqués.

Configuration de la tâche Surveillance de l'intégrité des fichiers

Pour configurer la tâche de groupe du Surveillance de l'intégrité des fichiers :

1. Dans l'arborescence de la Console d'administration Kaspersky Security Center, développez le nœud **Périphériques administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.

4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

   Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Pour en savoir plus sur la configuration des paramètres dans cette section, consultez le *Système d'aide de Kaspersky Security Center*.

5. Dans la section **Zone d'analyse**, procédez comme suit :

   a. Pour inclure un dossier dans la zone de la tâche Surveillance de l'intégrité des fichiers :

      1. Cliquez sur **Ajouter**.

         La fenêtre **Propriétés de la zone d'analyse** s'ouvre.

      2. Cochez ou décochez la case **Analyser cette zone**.

      3. Cliquez sur le bouton **Parcourir** pour désigner le dossier que vous souhaitez inclure dans la portée de la tâche Contrôle de l'intégrité des fichiers.

      4. Cochez la case **Analyser aussi les sous-dossiers** si vous souhaitez inclure tous les sous-dossiers dans la zone de la tâche Surveillance de l'intégrité des fichiers.

   b. Pour inclure ou exclure le dossier précédemment ajouté à la zone de la tâche Surveillance de l'intégrité des fichiers, cochez ou décochez la case à gauche du chemin d'accès au dossier dans le tableau **Zone d'analyse**.

   c. Pour supprimer le dossier précédemment ajouté à la zone de la tâche Surveillance de l'intégrité des fichiers, sélectionnez ce dossier dans le tableau **Zone d'analyse** et cliquez sur le bouton **Supprimer**.

6. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour des bases de l'application).

7. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

8. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le *Système d'aide de Kaspersky Security Center*.

9. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.
   Les paramètres de la tâche de groupe définis seront enregistrés.

Administration des tâches d'analyse à la demande via Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'une tâche sur un appareil protégé.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la tâche d'analyse à la demande

Pour ouvrir les paramètres généraux de la tâche Analyse à la demande via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche que vous souhaitez configurer.
3. Dans le volet résultats du nœud enfant, cliquez sur le lien **Propriétés**.
   La fenêtre **Paramètres de la tâche** s'ouvre.

Accès aux paramètres de la zone d'application de la tâche d'analyse à la demande

Pour ouvrir la fenêtre des paramètres de la zone d'analyse via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.
3. Dans le volet résultats du nœud sélectionné, cliquez sur le lien **Configurer la zone d'analyse**.
   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

Création et configuration d'une tâche d'analyse à la demande

Vous pouvez créer des tâches définies par l'utilisateur pour un seul appareil protégé dans le nœud **Analyse à la demande**. Il est impossible de créer les tâches définies par l'utilisateur dans les autres composants fonctionnels de Kaspersky Embedded Systems Security.

Pour créer et configurer une tâche d'analyse à la demande :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Analyse à la demande**.
2. Choisissez l'option **Ajouter une tâche**.

   La fenêtre **Ajouter une tâche** s'ouvre.
3. Configurez les paramètres de la tâche suivants :

   - **Nom** : un nom de tâche contenant un maximum de 100 caractères. Il peut contenir n'importe quel caractère, sauf **" * < > & \ : |**.

     Vous ne pouvez pas enregistrer une nouvelle tâche ou passer à la configuration des paramètres de la nouvelle tâche sous les onglets **Planification**, **Avancé** et **Exécuter en tant que** si le nom de la tâche n'est pas défini.

   - **Description** : toute information complémentaires à propos de la tâche. Pas plus de 2 000 caractères. Ces informations figurent dans la fenêtre des propriétés de la tâche.
   - **Utiliser l'analyse heuristique**.
   - **Exécuter la tâche en arrière-plan**.
   - **Appliquer la zone de confiance**.
   - **Considérer l'exécution de la tâche comme une analyse rapide**.
   - **Utiliser KSN pour l'analyse**.
4. Configurez les paramètres de planification du lancement de la tâche sous les onglets **Planification** et **Avancé**.
5. Sous l'onglet **Exécuter en tant que**, vous pouvez configurer le lancement de la tâche sous les autorisations d'un compte utilisateur spécifique.
6. Dans la fenêtre **Ajouter une tâche**, cliquez sur le bouton **OK**.

   La tâche d'analyse à la demande définie par l'utilisateur a été créée. Un nœud portant le nom de la nouvelle tâche apparaît dans l'arborescence de la console de l'application. L'opération est enregistrée dans le journal d'audit système.
7. Sélectionnez **Configurer la zone d'analyse** dans le volet résultats du nœud sélectionné.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
8. Dans l'arborescence des ressources de fichier de l'appareil protégé ou dans la liste, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.
9. Sélectionnez un des niveaux de sécurité prédéfinis ou configurer les paramètres d'analyse manuellement.
10. Cliquez sur **Enregistrer** dans la fenêtre **Configuration de la zone d'analyse**.

Les paramètres configurés seront appliqués lors de la prochaine exécution de la tâche.

Zone d'analyse dans les tâches d'analyse à la demande

Cette section fournit des informations sur la création et l'utilisation d'une zone d'analyse dans les tâches d'analyse à la demande.

Configuration de l'affichage des ressources de fichier réseau

Pour sélectionner le mode d'affichage des ressources de fichier réseau lors de la configuration des paramètres de la zone d'analyse, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez l'une des options suivantes :
   - Choisissez le point **Afficher sous forme d'arborescence** si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une arborescence.
   - Choisissez le point **Afficher sous forme de liste**, si vous voulez que les ressources de fichier réseau s'affichent sous la forme d'une liste.

   Par défaut les ressources de fichier réseau de l'appareil protégé s'affichent sous la forme d'une liste.
3. Cliquez sur le bouton **Enregistrer**.

Constitution d'une zone d'analyse

Si vous administrez Kaspersky Embedded Systems Security sur le périphérique protégé à distance via la Console de l'application installée sur le poste de travail de l'administrateur, vous devez faire partie du groupe des administrateurs sur l'ordinateur protégé pour consulter les dossiers du périphérique.

Les noms des paramètres peuvent varier selon les versions des systèmes d'exploitation Windows.

Si vous modifiez la zone d'analyse dans les tâches Analyse au démarrage du système d'exploitation et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la réparation de Kaspersky Embedded Systems Security (**Démarrer** > **Programmes** > **Kaspersky Embedded Systems Security** > **Modification ou suppression de Kaspersky Embedded Systems Security**). Dans l'assistant de configuration, sélectionnez **Réparation des composants installés**, puis cliquez sur **Suivant**. Cochez ensuite la case **Rétablir les paramètres recommandés de l'application**.

La procédure de constitution d'une zone d'analyse dans les tâches d'analyse à la demande dépend de l'affichage sélection des ressources de fichier réseau. Vous pouvez configurer l'affichage des ressources de fichier réseau en tant qu'arborescence ou que liste (affichage par défaut).

Pour créer une zone d'analyse à l'aide de l'arborescence des ressources de fichier réseau, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.

2. Dans la section gauche de la fenêtre, déployez l'arborescence des ressources de fichier réseau pour afficher tous les nœuds et les nœuds enfants.

3. Exécutez les actions suivantes :

   - Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.

   - Pour inclure certaines entrées dans la zone d'analyse, décochez la case **Poste de travail** et procédez comme suit :

     - Si vous souhaitez inclure dans la zone d'analyse tous les disques d'un type particulier, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur l'appareil protégé, cochez la case **Disques amovibles**).

     - Si vous souhaitez inclure un disque d'un type particulier dans la zone d'analyse, développez le nœud qui contient les disques de ce type et cochez la case en regard du nom du disque requis. Par exemple, pour sélectionner le disque amovible **F:**, développez le nœud **Disques amovibles** et cochez la case en regard du **F:**.

     - Si vous souhaitez inclure dans la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case en regard de ce dossier ou de ce fichier.

4. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone d'analyse** se ferme. Les paramètres de la tâche définis seront enregistrés.

Pour créer une zone d'analyse à l'aide de la liste des ressources de fichier réseau, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.

2. Pour inclure certaines entrées dans la zone d'analyse, décochez la case **Poste de travail** et procédez comme suit :

   a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.

   b. Dans le menu contextuel, choisissez l'option **Ajout d'une zone d'analyse**.

   c. Dans la fenêtre **Ajout d'une zone d'analyse** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter :

      - **Zone prédéfinie**, si vous voulez ajouter une des zones prédéfinies sur un appareil protégé. Puis, dans la liste déroulante, choisissez la zone d'analyse souhaitée.

      - **Disque, dossier ou objet réseau**, si vous voulez ajouter à la zone d'analyse un disque, un dossier ou un objet réseau distinct. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.

      - **Fichier**, si vous voulez insérer dans la zone d'analyse uniquement un fichier distinct. Puis choisissez la zone souhaitée en cliquant sur le bouton **Parcourir**.

   Vous ne pouvez pas ajouter un objet à une zone d'analyse s'il est déjà ajouté en tant qu'exclusion d'une zone d'analyse.

3. Pour exclure certaines entrées de la zone d'analyse, décochez les cases en regard des noms de ces entrées ou réalisez les opérations suivantes :

a. Ouvrez le menu contextuel de la zone d'analyse d'un clic-droit de la souris.

b. Dans le menu contextuel, choisissez le point **Ajouter une exclusion**.

c. Dans la fenêtre **Ajouter une exclusion**, choisissez un type d'objet que vous voulez ajouter à titre d'exclusion de la zone d'analyse en suivant la procédure utilisée pour ajouter un objet à la zone d'analyse.

4. Pour modifier la zone d'analyse ou une exclusion ajoutée, dans le menu contextuel de la zone d'analyse nécessaire, choisissez l'option **Modifier la zone**.

5. Pour masquer la zone d'analyse ou une exclusion ajoutée au préalable à la liste des ressources de fichier réseau, dans le menu contextuel de la zone d'analyse correspondante, choisissez l'option **Supprimer de la liste**.

La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone d'analyse** se ferme. Les paramètres de la tâche définis seront enregistrés.

Inclusion des objets réseau dans la zone d'analyse

Vous pouvez inclure dans la zone d'analyse des disques réseau, des répertoires ou des fichiers en indiquant leur chemin d'accès de réseau au format UNC (Universal Naming Convention).

Vous ne pouvez pas analyser les dossiers réseau en cas d'utilisation du compte système.

Pour ajouter un emplacement réseau à la zone d'analyse, procédez comme suit :

1. Ouvrez la fenêtre Configuration de la zone d'analyse.

2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Afficher sous forme d'arborescence**.

3. Dans le menu contextuel du nœud **Réseau** :

   - Choisissez l'option **Ajouter un dossier de réseau** si vous souhaitez ajouter un dossier réseau à la zone d'analyse.

   - Choisissez l'option **Ajouter un fichier de réseau** si vous souhaitez ajouter un fichier réseau à la zone d'analyse.

4. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et appuyez sur la touche **ENTER**.

5. Cochez la case en regard du nom de l'objet réseau ajouté afin de l'inclure dans la zone d'analyse.

6. Le cas échéant, modifiez les paramètres de sécurité de l'objet réseau ajouté.

7. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Création d'une zone d'analyse virtuelle

Vous pouvez insérer dans la zone d'analyse des disques, des dossiers et des fichiers virtuels ou créer une zone d'analyse virtuelle.

Vous pouvez étendre la zone d'analyse en ajoutant des disques virtuels, des dossiers ou des fichiers distincts, uniquement si la zone de d'analyse s'affiche sous la forme d'une arborescence de ressources de fichiers.

Pour ajouter un disque virtuel à la zone d'analyse, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Afficher sous forme d'arborescence**.
3. Dans l'arborescence des ressources de fichier de l'appareil protégé, ouvrez le menu contextuel du nœud **Disques virtuels**, cliquez sur **Ajouter un disque virtuel**, puis sélectionnez le nom du disque virtuel dans la liste des noms disponibles.
4. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone d'analyse.
5. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Pour ajouter un dossier ou un fichier virtuel à la zone d'analyse, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Ouvrez la liste déroulante dans le coin supérieur gauche de la fenêtre, puis sélectionnez **Afficher sous forme d'arborescence**.
3. Dans l'arborescence des ressources fichiers de l'appareil protégé, ouvrez le menu contextuel du nœud auquel vous souhaitez ajouter le répertoire ou le fichier et sélectionnez l'une des options suivantes :
   - **Ajouter un dossier virtuel**, si vous souhaitez ajouter un dossier virtuel à la zone d'analyse.
   - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone d'analyse.
4. Dans le champ, saisissez le nom du dossier ou du fichier.
5. Dans la ligne contenant le nom du dossier ou du fichier, cochez la case afin de l'inclure dans la zone d'analyse.
6. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Configuration des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse.

Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone d'analyse ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil protégé.

Lorsque vous utilisez l'arborescence des ressources de fichier réseau, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds enfants. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Pour configurer manuellement les paramètres de sécurité :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Dans la section gauche de la fenêtre, sélectionnez le nœud ou l'élément dont vous souhaitez configurer les paramètres de sécurité.

   Il est possible d'appliquer un modèle prédéfini contenant les paramètres de sécurité à un nœud ou élément sélectionné dans la zone d'analyse.

   Dans la section gauche de la fenêtre, vous pouvez sélectionner la vue des ressources de fichier réseau , créer une zone d'analyse ou créer une zone d'analyse virtuelle.
3. Dans la partie droite de la fenêtre, exécutez l'une des actions suivantes :
   - Sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité que vous souhaitez appliquer.
   - Sous les onglets suivants, configurez les paramètres de sécurité requis pour le nœud ou l'élément sélectionné en fonction de vos exigences :
     - **Général**
     - **Actions**
     - **Optimisation**
     - **Stockage hiérarchique**
4. Cliquez sur **Enregistrer** dans la fenêtre **Configuration de la zone d'analyse**.

Les paramètres de la nouvelle zone d'analyse sont enregistrés.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour le nœud sélectionné dans l'arborescence ou la liste des ressources de fichiers du périphérique protégé, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**.

Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Dans l'arborescence ou la liste des ressources de fichier réseau de l'appareil protégé, sélectionnez le nœud ou l'objet pour lequel vous souhaitez définir le niveau de sécurité.
3. Assurez-vous que le nœud ou l'élément sélectionné se trouve dans la zone d'analyse.
4. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez le niveau de sécurité à appliquer.

   La fenêtre reprend la liste des paramètres de sécurité correspondant au niveau de sécurité sélectionné.
5. Cliquez sur le bouton **Enregistrer**.

   Les paramètres de la tâche sont enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les paramètres modifiés sont appliqués au prochain lancement de la tâche.

Configuration des paramètres de tâche généraux

Pour configurer les paramètres de sécurité générale d'une tâche d'analyse à la demande :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Sélectionnez l'onglet **Général**.
3. Dans le groupe **Analyser les objets**, indiquez les types d'objets que vous souhaitez inclure dans la zone d'analyse :
   - **Objets à analyser** :
     - **Tous les objets**
     - **Objets analysés en fonction du format**
     - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**
     - **Objets analysés en fonction de la liste d'extensions indiquée**
   - **Analyser les secteurs d'amorçage et la partition MBR**
   - **Analyser les flux NTFS alternatifs**
4. Dans le groupe **Optimisation**, cochez ou décochez la case Analyser uniquement les nouveaux fichiers et les fichiers modifiés.

   > Pour passer d'une option à une autre lorsque la case est cochée, cliquez sur le lien **Tous/Nouveaux uniquement** de chacun des types d'objets composés.
5. Dans le groupe **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
   - **Toutes les / Les nouvelles archives**
   - **Toutes les / Les nouvelles archives SFX**

- **Toutes les** / **Les nouvelles bases de données d'emails**
- **Tous les** / **Les nouveaux objets compactés**
- **Tous les** / **Les nouveaux messages de texte brut**
- **Tous les** / **Les nouveaux objets OLE incorporés**

6. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration des actions

Pour configurer les actions sur les objets infectés et les autres objets détectés pour la tâche Analyse à la demande :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Sélectionnez l'onglet **Actions**.
3. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
   - **Informer uniquement**.
   - **Désinfecter**.
   - **Désinfecter. Supprimer si la désinfection est impossible**.
   - **Supprimer**.
   - **Exécuter l'action recommandée**.
4. Sélectionnez l'action à exécuter sur les objets probablement infectés :
   - **Informer uniquement**.
   - **Quarantaine**.
   - **Supprimer**.
   - **Exécuter l'action recommandée**.
5. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
   a. Cochez ou décochez la case **Exécuter les actions en fonction du type d'objet détecté**.
   b. Cliquez sur le bouton **Configuration**.
   c. Dans la fenêtre qui s'ouvre, choisissez une action principale et une action secondaire (à exécuter si la première échoue) pour chaque type d'objet détecté.
   d. Cliquez sur le bouton **OK**.

6. Choisissez l'action à exécuter sur les objets composés qui ne peuvent être désinfectés : cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**.

7. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration de l'optimisation

Pour configurer la performance de la tâche Analyse à la demande :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Sélectionnez l'onglet **Optimisation**.
3. Dans la section **Exclusions** :
   - Cochez ou décochez la case **Exclure les fichiers**.
   - Cochez ou décochez la case **Ne pas détecter**.
   - Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.
4. Dans la section **Paramètres avancés** :
   - **Arrêter si l'analyse dure plus de (s.)**
   - **Ne pas analyser les objets composés de plus de (Mo)**
   - **Utiliser la technologie iSwift**
   - **Utiliser la technologie iChecker**
5. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Configuration du stockage hiérarchique

Pour configurer les actions réalisées sur les objets infectés et les autres objets détectés pour la tâche Analyse à la demande :

1. Ouvrez la fenêtre **Configuration de la zone d'analyse**.
2. Sélectionnez l'onglet **Stockage hiérarchique**.
3. Sélectionnez l'action à exécuter sur les fichiers :
   - **Ne pas analyser**.
   - **Analyser seulement la partie résidente du fichier**.

- **Analyser le fichier en entier**.

  Si cette action est sélectionnée, vous pouvez spécifier les options suivantes :

  - Cochez ou décochez la case **Uniquement si le fichier a été sollicité durant la période indiquée (jours)**, et désignez le nombre de jours.
  - Cochez ou décochez la case **Ne pas copier le fichier sur le disque dur local si possible**.

4. Cliquez sur **Enregistrer**.

La configuration de la nouvelle tâche sera enregistrée.

Analyse des disques amovibles

Pour configurer l'analyse des disques amovibles dans la Console de l'application lorsqu'ils sont connectés à l'appareil protégé, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security** et sélectionnez l'option **Configurer l'analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.

2. Dans la section **Analyse à la connexion**, procédez comme suit :

   - Cochez la case **Analyser les disques amovibles à la connexion via USB** si vous souhaitez que Kaspersky Embedded Systems Security lance automatiquement l'analyse des disques amovibles à la connexion.
   - Le cas échéant, cochez la case **Analyser les disques amovibles si leurs volume de données stockées ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.

3. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés et appliqués.

Statistiques des tâches d'analyse à la demande

Pendant l'exécution de la tâche d'analyse à la demande, vous pouvez consulter des informations détaillées sur le nombre que Kaspersky Embedded Systems Security a traité depuis son lancement.

Ces informations seront accessibles même si vous arrêtez la tâche. Les statistiques de la tâche figurent dans le journal d'exécution de la tâche.

Pour consulter les statistiques d'une tâche d'analyse à la demande :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.

Le volet résultats du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Les informations relatives aux objets que Kaspersky Embedded Systems Security a traités depuis son lancement sont reprises dans le tableau ci-dessous.

Statistiques des tâches d'analyse à la demande

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Embedded Systems Security. Par exemple, si Kaspersky Embedded Systems Security a découvert une objet malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	Nombre d'objets que Kaspersky Embedded Systems Security a détectés et classés comme infectés ou nombre de fichiers de logiciels légitimes trouvés qui n'ont pas été exclus de la zone d'analyse et qui ont été considérés comme des logiciels légitimes que des intrus peuvent utiliser pour endommager votre périphérique ou vos données personnelles.
Objets probablement infectés détectés	Nombre d'objets détectés par Kaspersky Embedded Systems Security et considérés comme probablement infectés.
Objets non désinfectés	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu désinfecter pour les raisons suivantes : • L'objet détecté appartient à un type d'objet qui ne peut être désinfecté. • une erreur s'est produite lors de la désinfection.
Objets non placés en quarantaine	Nombre d'objets que Kaspersky Embedded Systems Security a tenté en vain de mettre en quarantaine, par exemple à cause d'un manque d'espace sur le disque.
Objets non supprimés	Nombre d'objets que Kaspersky Embedded Systems Security a tenté de supprimer sans y parvenir car, par exemple, l'accès à l'objet est bloqué par une autre application.
Objets non analysés	Nombre d'objets de la zone de protection que Kaspersky Embedded Systems Security n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
Objets non sauvegardés	Nombre d'objets pour lesquels Kaspersky Embedded Systems Security a tenté en vain de placer une copie dans la sauvegarde, par exemple à cause d'un manque d'espace sur le disque.
Erreurs de traitement	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
Objets désinfectés	Nombre d'objets désinfectés par Kaspersky Embedded Systems Security.
Objets placés en quarantaine	Nombre d'objets placés en quarantaine par Kaspersky Embedded Systems Security.
Objets sauvegardés	Nombre d'objets dont une copie a été placée dans la Sauvegarde par Kaspersky Embedded Systems Security.
Objets supprimés	Nombre d'objets supprimés par Kaspersky Embedded Systems Security.
Objets protégés par mot de passe	Nombre d'objets (archives, par exemple) que Kaspersky Embedded Systems Security a ignorés en raison d'une protection par mot de passe.
Objets endommagés	Nombre d'objets que Kaspersky Embedded Systems Security a ignorés à cause de leur format endommagé.

Objets traités	Nombre d'objets traités par Kaspersky Embedded Systems Security.

Vous pouvez aussi consulter les statistiques des tâches d'analyse à la demande dans le journal d'exécution de la tâche sélectionnée via le lien **Ouvrir le journal d'exécution de la tâche** dans la section **Administration** du volet résultats.

Nous recommandons le traitement manuel des événements enregistrés sous l'onglet **Événements** du journal d'exécution de la tâche à la fin de la tâche.

Création et configuration d'une tâche Surveillance de l'intégrité des fichiers

Pour créer ou configurer une nouvelle tâche de Surveillance de l'intégrité des fichiers :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Diagnostic du système**.
2. Sélectionnez **Créer une tâche Surveillance de l'intégrité des fichiers**.
   La fenêtre **Ajouter une tâche** s'ouvre.
3. Dans la liste déroulante **Algorithme de calcul de hash**, sélectionnez une des options :
   - **MD5**
   - **SHA256**
4. Dans le tableau **Zones d'analyse**, procédez comme suit:
   a. Pour ajouter un fichier ou un dossier à la zone portée de la tâche Surveillance de l'intégrité des fichiers :
      1. Cliquez sur **Ajouter**.
         La fenêtre des **Propriétés de la zone d'analyse** s'ouvre.
      2. Cochez ou décochez la case **Analyser cette zone**.
      3. Cliquez sur le bouton **Parcourir** pour désigner le fichier ou le dossier que vous souhaitez inclure dans la zone de la tâche Contrôle de l'intégrité des fichiers.
      4. Cochez la case **Analyser aussi les sous-dossiers** si vous souhaitez inclure tous les sous-dossiers dans la zone de la tâche Surveillance de l'intégrité des fichiers.
      5. Cliquez sur le bouton **OK**.
   b. Pour modifier un fichier ou un dossier précédemment ajouté à la zone de la tâche Surveillance de l'intégrité des fichiers :
      1. Cliquez sur le bouton **Modifier**.
         La fenêtre des **Propriétés de la zone d'analyse** s'ouvre.
      2. Cochez ou décochez la case **Analyser cette zone**.
      3. Cliquez sur le bouton **Parcourir** pour désigner le fichier ou le dossier que vous souhaitez inclure dans la zone de la tâche Contrôle de l'intégrité des fichiers.

4. Cochez ou décochez la case **Analyser aussi les sous-dossiers**, si vous souhaitez inclure ou exclure tous les sous-dossiers de la zone de la tâche Surveillance de l'intégrité des fichiers.

5. Cliquez sur le bouton **OK**.

c. Pour supprimer le fichier ou le dossier précédemment ajouté à la zone de la tâche Surveillance de l'intégrité des fichiers, sélectionnez ce fichier ou dossier dans le tableau **Zones d'analyse** et cliquez sur le bouton **Supprimer**.

5. Configurez les paramètres de planification du lancement de la tâche sous les onglets **Planification** et **Avancé**.

6. Sous l'onglet **Exécuter en tant que**, vous pouvez configurer le lancement de la tâche sous les autorisations d'un compte utilisateur spécifique.

7. Dans la fenêtre **Ajouter une tâche**, cliquez sur le bouton **OK**.

   Une nouvelle tâche Surveillance de l'intégrité des fichiers personnalisée est créée. Un nœud portant le nom de la nouvelle tâche apparaît dans l'arborescence de la console de l'application. L'opération est enregistrée dans le journal d'audit système.

Pour ouvrir les paramètres de la tâche Surveillance de l'intégrité des fichiers :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Diagnostic du système**.

2. Sélectionnez le nœud enfant qui correspond à la tâche que vous souhaitez configurer.

3. Dans le volet résultats du nœud enfant, cliquez sur le lien **Propriétés**.

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

Administration des tâches Analyse à la demande via le Plug-in Web

Cette section présente la navigation dans l'interface du Plug-in Web pour un seul ou pour l'ensemble des périphériques protégés du réseau.

Ouverture de l'assistant de tâche d'analyse à la demande

Pour commencer à créer une tâche Analyse à la demande locale :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique** → **Périphériques administrés**.

2. Cliquez sur l'onglet **Groupes** pour sélectionner le groupe d'administration auquel appartient l'appareil protégé.

3. Cliquez sur le nom de l'appareil protégé.

4. Dans la fenêtre **<nom du périphérique>** qui s'ouvre, sélectionnez l'onglet **Tâches**.

5. Cliquez sur **Ajouter**.

   La fenêtre **Assistant d'ajout d'une tâche** s'ouvre.

6. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.

7. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**.

8. Cliquez sur **Suivant**.

Configurez les paramètres de la tâche en fonction des besoins.

Pour commencer à créer une tâche de groupe Analyse à la demande :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Tâches**.
2. Cliquez sur l'onglet **Groupes** pour sélectionner le groupe d'administration pour lequel vous souhaitez créer une tâche.
3. Cliquez sur **Ajouter**.

   La fenêtre **Assistant d'ajout d'une tâche** s'ouvre.
4. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.
5. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**.
6. Cliquez sur **Suivant**.

Configurez les paramètres de la tâche en fonction des besoins.

Pour commencer à créer une tâche Analyse à la demande pour un groupe personnalisé :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique** → **Sélections de périphériques**.
2. Sélectionnez la sélection pour laquelle vous souhaitez créer une tâche.
3. Cliquez sur **Démarrer**.
4. Dans la fenêtre **Résultats de la sélection**, sélectionnez les périphériques pour lesquels vous souhaitez créer une tâche.
5. Cliquez sur **Nouvelle tâche**.
6. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.
7. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**.
8. Cliquez sur **Suivant**.

Configurez les paramètres de la tâche en fonction des besoins.

Pour configurer une tâche Analyse à la demande existante :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphériques** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

La fenêtre **<Nom de la tâche>** s'ouvre.

Accès aux propriétés de la tâche d'analyse à la demande

Pour accéder aux propriétés de l'application pour la tâche Analyse à la demande pour un appareil protégé unique :

1. Dans la fenêtre principale de Web Console, sélectionnez **Périphérique** → **Périphériques administrés**.
2. Cliquez sur l'onglet **Groupes** pour sélectionner le groupe d'administration auquel appartient l'appareil protégé.
3. Cliquez sur le nom de l'appareil protégé.
4. Dans la fenêtre **<nom du périphérique>** qui s'ouvre, sélectionnez l'onglet **Tâches**.
5. Dans la liste des tâches créées pour le périphérique, sélectionnez la tâche Analyse à la demande que vous avez créée.
6. Ouvrez l'onglet **Paramètres de l'application**.

Configuration de la zone d'analyse de la tâche

Pour configurer une zone d'analyse pour une tâche d'analyse à la demande existante :

1. Ouvrez les propriétés de la tâche d'analyse à la demande.
2. Sélectionnez la section **Zone d'analyse**.
3. Réalisez une des opérations suivantes :
   - Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle.
   - Sélectionnez une règle existante et cliquez sur le bouton **Modifier**.

   La fenêtre **Modifier la zone** s'ouvre.
4. Basculez le bouton bascule sur **Actif** et sélectionnez un type d'objet.
5. Configurez les paramètres suivants dans la section **Protection des objets** :
   - **Mode de protection d'objets** :
     - **Tous les objets**
     - **Objets analysés en fonction du format**
     - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**
     - **Objets analysés en fonction de la liste d'extensions indiquée**
   - **Sous-dossiers**
   - **Sous-fichiers**
   - **Analyser les secteurs d'amorçage et la partition MBR**
   - **Analyser les flux NTFS alternatifs**

- Protection uniquement des nouveaux fichiers et des fichiers modifiés

6. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

   - **Archives**
   - **Archives SFX**
   - **Objets compactés**
   - **Bases de données d'emails**
   - **Email en texte brut**
   - **Objets OLE intégrés**

7. Dans la section **Actions à exécuter sur les objets infectés et autres**, sélectionnez l'action à réaliser sur les objets infectés ou autres détectés :

   - **Informer uniquement**.
   - **Désinfecter**.
   - **Désinfecter. Supprimer si la désinfection est impossible**.
   - **Supprimer**.
   - **Recommandé**.

8. Dans la section **Actions à exécuter sur les objets probablement infectés**, sélectionnez l'action à exécuter sur les objets probablement infectés :

   - **Informer uniquement**.
   - **Quarantaine**.
   - **Supprimer**.
   - **Recommandé**.

9. Dans la section **Actions à exécuter sur les objets probablement infectés**, cochez ou décochez la case **Supprimer complètement le fichier composé que l'application ne peut modifier en cas de détection d'un objet intégré**.

10. Configurez les paramètres suivants dans la section **Exclusions** :

    - Cochez ou décochez la case **Exclure les fichiers**.
    - Cochez ou décochez la case **Ne pas détecter**.

11. Dans la section **Paramètres avancés**, définissez les valeurs suivantes :

    - **Arrêter si l'analyse dure plus de (s.)**
    - **Ne pas analyser les objets composés de plus de (Mo)**

- **Utiliser la technologie iSwift**
- **Utiliser la technologie iChecker**

12. Dans la section **Actions sur les fichiers autonomes**, sélectionnez l'action à effectuer sur les fichiers :

    - **Ne pas analyser**.
    - **Analyser seulement la partie résidente du fichier**.
    - **Analyser le fichier en entier**.

      Si cette action est sélectionnée, vous pouvez spécifier les options suivantes :

      - Cochez ou décochez la case **Uniquement si le fichier a été sollicité durant la période indiquée (jours)**, et désignez le nombre de jours.
      - Cochez ou décochez la case **Ne pas copier le fichier sur le disque dur local si possible**.

13. Cliquez sur le bouton **OK**.

Configuration des paramètres de la tâche

Pour configurer les paramètres d'une tâche Analyse à la demande existante :

1. Ouvrez les propriétés de la tâche d'analyse à la demande.
2. Sélectionnez la section **Options**.
3. Cochez ou décochez la case **Utiliser l'analyse heuristique**.
4. Si nécessaire, sélectionnez le niveau d'analyse à l'aide de la liste déroulante **Niveau de l'analyse heuristique**.
5. Configurez les paramètres suivants dans la section **Intégration aux autres composants** :

    - Cochez la case **Appliquer la zone de confiance** si vous souhaitez exclure de la zone d'analyse de la tâche les objets ajoutés à la liste Zone de confiance.
    - Cochez la case **Utiliser KSN pour l'analyse** si vous souhaitez utiliser les services cloud de Kaspersky Security Network pour la tâche.
    - Pour attribuer la priorité *faible* (Low) au processus de travail dans lequel la tâche va être exécutée, cochez la case **Exécuter la tâche en arrière-plan**.

      Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

    - Pour utiliser la tâche créée en tant que tâche d'analyse rapide, cochez la case **Considérer l'exécution de la tâche comme une analyse rapide**.

Zone de confiance

Cette section contient des informations sur la zone de confiance dans Kaspersky Embedded Systems Security, ainsi que des instructions pour ajouter des objets à la zone de confiance lors de l'exécution des tâches.

A propos de la zone de confiance

La zone de confiance est une liste d'exclusions de la zone de protection ou d'analyse que vous pouvez créer et appliquer aux tâches d'analyse à la demande et des protection des fichiers en temps réel créées, aux tâches d'analyse à la demande définies par l'utilisateur et à toutes les tâches d'analyse à la demande système, sauf la tâche d'analyse de la quarantaine.

Par défaut, la zone de confiance est appliquée dans les tâches Protection des fichiers en temps réel et Analyse à la demande.

Vous pouvez exporter la liste des règles de composition de la zone de confiance dans un fichier de configuration au format XML afin de pouvoir l'importer par la suite dans une version de Kaspersky Embedded Systems Security installée sur un autre périphérique protégé.

Processus de confiance

Applicable aux tâches de protection des fichiers en temps réel.

Certaines applications du périphérique protégé peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par Kaspersky Embedded Systems Security. Les contrôleurs de domaine sont un exemple d'applications appartenant à cette catégorie.

Afin de ne pas perturber la stabilité de telles applications, vous pouvez désactiver la protection des fichiers consultés par les processus exécutés de ces applications. Il faut pour cela créer une liste de processus de confiance dans la zone de confiance.

Microsoft Corporation recommande d'exclure de la Protection des fichiers en temps réel certains fichiers du système d'exploitation Microsoft Windows et les fichiers des applications de Microsoft qui ne peuvent être infectés. Les noms de certains d'entre eux sont repris sur le site Internet de Microsoft (code de l'article : KB822158).

Vous pouvez activer ou désactiver l'application des processus de confiance dans la zone de confiance.

> Si le fichier exécutable du processus change, par exemple suite à une mise à jour, Kaspersky Embedded Systems Security l'exclut de la liste des processus de confiance.

L'application n'utilise pas la valeur du chemin vers le fichier sur un appareil protégé pour faire confiance au processus. Le chemin d'accès au fichier sur l'appareil protégé est appliqué seulement pour la recherche du fichier et le calcul de sa somme de contrôle, ainsi que pour informer l'utilisateur sur la source du fichier exécutable.

Opérations de sauvegarde

Applicable aux tâches de protection en temps réel de l'ordinateur.

Lors de la sauvegarde des données des disques durs sur des périphériques externes, vous pouvez désactiver la protection des objets sollicités durant les opérations de sauvegarde. Kaspersky Embedded Systems Security n'analyse pas les objets que l'application de sauvegarde ouvre en lecture avec l'indice FILE_FLAG_BACKUP_SEMANTICS.

Exclusions

- Applicable à la protection des fichiers en temps réel.
- tous les objets détectables dans les zones désignées du périphérique protégé.
- objets détectables désignés selon le nom ou le masque de nom dans toute la zone de protection ou d'analyse.

Administration de la Zone de confiance via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration de la zone de confiance pour un seul ou pour l'ensemble des appareils protégés du réseau.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Ouverture des paramètres de la stratégie de Zone de confiance

Pour ouvrir une Zone de confiance via une stratégie de Kaspersky Security Center :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Complémentaire**.
6. Cliquez sur le bouton **Configuration** de la sous-section **Zone de confiance**.
   La fenêtre **Zone de confiance** s'ouvre.

Configurez la zone de confiance en fonction des besoins.

Si l'appareil protégé est administré par une stratégie active de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, ces paramètres ne peuvent pas être modifiés via la Console de l'application.

Ouverture de la fenêtre des propriétés de la Zone de confiance

Pour configurer la Zone de confiance dans la fenêtre des propriétés de l'application, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <Nom du périphérique>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - Sélectionnez l'option **Propriétés** dans le menu contextuel du périphérique protégé.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
5. Dans la section **Applications**, sélectionnez **Kaspersky Embedded Systems Security 3.2**.
6. Cliquez sur le bouton **Propriétés**.
   La fenêtre de configuration de l'application **Kaspersky Embedded Systems Security 3.2 s'ouvre**.
7. Sélectionnez la section **Complémentaire**.
8. Cliquez sur le bouton **Configuration** de la sous-section **Zone de confiance**.
   La fenêtre **Zone de confiance** s'ouvre.

Configurez la zone de confiance en fonction des besoins.

Configuration des paramètres de la Zone de confiance via le plug-in d'administration

La zone de confiance est appliquée par défaut à toutes les nouvelles tâches et stratégies.

Pour configurer les paramètres de la zone de confiance :

1. Spécifiez les objets que Kaspersky Embedded Systems Security doit ignorer pendant l'exécution de la tâche sous l'onglet **Exclusions**.
2. Spécifiez les processus que Kaspersky Embedded Systems Security doit ignorer pendant l'exécution de la tâche sous l'onglet **Processus de confiance**.
3. Appliquez le masque not-a-virus.

Ajout d'une exclusion

Pour ajouter une exclusion à la Zone de confiance via une stratégie de Kaspersky Security Center :

1. Ouvrez la fenêtre **Zone de confiance**.

2. Sous l'onglet **Exclusions**, indiquez les objets qui seront ignorés par Kaspersky Embedded Systems Security lors de l'analyse et de la protection :

   - Pour ajouter les exclusions recommandées, cliquez sur le bouton Ajouter les exclusions recommandées.
   - Pour importer des exclusions préconfigurées, cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration au format XML stocké sur votre appareil.

     Les exclusions du fichier XML seront ajoutées à la liste des exclusions.
   - Si vous souhaitez indiquer manuellement la condition qui, une fois satisfaite, permettra de considérer un objet comme un fichier de confiance, cliquez sur le bouton **Ajouter** et procédez aux étapes suivantes.

     La fenêtre **Exclusion** s'ouvre.

3. Si vous avez cliqué sur le bouton **Ajouter**, dans la section **L'objet n'est pas analysé si les conditions suivantes sont remplies**, spécifiez les objets à exclure de la zone de protection/zone d'analyse et les objets à exclure parmi les objets détectables :

   - Si vous souhaitez exclure un objet de la zone de protection ou d'analyse :

     a. Cochez la case Objet à analyser.

     b. Cliquez sur le bouton **Modifier**.

     La fenêtre **Sélectionnez un objet** s'ouvre.

     c. Renseignez l'objet que vous souhaitez exclure de la zone d'analyse.

     > Lors de la désignation des objets, vous pouvez utiliser des masques de noms (via les caractères ? et *) et tous les types de variables d'environnement. Les variables d'environnement (remplacement des variables par leurs valeurs) sont résolues par Kaspersky Embedded Systems Security lors du démarrage d'une tâche ou lors de l'application de nouveaux paramètres à une tâche en cours d'exécution (non applicable aux tâches d'analyse à la demande). Kaspersky Embedded Systems Security résout les variables d'environnement sous le compte utilisé pour démarrer la tâche. Pour en savoir plus sur les variables d'environnement, reportez-vous à la Base de connaissances Microsoft.

     d. Cliquez sur le bouton **OK**.

     e. Cochez la case **Appliquer aux sous-dossiers** si vous souhaitez exclure tous les fichiers et dossiers enfants de l'objet indiqué de la protection ou de la zone d'analyse.

   - Si vous spécifiez le nom d'un objet détectable :

     a. Cochez la case Objets à détecter.

     b. Cliquez sur le bouton **Modifier**.

     La fenêtre **Liste des objets à détecter** s'ouvre.

     c. Renseignez le nom ou le masque du nom de l'objet détectable en fonction de la classification de l'encyclopédie des virus.

     d. Cliquez sur **Ajouter**.

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

4. Dans la section **Zone d'application des exclusions**, cochez les cases en regard des noms des tâches auxquelles l'exclusion doit être appliquée.

5. Cliquez sur le bouton **OK**.

L'exclusion s'affiche dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

Ajout de processus de confiance

Pour ajouter un ou plusieurs processus à la liste des processus de confiance :

1. Ouvrez la fenêtre **Zone de confiance**.

2. Ouvrez l'onglet **Processus de confiance**.

3. Cochez la case Ne pas vérifier les opérations de sauvegarde de fichiers pour éviter l'analyse des opérations de lecture de fichiers.

4. Cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** pour éviter l'analyse des opérations sur les fichiers pour les processus de confiance.

5. Pour ajouter un processus à la liste des processus de confiance, réalisez une des opérations suivantes :

   - Pour importer des processus de confiance préconfigurés, cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration au format XML stocké sur votre appareil.

     Les processus du fichier XML seront ajoutés à la liste des processus de confiance.

   - Pour préciser manuellement les processus, cliquez sur le bouton **Ajouter** et passez aux étapes suivantes.

6. Si vous avez cliqué sur le bouton **Ajouter**, dans le menu contextuel du bouton, sélectionnez l'une des options suivantes :

   - **Processus multiples**.

     Configurez les paramètres suivants dans la fenêtre **Ajout de processus de confiance** qui s'ouvre :

     a. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

     b. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

     c. Cliquez sur le bouton **Parcourir** pour ajouter des données sur la base de processus exécutables.

     d. Dans la fenêtre qui s'ouvre, sélectionnez un fichier exécutable.

     > Vous pouvez ajouter un seul fichier exécutable à la fois. Répétez les étapes c-d pour ajouter d'autres fichiers exécutables.

     e. Cliquez sur le bouton **Processus** pour ajouter des données sur la base de processus en cours.

     f. Dans la fenêtre qui s'ouvre, sélectionnez des processus. Pour sélectionner plusieurs processus, maintenez la touche **CTRL** enfoncée.

     g. Cliquez sur le bouton **OK**.

Le compte utilisateur sous les privilèges duquel la tâche Protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur l'appareil où Kaspersky Embedded Systems Security est installé afin de pouvoir consulter la liste des processus actifs. Vous pouvez trier les processus dans la liste des processus actifs selon le nom du fichier, l'identificateur de processus (PID) ou le chemin d'accès au fichier exécutable du processus sur l'appareil local. Vous pouvez sélectionner des processus en cours d'exécution en cliquant sur le bouton **Processus** uniquement si vous utilisez la Console de l'application sur un périphérique protégé ou dans les paramètres de l'hôte indiqué via Kaspersky Security Center.

- **Un seul processus basé sur le nom et le chemin du fichier**.

  Dans la fenêtre **Ajout d'un processus** qui s'ouvre, procédez comme suit :

  a. Saisissez un chemin d'accès à un fichier exécutable (y compris le nom du fichier).

  Lors de la désignation des objets, vous pouvez utiliser des masques de noms (via les caractères `?` et `*`) et tous les types de variables d'environnement. Les variables d'environnement (remplacement des variables par leurs valeurs) sont résolues par Kaspersky Embedded Systems Security lors du démarrage d'une tâche ou lors de l'application de nouveaux paramètres à une tâche en cours d'exécution (non applicable aux tâches d'analyse à la demande). Kaspersky Embedded Systems Security résout les variables d'environnement sous le compte utilisé pour démarrer la tâche. Pour en savoir plus sur les variables d'environnement, reportez-vous à la Base de connaissances Microsoft.

  b. Cliquez sur le bouton **OK**.

- **Un seul processus basé sur les propriétés**.

  Configurez les paramètres suivants dans la fenêtre **Ajout d'un processus de confiance** qui s'ouvre :

  a. Cliquez sur le bouton **Parcourir** et sélectionnez un processus.

  b. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

  c. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

  d. Cliquez sur le bouton **OK**.

  Pour ajouter le processus sélectionné à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

7. Dans la fenêtre **Zone de confiance**, cliquez sur le bouton **OK**.

Le fichier ou le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

Application du masque not-a-virus

Le masque not-a-virus permet de sauter l'analyse des fichiers logiciels et des ressources internet légitimes, qui peuvent être considérés comme nuisibles. Le masque concerne les tâches suivantes :

- Protection des fichiers en temps réel.

- Analyse à la demande.

Si le masque n'est pas ajouté à la liste d'exclusions, Kaspersky Embedded Systems Security applique les actions spécifiées dans les paramètres d'exécution de la tâche pour le logiciel qui entre dans cette catégorie.

Pour appliquer le masque not-a-virus, procédez comme suit :

1. Ouvrez la fenêtre **Zone de confiance**.
2. Dans la colonne **Objets à détecter** de l'onglet **Exclusions**, faites défiler la liste et sélectionnez la ligne avec la valeur not-a-virus:* si la case est décochée.
3. Cliquez sur le bouton **OK**.

La nouvelle configuration est appliquée.

Administration de la Zone de confiance via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration de la Zone de confiance sur un appareil protégé.

Application de la Zone de confiance aux tâches dans la Console de l'application

La zone de confiance est appliquée par défaut dans les tâches de protection des fichiers en temps réel, dans les tâches définies par l'utilisateur nouvellement créées d'analyse à la demande et dans toutes les tâches système d'analyse à la demande, à l'exception de la tâche d'analyse de la quarantaine.

Dès que la zone de confiance est activée/désactivée, les exclusions définies dans celle-ci seront ou ne seront plus appliquées dans les tâches exécutées immédiatement.

Pour activer ou désactiver l'utilisation d'une Zone de confiance dans les tâches de Kaspersky Embedded Systems Security, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer l'utilisation de la zone de confiance.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Général** et réalisez une des opérations suivantes :
   - Si vous souhaitez utiliser une zone de confiance dans la tâche, cochez la case **Appliquer la zone de confiance**.
   - Si vous ne souhaitez pas utiliser une zone de confiance, décochez la case **Appliquer la zone de confiance**.
4. Pour configurer les paramètres de la Zone de confiance, cliquez sur le lien dans le nom de la case **Appliquer la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.

   Dans la fenêtre **Zone de confiance**, configurez les exclusions et les processus de confiance, puis cliquez sur **OK**.

5. Cliquez sur le bouton **OK** dans la fenêtre **Paramètres de la tâche** pour enregistrer les modifications.

Configuration des paramètres de la Zone de confiance dans la Console de l'application

Pour configurer les paramètres de la zone de confiance :

1. Spécifiez les objets que Kaspersky Embedded Systems Security doit ignorer pendant l'exécution de la tâche sous l'onglet **Exclusions**.
2. Spécifiez les processus que Kaspersky Embedded Systems Security doit ignorer pendant l'exécution de la tâche sous l'onglet **Processus de confiance**.
3. Appliquez la Zone de confiance aux tâches de l'application.
4. Appliquez le masque not-a-virus.

Ajout d'une exclusion à la zone de confiance

Pour ajouter manuellement une exclusion à la zone de confiance via la Console de l'application, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.

   La fenêtre **Zone de confiance** s'ouvre.
3. Sélectionnez l'onglet **Exclusions**.
4. Spécifiez les objets que Kaspersky Embedded Systems Security doit ignorer pendant l'analyse et la protection :

   - Pour importer des exclusions préconfigurées, cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration au format XML stocké sur votre appareil.

     Les exclusions du fichier XML seront ajoutées à la liste des exclusions.

   - Si vous souhaitez indiquer manuellement la condition qui, une fois satisfaite, permettra de considérer un objet comme un fichier de confiance, cliquez sur le bouton **Ajouter** et procédez aux étapes suivantes.

     La fenêtre **Exclusion** s'ouvre.
5. Si vous avez cliqué sur le bouton **Ajouter**, dans la section **L'objet n'est pas analysé si les conditions suivantes sont remplies**, spécifiez les objets à exclure de la zone de protection/zone d'analyse et les objets à exclure parmi les objets détectables :

   - Si vous souhaitez exclure un objet de la zone de protection ou d'analyse :

     a. Cochez la case Objet à analyser.

     b. Cliquez sur le bouton **Modifier**.

La fenêtre **Sélectionnez un objet** s'ouvre.

c. Renseignez l'objet que vous souhaitez exclure de la zone d'analyse.

> Lors de la désignation des objets, vous pouvez utiliser des masques de noms (via les caractères ? et *) et tous les types de variables d'environnement. Les variables d'environnement (remplacement des variables par leurs valeurs) sont résolues par Kaspersky Embedded Systems Security lors du démarrage d'une tâche ou lors de l'application de nouveaux paramètres à une tâche en cours d'exécution (non applicable aux tâches d'analyse à la demande). Kaspersky Embedded Systems Security résout les variables d'environnement sous le compte utilisé pour démarrer la tâche. Pour en savoir plus sur les variables d'environnement, reportez-vous à la Base de connaissances Microsoft.

d. Cliquez sur le bouton **OK**.

e. Cochez la case **Appliquer aux sous-dossiers** si vous souhaitez exclure tous les fichiers et dossiers enfants de l'objet indiqué de la protection ou de la zone d'analyse.

- Si vous spécifiez le nom d'un objet détectable :

a. Cochez la case Objets à détecter.

b. Cliquez sur le bouton **Modifier**.

La fenêtre **Liste des objets à détecter** s'ouvre.

c. Renseignez le nom ou le masque du nom de l'objet détectable en fonction de la classification de l'encyclopédie des virus.

d. Cliquez sur **Ajouter**.

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

6. Dans la section **Zone d'application des exclusions**, cochez les cases en regard des noms des tâches auxquelles l'exclusion doit être appliquée.

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

L'exclusion s'affiche dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

Ajout de processus de confiance

Vous pouvez ajouter un processus à la liste des processus de confiance d'une des manières suivantes :

- Sélectionner ce processus dans la liste des processus exécutés sur l'appareil protégé.
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

> Si le fichier exécutable d'un processus est modifié, Kaspersky Embedded Systems Security l'exclut de la liste des processus de confiance.

Pour ajouter un ou plusieurs processus à la liste des processus de confiance :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.

   La fenêtre **Zone de confiance** s'ouvre.

3. Ouvrez l'onglet **Processus de confiance**.

4. Cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers** pour éviter l'analyse des opérations de lecture de fichiers.

5. Cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés** pour éviter l'analyse des opérations sur les fichiers pour les processus de confiance.

6. Pour ajouter un processus à la liste des processus de confiance, réalisez une des opérations suivantes :

   - Pour importer des processus de confiance préconfigurés, cliquez sur le bouton **Importer** et, dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration au format XML stocké sur votre appareil.

     Les processus du fichier XML seront ajoutés à la liste des processus de confiance.

   - Pour préciser manuellement les processus, cliquez sur le bouton **Ajouter** et passez aux étapes suivantes.

7. Si vous avez cliqué sur le bouton **Ajouter**, dans le menu contextuel du bouton, sélectionnez l'une des options suivantes :

   - **Processus multiples**.

     Configurez les paramètres suivants dans la fenêtre **Ajout de processus de confiance** qui s'ouvre :

     a. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

     b. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

     c. Cliquez sur le bouton **Parcourir** pour ajouter des données sur la base de processus exécutables.

     d. Dans la fenêtre qui s'ouvre, sélectionnez un fichier exécutable.

     > Vous pouvez ajouter un seul fichier exécutable à la fois. Répétez les étapes c-d pour ajouter d'autres fichiers exécutables.

     e. Cliquez sur le bouton **Processus** pour ajouter des données sur la base de processus en cours.

     f. Dans la fenêtre qui s'ouvre, sélectionnez des processus. Pour sélectionner plusieurs processus, maintenez la touche **CTRL** enfoncée.

     g. Cliquez sur le bouton **OK**.

Le compte utilisateur sous les privilèges duquel la tâche Protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur l'appareil où Kaspersky Embedded Systems Security est installé afin de pouvoir consulter la liste des processus actifs. Vous pouvez trier les processus dans la liste des processus actifs selon le nom du fichier, l'identificateur de processus (PID) ou le chemin d'accès au fichier exécutable du processus sur l'appareil local. Vous pouvez sélectionner des processus en cours d'exécution en cliquant sur le bouton **Processus** uniquement si vous utilisez la Console de l'application sur un périphérique protégé ou dans les paramètres de l'hôte indiqué via Kaspersky Security Center.

- **Un seul processus basé sur le nom et le chemin du fichier**.

  Dans la fenêtre **Ajout d'un processus** qui s'ouvre, procédez comme suit :

  a. Saisissez un chemin d'accès à un fichier exécutable (y compris le nom du fichier).

  Lors de la désignation des objets, vous pouvez utiliser des masques de noms (via les caractères `?` et `*`) et tous les types de variables d'environnement. Les variables d'environnement (remplacement des variables par leurs valeurs) sont résolues par Kaspersky Embedded Systems Security lors du démarrage d'une tâche ou lors de l'application de nouveaux paramètres à une tâche en cours d'exécution (non applicable aux tâches d'analyse à la demande). Kaspersky Embedded Systems Security résout les variables d'environnement sous le compte utilisé pour démarrer la tâche. Pour en savoir plus sur les variables d'environnement, reportez-vous à la Base de connaissances Microsoft.

  b. Cliquez sur le bouton **OK**.

- **Un seul processus basé sur les propriétés**.

  Configurez les paramètres suivants dans la fenêtre **Ajout d'un processus de confiance** qui s'ouvre :

  a. Cliquez sur le bouton **Parcourir** et sélectionnez un processus.

  b. **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance**.

  c. **Utiliser le hash du fichier de processus pour le considérer comme de confiance**.

  d. Cliquez sur le bouton **OK**.

  Pour ajouter le processus sélectionné à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

8. Dans la fenêtre **Zone de confiance**, cliquez sur le bouton **OK**.

Le fichier ou le processus sélectionné sera ajouté à la liste des processus de confiance dans la fenêtre **Zone de confiance**.

Application du masque not-a-virus

Le masque not-a-virus permet de sauter l'analyse des fichiers logiciels et des ressources internet légitimes, qui peuvent être considérés comme nuisibles. Le masque concerne les tâches suivantes :

- Protection des fichiers en temps réel.

- Analyse à la demande.

Si le masque n'est pas ajouté à la liste d'exclusions, Kaspersky Embedded Systems Security applique les actions spécifiées dans les paramètres d'exécution de la tâche pour les ressources logicielles ou Internet qui entrent dans cette catégorie.

Pour appliquer le masque not-a-virus, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance** du menu.

   La fenêtre **Zone de confiance** s'ouvre.
3. Sélectionnez l'onglet **Exclusions**.
4. Faites défiler la liste jusqu'à la valeur *not-a-virus:**.
5. Cochez la case correspondant, au cas où elle aurait été décochée.
6. Cliquez sur le bouton **OK**.

La nouvelle configuration est appliquée.

Administration de la Zone de confiance via le Plug-in Web

Pour configurer la zone de confiance via le Plug-in Web :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Complémentaire**.
5. Cliquez sur **Configuration** de la sous-section **Zone de confiance**.
6. Configurez la zone de confiance en fonction des besoins.

Protection contre les exploits

Cette section contient les instructions de configuration des paramètres de la protection de la mémoire du processus contre l'exploitation des vulnérabilités.

A propos de la protection contre les exploits

Kaspersky Embedded Systems Security permet de protéger la mémoire du processus contre les exploits. Cette fonction est mise en œuvre via le module Protection contre les exploits. Vous pouvez modifier l'état de l'activité du composant, ainsi que configurer les paramètres de protection de mémoire du processus contre l'exploitation des vulnérabilités.

Le composant protège la mémoire du processus contre les Exploits à l'aide de l'Agent de protection des processus (ci après Agent) externe intégré au processus protégé.

L'Agent de protection de processus est un module de Kaspersky Embedded Systems Security chargé dynamiquement qui s'intègre aux processus protégés en vue de contrôler leur intégrité et de réduire l'impact de l'exploitation des vulnérabilités.

Le fonctionnement de l'Agent à l'intérieur du processus protégé dépend des itérations de lancement et d'arrêt de ce processus : le chargement primaire de l'Agent dans le processus ajouté à la liste des processus protégés est possible seulement au relancement du processus. Le déchargement de l'Agent de processus une fois supprimé de la liste est possible seulement après le relancement du processus.

Il convient d'arrêter l'Agent avant de le décharger des processus protégés : lors de la suppression du composant Protection contre les exploits, l'application gèle l'environnement et force le déchargement de l'Agent des processus protégés. Si, au cours de la désinstallation du composant, l'agent est inséré dans un des processus protégés, vous devez arrêter le processus affecté. Un redémarrage de l'appareil protégé peut être nécessaire (par exemple, si le processus système est protégé).

En cas de détection de signes d'une attaque de l'Exploit sur le processus protégé, Kaspersky Embedded Systems Security exécute une des actions suivantes :

- termine le processus lors de la tentative d'exploitation de la vulnérabilité ;
- informe que le processus a été compromis .

Vous pouvez arrêter la protection des processus d'une des manières suivantes :

- supprimer le composant ;
- supprimer le processus de la liste des processus protégés et le relancer.

Service Kaspersky Security Exploit Prevention

Pour garantir l'efficacité du composant Protection contre les exploits, le service Kaspersky Security Exploit Prevention est requis sur l'appareil protégé. Ce service et le module Protection contre les exploits font partie de l'installation recommandée. Lors de l'installation du service sur l'appareil protégé, le processus kavfswh est créé et lancé. Celui-ci transmet les informations relatives aux processus protégés depuis le module vers l'Agent de sécurité.

Après l'arrêt du service Kaspersky Security Exploit Prevention, Kaspersky Embedded Systems Security continue de protéger les processus qui ont été ajoutés à la liste des processus protégés, puis il est également chargé dans les nouveaux processus ajoutés et applique toutes les techniques disponibles de protection contre les exploits pour protéger la mémoire du processus.

Si votre appareil tourne sous le système d'exploitation Windows 10 ou suivant, l'application cesse de protéger les processus et la mémoire du processus après l'arrêt du Service Kaspersky Security Exploit Prevention.

En cas d'arrêt du service Kaspersky Security Exploit Prevention Broker Host, l'application ne reçoit pas les données sur les événements qui se produisent avec les processus protégés (y compris, les données sur les attaques des exploits et l'achèvement des processus). L'Agent ne pourra pas non plus recevoir les données sur les nouveaux paramètres de protection et sur l'ajout des nouveaux processus à la liste des processus protégés.

Mode de protection contre les exploits

Vous pouvez configurer les actions de réduction de l'impact de l'exploitation des vulnérabilités dans les processus protégés, en sélectionnant un de deux modes :

- **Terminer en cas d'exploit** : appliquez ce mode pour terminer le processus en cas de tentative d'exploitation d'une vulnérabilité.

  En cas de détection d'une tentative d'exploitation d'une vulnérabilité dans un processus du système d'exploitation critique protégé, Kaspersky Embedded Systems Security ne termine pas ce processus quel que soit le mode indiqué dans les paramètres du module Protection contre les exploits.

- **Informer uniquement** : appliquez ce mode pour recevoir des informations sur les instances d'exploits dans les processus protégés à l'aide des événements dans les journaux de sécurité.

  Si ce mode est sélectionné, Kaspersky Embedded Systems Security crée des événements pour consigner toutes les tentatives d'exploit de vulnérabilités.

Administration de la Protection contre les exploits via le plug-in d'administration

Cette section présente la navigation dans l'interface du plug-in d'administration et la configuration des paramètres du composant pour un seul ou pour l'ensemble des appareils protégés du réseau.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres de la stratégie pour la Protection contre les exploits

Pour accéder aux paramètres de protection contre les exploits via une stratégie de Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.
5. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, sélectionnez la section **Protection en temps réel de l'ordinateur**.
6. Cliquez sur le bouton **Configuration** dans la sous-section **Protection contre les exploits**.
   La fenêtre **Protection contre les exploits** s'ouvre.

Configurez la Protection contre les exploits en fonction des besoins.

Ouverture de la fenêtre des propriétés de la Protection contre les exploits

Pour ouvrir la fenêtre des propriétés de la Protection contre les exploits :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Périphériques**.
4. Ouvrez la fenêtre **Propriétés : <Nom du périphérique>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - Sélectionnez l'option **Propriétés** dans le menu contextuel du périphérique protégé.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
5. Dans la section **Applications**, sélectionnez **Kaspersky Embedded Systems Security 3.2**.
6. Cliquez sur le bouton **Propriétés**.
   La fenêtre de configuration de l'application **Kaspersky Embedded Systems Security 3.2 s'ouvre**.
7. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
8. Cliquez sur le bouton **Configuration**dans la sous-section **Protection contre les exploits**.
   La fenêtre **Protection contre les exploits** s'ouvre.

Configurez la Protection contre les exploits en fonction des besoins.

Configuration des paramètres de protection de la mémoire du processus

Pour configurer les paramètres de protection des Exploits pour les processus ajoutés à la liste des processus protégés, procédez comme suit :

1. Ouvrez la fenêtre **Protection contre les exploits**.
2. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :
   - **Empêcher l'exploit des processus vulnérables**.
     - **Terminer en cas d'exploit**.
     - **Informer uniquement**.
3. Configurez les paramètres suivants dans le groupe **Actions de prévention** :
   - **Signaler les processus exploités via le service de terminal**.
   - **Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé**.
4. Dans la fenêtre **Protection contre les exploits**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security enregistre les paramètres de protection de mémoire du processus configurés et les applique.

Ajout d'un processus à la zone de protection

Le composant Protection contre les exploits offre une protection contre plusieurs processus par défaut. Vous pouvez exclure les processus de la zone de protection en décochant les cases correspondantes dans la liste.

Pour ajouter un processus à la liste des processus protégés :

1. Ouvrez la fenêtre **Protection contre les exploits**.
2. Cliquez sur le bouton **Parcourir** sous l'onglet **Processus protégés**.

   Une fenêtre standard de l'Explorateur Microsoft Windows s'ouvre.
3. Choisissez le processus que vous voulez ajouter à la liste.
4. Cliquez sur le bouton **Ouvrir**.

   Le nom du processus apparaît dans la ligne.
5. Cliquez sur **Ajouter**.

   Le processus indiqué est ajouté à la liste des processus protégés.
6. Sélectionnez le processus ajouté.
7. Cliquez sur **Définir les techniques de protection contre les exploits**.

   La fenêtre **Techniques de protection contre les exploits** s'ouvre.
8. Choisissez une des options d'application de la technique de réduction de l'impact :
   - **Appliquer toutes les techniques de protection contre les exploits disponibles**.

     Quand cette option a été sélectionnée, il est impossible de modifier la liste. Par défaut, toutes les techniques disponibles sont appliquées à un processus.
   - **Appliquer les techniques de protection contre les exploits indiquées**.

Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :

a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.

b. Cochez ou décochez la case **Appliquer la technique Attack Surface Reduction**.

9. Configurez les paramètres de la technique Attack Surface Reduction :

- Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
- Dans le champ **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :
  - **Internet**
  - **Intranet local**
  - **URL de confiance**
  - **URL à accès restreint**
  - **Ordinateur**

Ces paramètres s'appliquent uniquement à Internet Explorer®.

10. Cliquez sur le bouton **OK**.

Le processus est ajouté à la zone de protection de la tâche.

Administration de la Protection contre les exploits via la Console de l'application

Cette section présente la navigation dans l'interface de la Console de l'application et la configuration des paramètres d'un composant sur un appareil protégé.

Navigation

Apprenez à accéder aux paramètres de la tâche requis via l'interface sélectionnée.

Accès aux paramètres généraux de la Protection contre les exploits

*Pour ouvrir la fenêtre **Paramètres de protection contre les exploits**, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection des fichiers en temps réel**.

2. Sélectionnez le nœud **Protection contre les exploits**.

3. Dans la section **Paramètres de protection des processus**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de protection contre les exploits** s'ouvre.

Configurez les paramètres généraux pour la Protection contre les exploits en fonction des besoins.

Accès aux paramètres de protection du processus Protection contre les exploits

*Pour ouvrir la fenêtre **Paramètres de protection des processus**, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection des fichiers en temps réel**.

2. Sélectionnez le nœud **Protection contre les exploits**.

Dans la section **Paramètres de protection des processus**, cliquez sur le lien **Paramètres de protection des processus**.

La fenêtre **Paramètres de protection des processus** s'ouvre.

Configurez les paramètres de protection du processus pour la Protection contre les exploits en fonction des besoins.

Configuration des paramètres de protection de la mémoire du processus

Pour ajouter un processus à la liste des processus protégés :

1. Ouvrez la fenêtre **Paramètres de protection contre les exploits**.

2. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :

   - **Empêcher l'exploit des processus vulnérables**.
     - **Terminer en cas d'exploit**.
     - **Informer uniquement**.

3. Configurez les paramètres suivants dans le groupe **Actions de prévention** :

   - **Signaler les processus exploités via le service de terminal**.
   - **Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé**.

4. Dans la fenêtre des paramètres de la **Paramètres de protection contre les exploits**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security enregistre les paramètres de protection de mémoire du processus configurés et les applique.

Ajout d'un processus à la zone de protection

Le composant Protection contre les exploits offre une protection contre plusieurs processus par défaut. Vous pouvez décocher les processus que vous ne souhaitez pas protéger dans la liste des processus protégés.

Pour ajouter un processus à la liste des processus protégés :

1. Ouvrez la fenêtre **Paramètres de protection des processus**.
2. Pour ajouter un processus et le protéger contre l'intrusion de code malveillant ou réduire l'impact d'un exploit potentiel, procédez comme suit :
   a. Cliquez sur le bouton **Parcourir**.
      La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.
   b. Dans la fenêtre qui s'ouvre, choisissez le processus que vous voulez ajouter à la liste.
   c. Cliquez sur le bouton **Ouvrir**.
   d. Cliquez sur **Ajouter**.
      Le processus indiqué est ajouté à la liste des processus protégés.
3. Sélectionnez le processus ajouté dans la liste.
4. La configuration actuelle s'affiche sous l'onglet **Paramètres de protection des processus** :
   - **Nom du processus**.
   - **Exécution en cours**.
   - **Techniques de protection contre les exploits appliquées**.
   - **Paramètres de la technique Attack Surface Reduction**.
5. Pour modifier les techniques de protection contre les exploits appliquées au processus, sélectionnez l'onglet **Interdire le chargement de modules**.
6. Choisissez une des options d'application de la technique de réduction de l'impact :
   - **Appliquer toutes les techniques de protection contre les exploits disponibles**.
     Quand cette option a été sélectionnée, il est impossible de modifier la liste. Par défaut, toutes les techniques disponibles sont appliquées à un processus.
   - **Appliquer les techniques de protection contre les exploits indiquées pour le processus**.
     Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :
     a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.
7. Configurez les paramètres de la technique Attack Surface Reduction :
   - Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
   - Dans la section **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :

- **Internet**
- **Intranet local**
- **URL de confiance**
- **Sites à accès restreint**
- **Ordinateur**

Ces paramètres s'appliquent uniquement à Internet Explorer®.

8. Cliquez sur **Enregistrer**.

Le processus est ajouté à la zone de protection de la tâche.

Administration de la Protection contre les exploits via le Plug-in Web

Cette section présente la navigation dans l'interface du Plug-in Web et la configuration des paramètres d'un composant sur un périphérique protégé.

Configuration des paramètres de protection de la mémoire du processus

Pour configurer les paramètres de protection des Exploits pour les processus ajoutés à la liste des processus protégés, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection contre les exploits**.
6. Ouvrez l'onglet **Paramètres de protection contre les exploits**.
7. Configurez les paramètres suivants dans le groupe **Mode de protection contre les exploits** :
   - Empêcher l'exploit des processus vulnérables.
     - Terminer en cas d'exploit.
     - Informer uniquement.
8. Configurez les paramètres suivants dans le groupe **Actions de prévention** :
   - Signaler les processus exploités via le service de terminal.

- Empêcher l'exploit des processus vulnérables même si le service Kaspersky Security est désactivé.

9. Dans la fenêtre **Protection contre les exploits**, cliquez sur le bouton **OK**.

Kaspersky Embedded Systems Security enregistre les paramètres de protection de mémoire du processus configurés et les applique.

Ajout d'un processus à la zone de protection

Pour configurer les paramètres de protection des Exploits pour les processus ajoutés à la liste des processus protégés, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Stratégies et profils**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur **Configuration** dans la sous-section **Protection contre les exploits**.
6. Ouvrez l'onglet **Processus protégés**.
7. Cliquez sur **Ajouter**.
8. La fenêtre **Techniques de protection contre les exploits** s'ouvre.
9. Définissez le nom du processus.
10. Choisissez une des options d'application de la technique de réduction de l'impact :
    - **Appliquer toutes les techniques de protection contre les exploits disponibles**.

      Quand cette option a été sélectionnée, il est impossible de modifier la liste. Par défaut, toutes les techniques disponibles sont appliquées à un processus.
    - **Appliquer les techniques de protection contre les exploits indiquées**.

      Si vous choisissez cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer :

      a. Cochez les cases en regard des techniques que vous souhaitez appliquer à la protection du processus choisi.

      b. Cochez ou décochez la case **Appliquer la technique Attack Surface Reduction**.
11. Configurez les paramètres de la technique Attack Surface Reduction :
    - Saisissez les noms des modules dont le lancement sera interdit depuis le processus protégé dans le champ **Interdire les modules**.
    - Dans le champ **Ne pas interdire les modules si exécutés dans la Zone Internet**, cochez les cases en regard des options dans lesquelles vous souhaitez autoriser le lancement des modules :
      - **Internet**

- **Intranet local**
- **URL de confiance**
- **URL à accès restreint**
- **Ordinateur**

Ces paramètres s'appliquent uniquement à Internet Explorer®.

12. Cliquez sur le bouton **OK**.

Le processus est ajouté à la zone de protection de la tâche.

Techniques de protection contre les exploits

Techniques de protection contre les exploits

Technique de protection contre les exploits	Description
Data Execution Prevention (DEP)	Prévention de l'exécution des données, à savoir l'interdiction de l'exécution d'un code aléatoire dans un secteur protégé de la mémoire.
Address Space Layout Randomization (ASLR)	Modification de la disposition des structures de données dans l'espace d'adresse du processus.
Structured Exception Handler Overwrite Protection (SEHOP)	Substitution de l'enregistrement dans la structure des exclusions ou substitution du processeur d'exclusions.
Null Page Allocation	Prévention de la réorientation de l'index nul.
LoadLibrary Network Call Check (Anti ROP)	Protection contre le chargement des bibliothèques dynamiques depuis les chemins de réseau.
Executable Stack (Anti ROP)	Interdiction de l'exécution non autorisée des zones de la pile.
Anti RET Check (Anti ROP)	Contrôle de l'invocation sûre d'une fonction via l'instruction CALL.
Anti Stack Pivoting (Anti ROP)	Protection contre le déplacement de l'index de pile ESP vers l'adresse exploitée.
Simple Export Adress Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection de l'accès en lecture du tableau d'exportation des adresses (Export Address Table) pour les modules kernel32.dll, kernelbase.dll et ntdll.dll
Heap Spray Allocation (Heapspray)	Protection contre l'attribution de mémoire en cas d'exécution d'un code malveillant.
Execution Flow Simulation (Anti Return Oriented Programming)	Détection de chaînes d'instructions potentiellement dangereuses (gadget ROP possible) dans le composant Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection contre l'élévation de privilèges via une vulnérabilité dans le pilote AFD (exécution du code arbitraire sur le cercle nul dans l'appel QueryIntervalProfile).
Attack Surface Reduction (ASR)	Interdiction du lancement de modules vulnérables via le processus protégé.

Anti Process Hollowing (Hollowing)	Protection contre la création et l'exécution des copies malveillantes des processus douteux.
Anti AtomBombing (APC)	Exploit global atom table via des appels APC.
Anti CreateRemoteThread (RThreadLocal)	Un autre processus a créé une thread dans un processus protégé.
Anti CreateRemoteThread (RThreadRemote)	Un autre processus a créé une thread de contrôle dans un processus protégé.

Intégration aux systèmes tiers

Cette section décrit l'intégration de Kaspersky Embedded Systems Security aux fonctions et technologies tierces.

Compteurs de performance pour l'application Moniteur système

Cette section fournit des informations sur les compteurs de performance pour l'application Moniteur Système de Microsoft Windows enregistrés par Kaspersky Embedded Systems Security pendant l'installation.

A propos des compteurs de performance de Kaspersky Embedded Systems Security

Les composants à installer de Kaspersky Embedded Systems Security incluent par défaut le composant Compteurs de performance. Pendant l'installation, Kaspersky Embedded Systems Security enregistre ses compteurs de performance pour l'application Moniteur système de Microsoft Windows.

Grâce aux compteurs de Kaspersky Embedded Systems Security, vous pouvez contrôler les performances de l'application durant l'exécution des tâches de protection en temps réel de l'ordinateur. Vous pouvez identifier les goulots d'étranglement en cas d'utilisation avec d'autres applications et les manques de ressources. Vous pouvez diagnostiquer les plantages de Kaspersky Embedded Systems Security et identifier les paramètres indésirables.

Pour consulter les compteurs de performance de Kaspersky Embedded Systems Security, ouvrez la console **Optimisation** dans la section **Administration** du panneau de configuration de Windows.

Les sections suivantes abordent la définition des compteurs, les intervalles de calcul des relevés recommandés, les seuils et les recommandations pour la configuration de Kaspersky Embedded Systems Security lorsque les compteurs dépassent ces valeurs.

Total de requêtes rejetées (Total number of requests denied)

Total de requêtes rejetées (Total number of requests denied)

Nom	Total de requêtes rejetées (Total number of requests denied)
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de l'application, le calcul est réalisé depuis la dernière exécution de Kaspersky Embedded Systems Security. L'application ignore les objets dont les requêtes de traitement sont rejetées par les processus de Kaspersky Embedded Systems Security.
Fonction	Ce compteur permet d'identifier : • Protection en temps réel de l'ordinateur réduite en raison d'une surcharge des processus de Kaspersky Embedded Systems Security. • Interruption de la protection en temps réel de l'ordinateur en raison d'échecs des gestionnaires d'interception de fichier.
Valeur normale / seuil	0 / 1.

Intervalle de calcul des relevés recommandé	1 heure.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés. Les situations suivantes sont envisageables en fonction du "comportement" du compteur : • Le compteur indique certains plusieurs requêtes rejetées durant une longue période : tous les processus de Kaspersky Embedded Systems Security étaient complètement occupés, si bien que Kaspersky Embedded Systems Security n'a pas pu analyser les objets. Pour éviter que des objets soient ignorés, augmentez le nombre de processus de l'application pour les tâches Protection en temps réel de l'ordinateur. Vous pouvez utiliser le paramètre de Kaspersky Embedded Systems Security **Nombre de processus de protection en temps réel**. • Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : le gestionnaire d'intercepteurs de fichiers ne fonctionne plus. Kaspersky Embedded Systems Security n'analyse pas les objets à l'accès. Relancez Kaspersky Embedded Systems Security.

Total de requêtes ignorées (Total number of requests skipped).

Total de requêtes ignorées (Total number of requests skipped).

Nom	Total de requêtes ignorées (Total number of requests skipped).
Définition	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par Kaspersky Embedded Systems Security et qui n'ont pas généré d'événement sur la fin du traitement, ce nombre est calculé depuis la dernière exécution de l'application. Si une requête de traitement d'un objet est acceptée par un des processus de travail mais n'envoie pas un événement signalant que le traitement est terminé, le pilote transmet cette requête à un autre processus et la valeur du compteur **Total des requêtes ignorées** augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a accepté la requête de traitement (ils étaient occupés) ou n'a pas envoyé un événement sur la fin du traitement, Kaspersky Embedded Systems Security ignore cet objet et la valeur du compteur **Total des requêtes rejetées** augmente d'une unité.
Fonction	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
Valeur normale / seuil	0 / 1
Intervalle de calcul des relevés recommandé	1 heure
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur diffère de zéro, cela signifie qu'un ou plusieurs flux du gestionnaire d'intercepteurs de fichiers sont gelés. La valeur du compteur correspond au nombre de flux gelés en ce moment. Si la vitesse d'analyse n'est pas satisfaisante, redémarrez Kaspersky Embedded Systems Security afin de rétablir les flux gelés.

Nombre de requêtes non traitées en raison d'un manque de ressources système

Nombre de requêtes non traitées en raison d'un manque de ressources système

Nom	Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources).
Définition	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources système (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security ignore les requêtes de traitement d'objet qui ne sont pas traitées par le pilote d'interception de fichiers.
Fonction	Le compteur permet de repérer et de résoudre une éventuelle baisse de la qualité de la Protection en temps réel de l'ordinateur provoquée par un manque de ressources.
Valeur normale / seuil	0 / 1.
Intervalle de calcul des relevés recommandé	1 heure.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si le compteur affiche une valeur différente de zéro, les processus de travail de Kaspersky Embedded Systems Security ont besoin de plus de mémoire vive pour traiter les requêtes. Il se peut que les processus actifs d'autres applications utilisent toute la mémoire vive disponible.

Nombre de requêtes envoyées pour traitement

Nombre de requêtes envoyées pour traitement

Nom	Nombre de requêtes envoyées pour traitement.
Définition	Nombre d'objets en attente de traitement par les processus actifs.
Fonction	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Embedded Systems Security et le niveau général de l'activité de fichiers sur le périphérique protégé.
Valeur normale / seuil	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur l'appareil protégé.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	S/O

Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers.
Définition	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (moyenne pour tous les processus impliqués dans les tâches de protection en temps réel de l'ordinateur à ce moment).
Fonction	Ce compteur permet d'identifier une éventuelle détérioration de la qualité de la Protection en temps réel de l'ordinateur en raison de la charge des processus de Kaspersky Embedded Systems Security et d'y remédier.
Valeur normale / seuil	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Chaque processus actif peut accepter un maximum de 60 flux du gestionnaire d'intercepteurs de fichiers. Si le compteur approche de 60, il se peut qu'aucun des processus actifs ne puisse accepter une nouvelle requête de traitement du pilote d'intercepteurs de fichiers et Kaspersky Embedded Systems Security ignorera l'objet. Augmentez le nombre de processus de Kaspersky Embedded Systems Security pour les tâches de protection en temps réel de l'ordinateur. Vous pouvez utiliser le paramètre de Kaspersky Embedded Systems Security **Nombre de processus de protection en temps réel**.

Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Nom	Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers.
Définition	Nombre de flux du gestionnaire d'intercepteurs de fichiers dans un processus actif (maximum pour tous les processus impliqués dans les tâches de protection en temps réel de l'ordinateur à ce moment).
Fonction	Ce compteur permet d'identifier une réduction des performances en raison d'une répartition inégale de la charge dans les processus actifs exécutés et d'y remédier
Valeur normale / seuil	Varie/40.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur de ce compteur dépasse en permanence et de beaucoup le **Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers**, Kaspersky Embedded Systems Security répartit de manière inégale la charge sur les processus exécutés. Relancez Kaspersky Embedded Systems Security.

Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)

Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)

Nom	Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue).
Définition	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce

	moment.
Fonction	Ce compteur permet d'identifier : • Interruption de la protection en temps réel de l'ordinateur en raison d'échecs potentiels des gestionnaires d'interception de fichier. • Surcharge des processus suite à une répartition inégale du temps de processeur entre différents processus de travail et Kaspersky Embedded Systems Security. • Les épidémies de virus.
Valeur normale / seuil	La valeur du compteur peut être différente de zéro tant que Kaspersky Embedded Systems Security traite les objets probablement infectés ou infectés découverts mais elle revient sur zéro juste après le traitement / La valeur du compteur est différente de zéro pendant une longue période.
Intervalle de calcul des relevés recommandé	Une minute
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur n'est pas égale à zéro pendant une longue période : • Kaspersky Embedded Systems Security ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit arrêté) ; Relancez Kaspersky Embedded Systems Security. • Il peut ne pas y avoir assez de temps de processeur pour traiter les objets. Accordez à Kaspersky Embedded Systems Security plus de temps de processeur, par exemple en réduisant la charge des autres applications sur le périphérique protégé. • Une épidémie de virus s'est déclenchée. L'émergence d'une épidémie de virus est également indiquée par le nombre élevé d'objets infectés ou probablement infectés découverts dans la tâche Protection des fichiers en temps réel. Les informations relatives au nombre d'objets détectés figure dans les statistiques de la tâche ou dans le journal d'exécution de la tâche.

Nombre d'objets traités par seconde

Nombre d'objets traités par seconde

Nom	Nombre d'objets traités par seconde.
Définition	Nombre d'objets traités par unité de temps pendant laquelle ces objets ont été traités ; le décompte s'opère sur des intervalles de temps égaux
Fonction	Ce compteur affiche la vitesse de traitement des objets ; il permet d'identifier une baisse des performances du périphérique protégé en raison d'un manque de temps de processeur actif pour les processus de Kaspersky Embedded Systems Security ou d'erreurs de fonctionnement de Kaspersky Embedded Systems Security et d'y remédier.
Valeur normale / seuil	Varie / non.
Intervalle de calcul des relevés recommandé	Une minute.

Recommandation pour la configuration si la valeur dépasse la valeur limite	Les valeurs du compteur dépendent des paramètres définies dans Kaspersky Embedded Systems Security et de la charge des processus des autres applications sur le périphérique protégé. Observez le niveau moyen du compteur au cours d'une longue période. Si le niveau du compteur a diminué, c'est peut-être à cause d'une des situations suivantes : • Les processus de travail de Kaspersky Embedded Systems Security ne disposent pas des ressources de processeur suffisantes pour traiter les objets. Accordez à Kaspersky Embedded Systems Security plus de temps de processeur, par exemple en réduisant la charge des autres applications sur le périphérique protégé. • Un échec s'est produit dans le fonctionnement de Kaspersky Embedded Systems Security (plusieurs flux sont gelés). Relancez Kaspersky Embedded Systems Security.

Compteurs et interruptions SNMP de Kaspersky Embedded Systems Security

Cette section contient des informations sur les compteurs et les interruptions SNMP de Kaspersky Embedded Systems Security.

A propos des compteurs et interruptions SNMP de Kaspersky Embedded Systems Security

Si vous avez inclus le composant Compteurs et pièges SNMP dans les composants antivirus à installer, vous pouvez consulter les compteurs et les interruptions de Kaspersky Embedded Systems Security à l'aide du protocole Simple Network Management Protocol (SNMP).

Pour consulter les compteurs et les interruptions de Kaspersky Embedded Systems Security depuis le poste de travail de l'administrateur, lancez sur le périphérique protégé le service SNMP (SNMP Service) et le service d'interruptions SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

Compteurs SNMP de Kaspersky Embedded Systems Security

Cette section propose un tableau contenant la description des paramètres des compteurs SNMP de Kaspersky Embedded Systems Security.

Compteurs de performance

Compteurs de performance

Compteur	Définition
currentRequestsAmount	Nombre de requêtes envoyées pour traitement

currentInfectedQueueLength	Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)
currentObjectProcessingRate	Nombre d'objets traités par seconde
currentWorkProcessesNumber	Nombre actuel de processus de travail utilisés par Kaspersky Embedded Systems Security

Compteurs de quarantaine

Compteurs de quarantaine

Compteur	Définition
totalObjects	Nombre d'objets présents actuellement en quarantaine
totalSuspiciousObjects	Nombre d'objets probablement infectés présents actuellement en quarantaine
currentStorageSize	Volume total de données en quarantaine (Mo)

Compteur de sauvegarde

Compteur de sauvegarde

Compteur	Définition
currentBackupStorageSize	Volume total de données en sauvegarde (Mo)

Compteurs généraux

Compteurs généraux

Compteur	Définition
lastCriticalAreasScanAge	Période écoulée depuis la dernière analyse rapide du périphérique protégé (intervalle de temps en secondes entre la date de fin de la tâche portant le statut Tâche d'analyse rapide et le moment actuel).
licenseExpirationDate	Date d'expiration de la licence. Si des clés active et additionnelle ont été ajoutées, la date affichée est la date d'échéance de la licence associée à la clé additionnelle.
currentApplicationUptime	Durée de fonctionnement de Kaspersky Embedded Systems Security depuis sa dernière exécution (en centièmes de secondes).

Compteur de mise à jour

Compteur de mise à jour

Compteur	Définition
avBasesAge	"Age" des bases (intervalle de temps en centièmes de seconde écoulé depuis la date de création des dernières mises à jour installées).

Compteurs de Protection des fichiers en temps réel

Compteurs de Protection des fichiers en temps réel

Compteur	Définition
totalObjectsProcessed	Nombre d'objets analysés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalInfectedObjectsFound	Nombre d'objets infectés et autres découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalSuspiciousObjectsFound	Nombre d'objets probablement infectés découverts depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalVirusesFound	Nombre d'objets détectés depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsQuarantined	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Embedded Systems Security a placé en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotQuarantined	Nombre total d'objets infectés ou probablement infectés que Kaspersky Embedded Systems Security a tenté de placer en vain en quarantaine ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsDisinfected	Nombre total d'objets infectés qui ont été désinfectés par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDisinfected	Nombre total d'objets infectés ou autres que Kaspersky Embedded Systems Security a tenté de désinfecter en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsDeleted	Nombre total d'objets infectés, probablement infectés ou autres supprimés par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotDeleted	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Embedded Systems Security a tenté de supprimer en vain ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsBackedUp	Nombre total d'objets infectés ou autres placés dans la Sauvegarde par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel
totalObjectsNotBackedUp	Nombre total d'objets infectés ou autres que Kaspersky Embedded Systems Security a tenté de placer en vain dans la Sauvegarde ; ce nombre est calculé depuis la dernière exécution de la tâche Protection des fichiers en temps réel

Interruptions SNMP de Kaspersky Embedded Systems Security et leur option

Les options des interruptions SNMP de Kaspersky Embedded Systems Security sont résumées comme suit :

- eventThreatDetected : un objet a été détecté.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - computerName
  - UserName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds : dépassement de la taille maximale de la Sauvegarde. Le volume total de données de la Sauvegarde dépasse la valeur du paramètre **Taille maximale de sauvegarde (Mo)**. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds : le seuil d'espace libre pour la sauvegarde est atteint. Le volume d'espace disponible dans la Sauvegarde est inférieur ou égal à la moitié de la valeur du champ **Seuil d'espace disponible (Mo)**. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds : dépassement de la taille maximum de la quarantaine. Le volume total de données de la Quarantaine a dépassé la valeur du paramètre **Taille maximale de la quarantaine (Mo)**. Kaspersky Embedded Systems Security poursuit la mise en quarantaine des objets probablement infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds : le seuil d'espace libre pour la quarantaine est atteint. La quantité d'espace disponible dans la Quarantaine, définie par le paramètre **Seuil d'espace disponible (Mo)**, est inférieure ou égale à la valeur indiquée. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined : Erreur de quarantaine.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - UserName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped : erreur d'enregistrement d'une copie de l'objet dans la Sauvegarde.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - UserName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError : Erreur de quarantaine interne.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventReason

- eventBackupInternalError : Erreur de sauvegarde.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated : La base antivirus n'est plus à jour. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de l'application (tâche locale, tâche de groupe ou tâche pour les sélections d'appareils protégés).

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated : La base antivirus est périmée. Nombre de jours écoulés depuis la dernière exécution de la tâche de mise à jour des bases de l'application (tâche locale, tâche de groupe ou tâche pour les sélections d'appareils protégés).

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted : Kaspersky Embedded Systems Security est en cours d'exécution.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown : Kaspersky Embedded Systems Security est arrêté.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime

- eventSource

- eventCriticalAreasScanWasntPerformForALongTime : Analyse rapide non réalisée depuis longtemps. Nombre de jours écoulés depuis la dernière exécution de la tâche Analyse rapide.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired : Licence expirée.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon : Si la durée de validité de la licence arrive bientôt à échéance. Le nombre de jour restant avant la fin de la validité de la licence est compté

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError : erreur d'exécution de la tâche.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError : erreur lors de l'exécution de la tâche de mise à jour.

  Les options d'interruptions sont les suivantes :

  - eventSeverity

- eventDateAndTime
- taskName
- updaterErrorEventReason

Descriptions et valeurs possibles des options d'interruptions SNMP de Kaspersky Embedded Systems Security

Les descriptions des options d'interruption et valeurs possibles des paramètres sont reprises ci-après :

- eventDateAndTime : date et heure de l'événement.
- eventSeverity : niveau d'importance.

  L'option peut prendre les valeurs suivantes :

  - critical (1) – critique,
  - warning (2) – avertissement,
  - info (3) – informations.
- userName : un nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté).
- computerName : nom de l'appareil protégé (par exemple, nom de l'appareil protégé depuis lequel l'utilisateur a tenté d'accéder à un fichier infecté).
- eventSource : composant fonctionnel qui a généré l'événement.

  L'option peut prendre les valeurs suivantes :

  - unknown (0) – composant fonctionnel non identifié ;
  - quarantine (1) – Quarantaine ;
  - backup (2) – Sauvegarde ;
  - reporting (3) – Journaux d'exécution des tâches ;
  - updates (4) – Mise à jour ;
  - realTimeProtection (5) –Protection des fichiers en temps réel ;
  - onDemandScanning (6) – Analyse à la demande
  - product (7) – événement lié non pas au fonctionnement d'un composant particulier mais au fonctionnement de Kaspersky Embedded Systems Security dans son ensemble ;
  - systemAudit (8) – Journal d'audit système.
- eventReason : déclencheur de l'événement : cause de l'événement.

  L'option peut prendre les valeurs suivantes :

- reasonUnknown(0) – cause indéterminée.
- reasonInvalidSettings (1) – uniquement pour les événements de la Sauvegarde et de la Quarantaine, s'affiche si la Sauvegarde ou la Quarantaine est inaccessible (privilèges d'accès insuffisants ou dossier incorrect indiqué dans les paramètres de la Quarantaine, par exemple le chemin de réseau indiqué est incorrect). Dans ce cas, Kaspersky Embedded Systems Security utilise le dossier de sauvegarde ou de quarantaine indiqué par défaut.

- objectName : nom de l'objet (par exemple, nom du fichier contenant le virus).
- threatName : nom de l'objet détecté selon la classification de l'Encyclopédie des virus. Ce nom figure dans le nom complet que Kaspersky Embedded Systems Security renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
- detectType : type d'objet détecté.

  L'option peut prendre les valeurs suivantes :

  - undefined (0) – indéterminé ;
  - virware – virus et vers de réseau traditionnels ;
  - trojware – chevaux de Troie ;
  - malware – autres applications malveillantes ;
  - adware – applications publicitaires ;
  - pornware – logiciels pornographiques ;
  - riskware – applications légitimes pouvant être utilisées à des fins malveillantes pour endommager l'appareil ou les données personnelles de l'utilisateur.
- detectCertainty : coefficient de certitude pour la détection d'une menace.

  L'option peut prendre les valeurs suivantes :

  - Suspicion (probablement infecté) : Kaspersky Embedded Systems Security a détecté une correspondance partielle entre un morceau de code de l'objet et un morceau de code malveillant connu.
  - Sure (infecté) : Kaspersky Embedded Systems Security a détecté une équivalence parfaite entre une partie du code de l'objet et une partie d'un code malveillant connu.
- days : nombre de jours (par exemple, nombre de jours d'ici la fin de la validité de la licence).
- errorCode : un code d'erreur.
- knowledgeBaseId : adresse de l'article dans la banque de solutions (par exemple, adresse de l'article décrivant une erreur quelconque).
- taskName : un nom de tâche.
- updaterErrorEventReason : cause de l'erreur de mise à jour.

  L'option peut prendre les valeurs suivantes :

  - reasonUnknown(0) : cause indéterminée.
  - reasonAccessDenied : accès refusé.

- reasonUrlsExhausted : fin de la liste des sources de mise à jour.
- reasonInvalidConfig : fichier de configuration incorrect.
- reasonInvalidSignature : signature non valide.
- reasonCantCreateFolder : création du répertoire impossible.
- reasonFileOperError : erreur de fichier.
- reasonDataCorrupted : objet endommagé.
- reasonConnectionReset : réinitialisation de la connexion.
- reasonTimeOut : délai d'attente pour la connexion expiré.
- reasonProxyAuthError : erreur d'authentification sur le serveur proxy.
- reasonServerAuthError : erreur d'authentification sur le serveur.
- reasonHostNotFound : périphérique introuvable.
- reasonServerBusy : serveur inaccessible.
- reasonConnectionError : erreur de connexion.
- reasonModuleNotFound : objet introuvable.
- reasonBlstCheckFailed(16) : erreur lors de la vérification de la liste de refus des clés. Il se peut qu'une mise à jour des bases de l'application ait été diffusée au moment de la mise à jour. Essayez à nouveau de réaliser la mise à jour dans quelques minutes.

- storageObjectNotAddedEventReason : cause du non placement de l'objet en sauvegarde ou en quarantaine.

  L'option peut prendre les valeurs suivantes :

  - reasonUnknown(0) – cause indéterminée.
  - reasonStorageInternalError : erreur ; Kaspersky Embedded Systems Security doit être restauré.
  - reasonStorageReadOnly : la base de données est en lecture seule ; Kaspersky Embedded Systems Security doit être restauré.
  - reasonStorageIOError : erreur entrée/sortie : a) Kaspersky Embedded Systems Security est endommagé, Kaspersky Embedded Systems Security doit être restauré ; b) le disque contenant les fichiers de Kaspersky Embedded Systems Security est endommagé.
  - reasonStorageCorrupted : le stockage est endommagé ; Kaspersky Embedded Systems Security doit être restauré.
  - reasonStorageFull : la base de données est pleine ; un espace disque supplémentaire est requis.
  - reasonStorageOpenError : impossible d'ouvrir le fichier base de données ; Kaspersky Embedded Systems Security doit être restauré.
  - reasonStorageOSFeatureError – certaines particularités du système d'exploitation ne répondent pas aux exigences de Kaspersky Embedded Systems Security.

- reasonObjectNotFound : l'objet placé dans la Quarantaine n'existe pas sur le disque.
- reasonObjectAccessError : privilèges insuffisants pour l'utilisation de Backup API : le compte utilisateur sous les privilèges duquel l'opération est réalisée ne jouit pas des privilèges Backup Operator.
- reasonDiskOutOfSpace : espace insuffisant sur le disque.

Intégration à WMI

Kaspersky Embedded Systems Security prend en charge l'intégration à l'infrastructure de gestion Windows (WMI) : vous pouvez utiliser les systèmes clients qui emploient WMI pour recevoir les données via la norme Web-Based Enterprise Management (WBEM) afin d'obtenir des informations sur l'état de Kaspersky Embedded Systems Security et de ses composants.

Une fois installé, Kaspersky Embedded Systems Security enregistre un module exclusif dans le système afin de créer un espace de noms Kaspersky Embedded Systems Security sur le périphérique protégé. Un espace de noms Kaspersky Embedded Systems Security vous permet d'utiliser des catégories et des instances Kaspersky Embedded Systems Security et leurs propriétés.

Les valeurs de certaines propriétés d'instance dépendent des types de tâche.

Une *tâche non périodique* est une tâche d'application qui n'est pas limitée dans le temps et qui peut être en exécution constante ou arrêtée. Ces tâches n'affichent pas la progression de l'exécution. Les résultats de la tâche sont enregistrés en continu pendant l'exécution de la tâche en tant qu'événements uniques (par exemple, détection d'un objet infecté par une tâche quelconque de Protection en temps réel de l'ordinateur). Ce type de tâche est administré via les stratégies de Kaspersky Security Center.

Une *tâche périodique* est une tâche d'application qui est limitée dans le temps et dont l'état d'avancement est affiché en pour cent. Les résultats de la tâche sont générés quand la tâche est complétée et sont représentés en tant qu'élément unique ou qu'état modifié de l'application (par exemple, mise à jour des bases de l'application terminée, fichiers de configuration créés pour les tâches de création de règles). Plusieurs tâches périodiques du même type peuvent être exécutées simultanément sur un seul appareil protégé (par exemple, trois tâches d'analyse à la demande avec différentes zones d'analyse). Les tâches périodiques peuvent être administrées via Kaspersky Security Center en tant que tâches de groupe.

Si vous créez les requêtes d'espace de noms WMI à l'aide d'outils et si vous recevez les données dynamiques depuis les espaces de noms WMI sur votre réseau d'entreprise, vous pourrez obtenir les informations relatives à l'état actuel de l'application (cf. tableau ci-dessous).

Informations sur l'état de l'application

Propriété de l'instance	Description	Valeurs
ProductName	Nom de l'application installée.	Nom complet de l'application sans le numéro de version.
ProductVersion	Version complète de l'application installée.	Numéro de version de l'application complet, avec le numéro de build.
InstalledPatches	Ensemble des noms affichés pour les correctifs installés.	Liste des correctifs critiques installés pour l'application.
IsLicenseInstalled	État de l'activation de l'application.	État de la clé utilisée pour activer l'application. Valeurs possibles : • False : aucune clé de licence n'a été ajoutée à l'application.

		• True : une clé de licence a été ajoutée à l'application.
LicenseDaysLeft	Affiche le nombre de jours restants avant l'expiration de la licence en cours.	Nombre de jour restants avant l'expiration de la licence en cours; Valeurs non positives possibles : • 0 : licence expirée. • -1 : impossible d'obtenir des informations sur la clé active ou la clé indiquée ne peut être utilisée pour activer l'application (par exemple, elle est bloquée sur la base d'une liste de refus de clés).
AVBasesDatetime	L'horodatage de la version actuelle des bases antivirus.	Date et heure de création des bases antivirus actuelles. Si l'application installée n'utilise pas de bases antivirus, le champ affiche la valeur Pas installé.
IsExploitPreventionEnabled	État du composant Protection contre les exploits.	État du composant Protection contre les exploits. Valeurs possibles : • True : le composant Protection contre les exploits est activé et offre une protection. • False : le composant Protection contre les exploits n'offre aucune protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.
ProtectionTasksRunning	L'ensemble des tâches de protection en cours d'exécution.	Liste des tâches de protection, de contrôle et de surveillance en cours d'exécution. Ce champ doit tenir compte de toutes les tâches non périodiques en cours d'exécution. Si une tâche non périodique est en cours d'exécution, le champ a la valeur "Aucune".
IsAppControlRunning	État de la tâche Contrôle du lancement des applications.	État de la tâche Contrôle du lancement des applications. • True : la tâche Contrôle du lancement des applications est en cours d'exécution. • False : la tâche Contrôle du lancement des applications n'est pas en cours d'exécution ou le composant Contrôle du lancement des applications n'est pas installé.
AppControlMode	Mode de la tâche du Contrôle du lancement des applications.	Description de l'état actuel du composant Contrôle du lancement des applications et du mode sélectionné pour la tâche correspondante.

		Valeurs possibles : • Active : le mode Actif est sélectionné dans les paramètres de la tâche. • Statistiquement seulement : le mode **Statistiques seulement** est sélectionné dans les paramètres de la tâche. • Not installed : le composant Contrôle du lancement des applications n'est pas installé.
AppControlRulesNumber	Nombre total de règles du contrôle du lancement des applications.	Le nombre de règles actuellement définies dans les paramètres de la tâche Contrôle du lancement des applications.
AppControlLastBlocking	L'horodatage de la dernière interdiction de lancement d'une application par la tâche Contrôle du lancement des applications dans n'importe quel mode.	Date et heure auxquelles le composant Contrôle du lancement des applications a bloqué pour la dernière fois le lancement d'une application. Ce champ reprend toutes les applications bloquées, quel que soit le mode de tâche. Si aucune instance d'interdiction de lancement d'une application n'est enregistré à l'heure du traitement de la requête WMI, la valeur "Aucune" est attribuée au champ.
PeriodicTasksRunning	L'ensemble des tâches de périodiques en cours d'exécution.	Liste des tâches d'analyse à la demande, de mise à jour et d'inventaire en cours d'exécution. Ce champ doit contenir toutes les tâches périodiques en cours d'exécution. Si aucune tâche périodique n'est en cours d'exécution, la valeur "Aucune" est attribuée au champ.
ConnectionState	État de la connexion entre le composant WMI Provider et le service Kaspersky Security (KAVFS).	Informations relatives à l'état de la connexion entre le composant WMI Provider et le service Kaspersky Security. Valeurs possibles : • Success : la connexion a été établie : le client WMI peut recevoir l'état de l'application. • Failed. Code erreur : <code> - impossible d'établir la connexion en raison de l'erreur portant le code indiqué.

Ces données représentent les propriétés de l'instance KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security où :

- KasperskySecurity_ProductInfo est le nom de la classe Kaspersky Embedded Systems Security class
- .ProductName=Kaspersky Embedded Systems Security désigne les propriétés de la clé de Kaspersky Embedded Systems Security

L'instance est créée dans l'espace de noms ROOT\Kaspersky\Security.

Utilisation de Kaspersky Embedded Systems Security depuis la ligne de commande

Cette section décrit l'utilisation de Kaspersky Embedded Systems Security via la ligne de commande.

Commandes

Vous pouvez exécuter les commandes de gestion de base de Kaspersky Embedded Systems Security à partir de la ligne de commande de l'appareil protégé à l'aide du composant Utilitaire de la ligne de commande inclus dans le groupe de composants logiciels de Kaspersky Embedded Systems Security.

La ligne de commande permet d'administrer uniquement les fonctions auxquelles vous avez accès selon vos privilèges dans Kaspersky Embedded Systems Security.

Certaines commandes de Kaspersky Embedded Systems Security sont exécutées les modes suivants :

- Mode synchrone : le contrôle revient à la console uniquement après la fin de l'exécution de la commande.
- Mode asynchrone : le contrôle revient à la console directement après le lancement de la commande.

Pour interrompre l'exécution d'une commande en mode synchrone,

appuyez sur la combinaison de touches **Ctrl+C**.

Respectez les règles suivantes lors de la saisie des instructions de Kaspersky Embedded Systems Security :

- Saisissez les paramètres et les instructions en majuscules ou en minuscules.
- Séparez les modificateurs par un espace.
- Si le chemin d'accès d'un fichier/dossier indiqué en tant que valeur contient un espace, saisissez ce chemin entre guillemets, par exemple : `"C:\TEST\test cpp.exe"`.
- Si nécessaire, vous pouvez utiliser des caractères génériques dans le nom de fichier ou le chemin, par exemple : « `C:\Temp\Temp*\` », « `C:\Temp\Temp???. Doc` », « `C:\Temp\Temp*. doc` ».

La ligne de commande vous permet d'effectuer toutes les opérations de gestion et d'administration de Kaspersky Embedded Systems Security (cf. tableau ci-dessous).

Commandes de Kaspersky Embedded Systems Security

Instruction	Description
KAVSHELL APPCONTROL	Mettez à jour la liste des règles en fonction de la règle d'importation sélectionnée.
KAVSHELL APPCONTROL /CONFIG	Définit les modes de fonctionnement de la tâche Contrôle du lancement des applications.
KAVSHELL APPCONTROL /GENERATE	Lance la tâche Génération des règles du Contrôle du lancement des applications.
KAVSHELL	Défragmente les fichiers journaux de Kaspersky Embedded Systems Security.

VACUUM	
KAVSHELL PASSWORD	Administre les paramètres de la protection par mot de passe.
KAVSHELL HELP	Affiche l'aide sur les commandes de Kaspersky Embedded Systems Security.
KAVSHELL START	Lancement du service Kaspersky Security.
KAVSHELL STOP	Arrêt du service Kaspersky Security.
KAVSHELL SCAN	Crée et lance une tâche d'analyse à la demande temporaire dont la zone d'analyse et les paramètres de sécurité sont définis par les arguments de la commande.
KAVSHELL SCANCRITICAL	Lance la tâche locale du système Analyse rapide.
KAVSHELL TASK	Lance, suspend/relance, arrête la tâche indiquée en mode asynchrone/renvoie l'état actuel de la tâche/les statistiques de la tâche.
KAVSHELL RTP	Lance ou arrête toutes les tâches de protection en temps réel de l'ordinateur.
KAVSHELL UPDATE	Lancez la tâche de mise à jour des bases de l'application selon les paramètres définis par les options de la ligne de commande.
KAVSHELL ROLLBACK	Remet les bases à l'état antérieur à la mise à jour.
KAVSHELL LICENSE	Ajoute ou supprime les clés. Affiche les informations relatives aux clés ajoutées.
KAVSHELL TRACE	Activer ou désactiver le traçage. Administrer les paramètres de traçage.
KAVSHELL DUMP	Active ou désactive la création de fichiers dump en cas d'arrêt anormal des processus de Kaspersky Embedded Systems Security.
KAVSHELL IMPORT	Importe les paramètres généraux de Kaspersky Embedded Systems Security, les paramètres de ses fonctions et de ses tâches depuis un fichier de configuration.
KAVSHELL EXPORT	Exporte tous les paramètres de Kaspersky Embedded Systems Security et des tâches existantes dans un fichier de configuration.
KAVSHELL DEVCONTROL	Enrichit la liste des règles du Contrôle des périphériques créées conformément au principe d'ajout sélectionné.

Affichage de l'aide sur les commandes de Kaspersky Embedded Systems Security : KAVSHELL HELP

Pour consulter a liste de toutes les instructions de Kaspersky Embedded Systems Security, exécutez une des commandes suivantes :

```
KAVSHELL
```

```
KAVSHELL HELP
```

```
KAVSHELL /?
```

Pour obtenir la description et la syntaxe d'une commande, exécutez une des commandes suivantes :

```
KAVSHELL HELP <instruction>
```

```
KAVSHELL <instruction> /?
```

Exemples pour KAVSHELL HELP

Pour consulter des informations plus détaillées sur l'instruction KAVSHELL SCAN, exécutez l'instruction suivante :

```
KAVSHELL HELP SCAN
```

Lancement et arrêt du Service Kaspersky Security KAVSHELL START : KAVSHELL STOP

Pour exécuter le Service Kaspersky Security, exécutez la commande :

```
KAVSHELL START
```

Le lancement du Service Kaspersky Security s'accompagne par défaut du lancement des tâches Protection des fichiers en temps réel et Analyse au démarrage du système d'exploitation ainsi que d'autres tâches planifiées pour démarrer **Au lancement de l'application**.

Pour arrêter le Service Kaspersky Security, exécutez la commande :

```
KAVSHELL STOP
```

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Analyse d'une zone sélectionnée : KAVSHELL SCAN

Pour lancer la tâche d'analyse de secteurs définis de l'appareil protégé, utilisez la commande `KAVSHELL SCAN`. Les arguments de cette commande définissent les paramètres de la zone d'analyse et les paramètres de sécurité du nœud sélectionné.

Une tâche d'analyse à la demande lancée à l'aide de l'instruction `KAVSHELL SCAN` est temporaire. Elle apparaît dans la console de l'application uniquement pendant son exécution (la console de l'application ne vous permet pas de consulter les paramètres de la tâche). Toutefois, un journal de performance de la tâche est généré et affiché dans le nœud **Journaux d'exécution de la tâche** dans la Console de l'application.

Vous pouvez employer une variable d'environnement pour désigner le chemin dans la tâche d'analyse de zones distinctes. Si vous utilisez une variable d'environnement utilisateur, exécuter la commande `KAVSHELL SCAN` sous l'utilisateur correspondant.

La commande `KAVSHELL SCAN` est exécutée en mode synchrone.

Pour lancer une tâche d'analyse à la demande existante via la ligne de commande, utilisez la commande KAVSHELL TASK.

Syntaxe de la commande KAVSHELL SCAN

```
KAVSHELL SCAN <zone d'analyse> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:< nom du fichier contenant la liste des zones d'analyse >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"masque">] [/ES:<taille>] [/ET:<nombre de
secondes>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<nom du fichier
journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction KAVSHELL SCAN contient des paramètres/options obligatoires et facultatifs (cf. tableau ci-dessous).

Exemples d'instruction KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log

KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Options/paramètres de la commande `KAVSHELL SCAN`

Paramètre/option	Description
Zone d'analyse. Paramètre obligatoire.	
<fichiers>	Zone d'analyse : liste de fichiers, de répertoires, de chemins de réseau et de zones prédéfinies. Définissez les chemins d'accès de réseau au format Universal Naming Convention (UNC). Dans l'exemple suivant, le dossier Folder4 est renseigné sans un chemin d'accès, ce qui signifie qu'il se trouve dans le dossier depuis lequel la commande KAVSHELL est exécutée : KAVSHELL SCAN Folder4 Si le nom de l'objet à analyser contient des espaces, il faudra l'indiquer entre guillemets. Si un dossier est renseigné, Kaspersky Embedded Systems Security analyse également l'ensemble de ses sous-dossiers. Pour analyser un groupe de fichiers, vous pouvez utiliser les caractères * ou ?
<répertoires>	
<chemin de réseau>	
/MEMORY	Analyse les objets dans la mémoire vive.
/SHARED	Analyse les dossiers partagés sur l'appareil protégé
/STARTUP	Analyse les objets de démarrage
/REMDRIVES	Analyse les disques amovibles.
/FIXDRIVES	Analyse les disques durs.
/MYCOMP	Analyse tous les secteurs de l'appareil protégé.
/L: <chemin du fichier contenant la liste des zones d'analyse>	Chemin d'accès complet au fichier contenant la liste des zones d'analyse. Utilisez un retour à la ligne pour séparer les zones d'analyse dans le fichier. Vous pouvez renseigner les zones d'analyse prédéfinies comme illustré dans l'exemple suivant de contenu d'un fichier contenant une liste de zones d'analyse : C:\

	D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Analyser les objets (Types de fichier). Si vous ne définissez aucune valeur pour cette option, Kaspersky Embedded Systems Security analyse les objets en fonction du format.	
/FA	Analyse tous les objets
/FC	Analyse les objets en fonction du format (par défaut). Kaspersky Embedded Systems Security analyse uniquement les objets dont le format figure dans la liste des formats des objets infectables.
/FE	Analyse les objets en fonction de l'extension. Kaspersky Embedded Systems Security analyse uniquement les objets dont l'extension figure dans la liste des extensions des objets infectables.
/NEWONLY	Analyser uniquement les nouveaux fichiers et les fichiers modifiés. Si vous n'utilisez pas cette option, Kaspersky Embedded Systems Security analyse tous les objets.
Actions à exécuter sur les objets infectés et autres. Si vous ne définissez aucune valeur pour cet argument, Kaspersky Embedded Systems Security applique l'action **Ignorer**.	
DISINFECT	Désinfecter, ignorer si la désinfection est impossible Les options DISINFECT et DELETE ont été maintenues dans la version actuelle de Kaspersky Embedded Systems Security pour garantir la compatibilité avec les versions antérieures. Ces options peuvent être utilisés à la place des options /AI et /AS. Dans ce cas, Kaspersky Embedded Systems Security ne traitera pas les objets probablement infectés.
DISINFDEL	Désinfecter, supprimer si la désinfection est impossible
DELETE	Supprimer Les options DISINFECT et DELETE ont été maintenues dans la version actuelle de Kaspersky Embedded Systems Security pour garantir la compatibilité avec les versions antérieures. Ces options peuvent être utilisés à la place des options /AI et /AS. Dans ce cas, Kaspersky Embedded Systems Security ne traitera pas les objets probablement infectés.
REPORT	Envoie un rapport (par défaut)
AUTO	Exécuter l'action recommandée
Actions à exécuter sur les objets probablement infectés. Si vous ne définissez aucune valeur pour cette option, Kaspersky Embedded Systems Security applique l'action **Ignorer**.	
QUARANTAINE	Quarantaine
DELETE	Supprimer
REPORT	Envoie un rapport (par défaut)
AUTO	Exécuter l'action recommandée
Exclusions	
/E:ABMSPO	Excluez les types suivants d'objets composés : A : archives SFX ; B : bases de données d'emails ; M : message de texte plat ;

	S : archives (y compris les archives SFX) ; P : objets compactés ; O : objets OLE intégrés.
/EM:<"masks">	Exclut les fichiers en fonction du masque. Vous pouvez définir plusieurs masques, par exemple : `EM: "*. Txt; * .png; C\Videos\*. Avi"`.
/ET:<nombre de secondes>	Arrête le traitement de l'objet s'il dure plus longtemps que la durée indiquée en secondes. Par défaut, il n'y a aucune restriction de temps.
/ES:<taille>	Exclut de l'analyse les objets composés dont la taille, en mégaoctets, dépasse la valeur de l'argument <taille>. Par défaut, Kaspersky Embedded Systems Security analyse les objets de toute taille.
/TZOFF	Annule les exclusions de la zone de confiance.
Paramètres avancés (Options)	
/NOICHECKER	Désactive l'utilisation de la technologie iChecker (activée par défaut).
/NOISWIFT	Désactive l'utilisation de la technologie iSwift (activée par défaut).
/ANALYZERLEVEL:<niveau de l'analyse heuristique>	Activation de l'utilisation de l'analyse heuristique et configuration du niveau d'analyse. Les niveaux d'analyse heuristique suivants sont disponibles : 1 – superficielle 2 – moyenne 3 – minutieuse. Si vous n'utilisez pas cette option, Kaspersky Embedded Systems Security n'utilise pas l'analyse heuristique.
/ALIAS:<nom alternatif de la tâche>	Attribue un nom temporaire à une tâche d'analyse à la demande, ce qui permet d'y faire référence pendant son exécution, par exemple, pour voir ses statistiques à l'aide de la commande TÂCHE. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants de Kaspersky Embedded Systems Security. Si cette option n'est pas définie, la tâche reçoit le nom temporaire scan_<kavshell_pid>, par exemple scan_1234. Dans la Console de l'application, la tâche reçoit le nom Analyser les objets (<date et heure>), par exemple, Analyser les objets 16/8/2007 5:13:14 PM.
Paramètres du journal d'exécution de la tâche (paramètres de Rapport)	
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez ce paramètre, Kaspersky Embedded Systems Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par le paramètre. Le fichier journal contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution de la tâche et le journal des événements de Kaspersky Embedded Systems Security dans la console « Observateur d'événements ». Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.

	Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud Journaux d'exécution de la tâche de la console de l'application. Si Kaspersky Embedded Systems Security ne parvient pas à créer le fichier journal, il affiche un message d'erreur, mais exécute malgré tout la commande.
/ANSI	Cette option utilise le codage ANSI pour enregistrer les événements dans le journal d'exécution de la tâche. L'option ANSI ne sera pas appliquée, si le paramètre W n'est pas défini. Si l'option ANSI n'est pas définie, UNICODE intervient dans la création du journal d'exécution de la tâche.

Lancement de la tâche Analyse rapide : KAVSHELL SCANCRITICAL

Utilisez la commande `KAVSHELL SCANCRITICAL` pour lancer la tâche Analyse rapide selon les paramètres définis dans la console de l'application.

Syntaxe de la commande KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<nom du fichier journal d'exécution de la tâche>]
```

Exemples d'instruction KAVSHELL SCANCRITICAL

Pour exécuter la tâche Analyse rapide et enregistrer le journal d'exécution de la tâche dans le fichier scancritical.log dans le répertoire en cours, exécutez la commande suivante :

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Vous pouvez utiliser le paramètre /W pour configurer l'emplacement du journal d'exécution de la tâche (cf. tableau ci-dessous).

Syntaxe du paramètre `/W` de la commande `KAVSHELL SCANCRITICAL`

Paramètre/option	Description
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez ce paramètre, Kaspersky Embedded Systems Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par le paramètre. Le fichier journal contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution de la tâche et le journal des événements de Kaspersky Embedded Systems Security dans la console « Observateur d'événements ». Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande.

	Le journal est affiché dans le nœud **Journaux d'exécution de la tâche** de la console de l'application. Si Kaspersky Embedded Systems Security ne parvient pas à créer le fichier journal, il affiche un message d'erreur, mais exécute malgré tout la commande.

Administration asynchrone des tâches : KAVSHELL TASK

La commande `KAVSHELL TASK` permet d'administrer la tâche indiquée : lancer, suspendre, reprendre ou arrêter la tâche ainsi que consulter son état actuel et ses statistiques. L'instruction est exécutée en monde asynchrone.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL TASK

```
KAVSHELL TASK [<nom alternatif de la tâche> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Exemples d'instruction KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

La commande `KAVSHELL TASK` peut être exécutée sans paramètres/options ou avec un ou plusieurs des paramètres/options (cf. tableau ci-après).

Options/paramètres de la commande KAVSHELL TASK

Paramètre/option	Description
Pas de paramètres	Renvoie la liste de toutes les tâches existantes de Kaspersky Embedded Systems Security. La liste contient les champs suivants : alias de la tâche, catégorie de tâche (système ou définie par l'utilisateur) et l'état actuel de la tâche.
<nom alternatif de la tâche>	Au lieu du nom de la tâche dans la commande SCAN TASK, utilisez son nom alternatif : bref nom complémentaire attribué aux tâches par Kaspersky Embedded Systems Security. Pour consulter les noms alternatifs des tâches dans Kaspersky Embedded Systems Security, saisissez la commande KAVSHELL TASK sans paramètre.
/START	Lance la tâche indiquée en mode asynchrone.
/STOP	Arrête la tâche indiquée.
/PAUSE	Suspend la tâche indiquée.
/RESUME	Relance la tâche indiquée en mode asynchrone.

/STATE	Récupère l'état actuel de la tâche (par exemple, *Exécution en cours*, *Complétée*, *En pause*, *Arrêtée*, *Échec*, *Lancement en cours*, *Reprise en cours*).
/STATISTICS	Récupère les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche.

Sachez que certaines tâches de Kaspersky Embedded Systems Security ne prennent pas complètement en charge les clés /PAUSE, /RESUME et /STATE.

Codes de retour de l'instruction KAVSHELL TASK.

Suppression de l'attribut PPL : KAVSHELL CONFIG

La commande `KAVSHELL CONFIG` vous permet de supprimer l'attribut PPL (Protected Process Light) pour le Service Kaspersky Security à l'aide du pilote ELAM installé lors de l'installation de l'application.

Syntaxe de la commande KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

Options/paramètres de la commande KAVSHELL CONFIG

Paramètre/option	Description
/PPL:OFF	Supprime l'attribut PPL pour le service Kaspersky Security.

Lancement et arrêt des tâches de protection en temps réel de l'ordinateur : KAVSHELL RTP

La commande `KAVSHELL RTP` vous permet de lancer ou d'arrêter toutes les tâches de protection en temps réel de l'ordinateur.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Exemples d'instruction KAVSHELL RTP

Pour lancer toutes les tâches de protection en temps réel de l'ordinateur, exécutez la commande suivante :

```
KAVSHELL RTP /START
```

La commande `KAVSHELL RTP` peut inclure n'importe laquelle des deux options (cf. tableau ci-dessous).

Options/paramètres de la commande KAVSHELL RTP

Paramètre/options	Description
/START	Lance toute les tâches de protection en temps réel de l'ordinateur : Protection des fichiers en temps réel et Utilisation du KSN.
/STOP	Arrête toutes les tâches de protection en temps réel de l'ordinateur.

Administration de la tâche Contrôle du lancement des applications : KAVSHELL APPCONTROL /CONFIG

A l'aide de la commande `KAVSHELL APPCONTROL/CONFIG`, vous pouvez configurer le mode de fonctionnement de la tâche Contrôle du lancement des applications et contrôle du chargement des modules DLL.

Syntaxe de la commande KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<chemin d'accès complet au fichier XML>
```

Exemples de commande KAVSHELL APPCONTROL /CONFIG

*Pour exécuter la tâche Contrôle du lancement des applications sous le mode **Actif** sans contrôle du chargement du module DLL et enregistrer les paramètres de la tâche à la fin, exécutez la commande :*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Vous pouvez configurer les paramètres de la tâche le Contrôle du lancement des applications à l'aide de clés (cf. tableau ci-dessous).

Options/paramètres de la commande `KAVSHELL APPCONTROL /CONFIG`

Paramètre/option	Description
`/mode:<applyrules|statistics>`	Mode de fonctionnement de la tâche Contrôle du lancement des applications. Vous avez le choix entre les modes suivants de fonctionnement de la tâche : • actif : appliquer les règles du Contrôle du lancement des applications ; • statistics : génère uniquement des statistiques.
`/dll:<no|yes>`	Désactiver ou activer le contrôle du chargement des modules DLL.
`/savetofile: <chemin d'accès complet au fichier XML>`	Exporte les règles précisées dans le fichier indiqué au format XML.
`/savetofile: <nom complet du fichier XML>`	Enregistrez la liste des règles dans un fichier.
`/savetofile: <nom complet du fichier`	Enregistrez la liste des règles du contrôle de la

XML> /sdc	distribution des logiciels.
/clearsdc	Supprimez de la liste toutes les règles du contrôle de la distribution des logiciels.

Génération des règles du Contrôle du lancement des applications : KAVSHELL APPCONTROL /GENERATE

La commande KAVSHELL APPCONTROL /GENERATE permet de composer la liste des règles du Contrôle du lancement des applications.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez [/pwd:<mot de passe>].

Syntaxe de la commande KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <chemin d'accès au dossier> | /source:<chemin d'accès au fichier contenant la liste des dossiers> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<utilisateur ou groupe d'utilisateurs>] [/export:<chemin d'accès complet au fichier XML>] [/import:<a|r|m>] [/prefix:<préfixe pour les noms de règles>] [/unique]
```

Exemples de commande KAVSHELL APPCONTROL /GENERATE

Pour créer des règles pour les fichiers des dossiers sélectionnés, exécutez la commande :

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

Pour créer les règles pour les fichiers exécutables de n'importe quelle extension dans le dossier indiqué et enregistrer à la fin de la tâche les règles créées dans le fichier indiqué au format XML, exécutez la commande :

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

Utilisez les paramètres/options de la ligne de commande pour configurer la génération automatique de règles pour la tâche Contrôle du lancement des applications (cf. tableau ci-dessous).

Options/paramètres de la commande KAVSHELL APPCONTROL /GENERATE

Paramètre/option	Description
Zone d'application des règles d'autorisation	
<chemin d'accès au dossier>	Définissez le chemin d'accès au dossier contenant les fichiers exécutables pour lesquels des règles d'autorisation seront créées automatiquement.
/source: <chemin d'accès à la liste des dossiers>	Définissez le chemin d'accès au fichier TXT reprenant une liste de dossiers contenant les fichiers exécutables pour lesquels des règles d'autorisation seront créées automatiquement.
/masks: <edms>	Définissez les extensions des fichiers exécutables pour lesquels des règles d'autorisation seront créées automatiquement.

	Vous pouvez inclure dans la zone d'application des règles les extensions suivantes : • e - fichiers portant l'extension exe ; • d - fichiers portant l'extension dll ; • m - fichiers portant l'extension msi ; • s - scripts.
/runapp	Lors de la génération de règles d'autorisation, tenez compte des applications en cours d'exécution sur l'appareil protégé.
Actions lors de la génération automatique de règles d'autorisation	
/rules: <ch|cp|h>	Définissez les actions à réaliser lors de la création des règles d'autorisation pour la tâche Contrôle du lancement des applications : • ch – utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser le hash SHA256. • cp – utiliser le certificat numérique. En cas d'absence de certificat, utiliser la valeur du chemin d'accès au fichier exécutable. • h – utiliser le hash SHA256.
/strong	Utiliser l'en-tête et l'empreinte du certificat numérique lors de la création automatique des règles d'autorisation pour la tâche Contrôle du lancement des applications. La commande est exécutée si le paramètre /rules: <ch|cp> a été défini.
/user: <utilisateur ou groupe d'utilisateurs>	Indiquer le nom d'utilisateur ou du groupe d'utilisateurs auxquels la règle sera appliquée. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini.
Actions à réaliser à la fin de la tâche Génération des règles du Contrôle du lancement des applications	
/export: <chemin d'accès au fichier XML>	Enregistrez les règles créées dans un fichier XML.
/unique	Ajouter des informations relatives à l'appareil protégé doté des applications qui servent à créer les règles d'autorisation du Contrôle du lancement des applications.
/prefix: <préfixe pour les noms de règle>	Définissez un préfixe pour les noms des règles d'autorisation du Contrôle du lancement des applications.
/import: <a|r|m>	Importez les règles créées dans la liste indiquée de règles du Contrôle du lancement des applications en fonction de la règle d'importation sélectionnée : • a - **Ajouter aux règles existantes** (les règles identiques apparaissent en double) ; • r - **Remplacer les règles existantes** (les nouvelles règles remplacent les règles définies) ; • m - **Fusionner avec les règles existantes** (les nouvelles règles dont les paramètres ne correspondent pas aux paramètres des règles déjà créées sont ajoutées).

Enrichissement de la liste des règles du Contrôle du lancement des applications : KAVSHELL APPCONTROL

La commande `KAVSHELL APPCONTROL` permet d'ajouter des règles depuis un fichier XML à la liste des règles de la tâche Contrôle du lancement des applications conformément au principe choisi et de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin
d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

Exemples d'instruction KAVSHELL APPCONTROL

Pour ajouter des règles depuis un fichier au format XML aux règles définies du contrôle du lancement des applications selon le principe Ajouter aux règles existantes, procédez comme suit :

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Vous pouvez utiliser les paramètres de la ligne de commande pour sélectionner le principe d'ajout de nouvelles règles depuis le fichier XML indiqué à la liste définie de règles du Contrôle du lancement des applications (cf. tableau ci-dessous).

Options/paramètres de la commande `KAVSHELL APPCONTROL`

Paramètre/option	Description
/append <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle du lancement des applications sur la base du fichier XML indiqué. Règle d'importation - **Ajouter aux règles existantes** (les règles identiques apparaissent en double).
/replace <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle du lancement des applications sur la base du fichier XML indiqué. Règle d'importation - **Remplacer les règles existantes** (les nouvelles règles remplacent les règles définies).
/merge <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle du lancement des applications sur la base du fichier XML indiqué. Règle d'importation - **Fusionner avec les règles existantes** (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
/clear	Purger la liste des règles du Contrôle du lancement des applications.

Enrichissement de la liste des règles du Contrôle des périphériques depuis un fichier : KAVSHELL DEVCONTROL

La commande `KAVSHELL DEVCONTROL` permet d'ajouter des règles depuis un fichier XML à la liste des règles de la tâche Contrôle des périphériques conformément au principe choisi et de supprimer toutes les règles définies de la liste.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <chemin d'accès complet au fichier XML> | /replace <chemin d'accès complet au fichier XML> | /merge <chemin d'accès complet au fichier XML> | /clear
```

Exemples d'instruction KAVSHELL DEVCONTROL

Pour ajouter des règles depuis un fichier XML aux règles existantes de la tâche Contrôle des périphériques en fonction de la règle d'importation Ajouter aux règles existantes, exécutez la commande suivante :

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Vous pouvez utiliser les paramètres de la ligne de commande pour sélectionner la règle d'importation à utiliser pour ajouter de nouvelles règles depuis le fichier XML indiqué à la liste définie de règles du Contrôle des périphériques (cf. tableau ci-dessous).

Options/paramètres de la commande `KAVSHELL DEVCONTROL`

Clé	Description
/append <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle des périphériques sur la base du fichier XML indiqué. Règle d'importation - **Ajouter aux règles existantes** (les règles identiques apparaissent en double).
/replace <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle des périphériques sur la base du fichier XML indiqué. Règle d'importation - **Remplacer les règles existantes** (les règles possédant des paramètres identiques ne sont pas ajoutées, la règle est ajouté si un moins un paramètre est unique).
/merge <chemin d'accès complet au fichier XML>	Met à jour la liste des règles du Contrôle des périphériques sur la base du fichier XML indiqué. Règle d'importation - **Fusionner avec les règles existantes** (les nouvelles règles identiques aux règles déjà définies ne sont pas ajoutées).
/clear	Purger la liste des règles du Contrôle des périphériques.

Lancement de la tâche Mise à jour des bases de l'application : KAVSHELL UPDATE

La commande KAVSHELL UPDATE vous permet de lancer la tâche de mise à jour des bases de Kaspersky Embedded Systems Security en mode synchrone.

Une tâche de mise à jour des bases de l'application lancée à l'aide de la commande KAVSHELL UPDATE est une tâche temporaire. Elle est affichée dans la console de l'application uniquement pendant son exécution. Toutefois, un journal d'exécution de la tâche est généré et affiché dans les **Journaux d'exécution de la tâche** dans la Console de l'application. Les stratégies de Kaspersky Security Center peuvent s'appliquer aux tâches de mise à jour créées et lancées via la commande KAVSHELL UPDATE, ainsi qu'aux tâches de mises à jour créées dans la console de l'application. Pour obtenir des informations sur l'utilisation de Kaspersky Security Center pour administrer Kaspersky Embedded Systems Security sur les périphériques protégés, consultez la section « Administration de Kaspersky Embedded Systems Security via Kaspersky Security Center ».

Vous pouvez utiliser des variables d'environnement pour indiquer la source des mises à jour dans cette tâche. En cas d'utilisation d'une variable d'environnement utilisateur, exécutez la commande KAVSHELL UPDATE sous l'utilisateur correspondant.

Syntaxe de la commande KAVSHELL UPDATE

```
KAVSHELL UPDATE < Source de la mise à jour | /AK | /KL> [/NOUSEKL] [/PROXY:<adresse>:
<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nom d'utilisateur>] [/PROXYPWD:<mot de passe>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/REG:<code iso3166>] [/W:<nom du
fichier journal d'exécution de la tâche>] [/ALIAS:<nom alternatif de la tâche>]
```

L'instruction KAVSHELL UPDATE contient des paramètres/options obligatoires et facultatifs (cf. tableau ci-dessous).

Exemples d'instruction KAVSHELL UPDATE

Pour lancer une tâche de mise à jour des bases de l'application définie par l'utilisateur, exécutez la commande suivante :

```
KAVSHELL UPDATE
```

Pour lancer une tâche de mise à jour des bases de l'application dont les fichiers de mise à jour se trouvent dans le dossier \\server\bases, exécutez la commande suivante :

```
KAVSHELL UPDATE \\server\bases
```

Pour lancer une tâche de mise à jour des bases de l'application depuis le serveur FTP ftp://dnl-ru1.kaspersky-labs.com/ et enregistrer tous les événements de la tâche dans le fichier journal c:\update_report.log, exécutez la commande suivante :

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

Pour télécharger les mises à jour des bases de l'application Kaspersky Embedded Systems Security à partir du serveur de mise à jour de Kaspersky, connectez-vous à la source de base de données via un serveur proxy (adresse du serveur proxy : proxy.company.com, port:8080). Pour accéder à l'appareil protégé par authentification NTLM Microsoft Windows avec le nom d'utilisateur : inetuser et le mot de passe : 123456, exécutez la commande suivante :

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

Options/paramètres de la commande KAVSHELL UPDATE

Paramètre/option	Description
Source des mises à jour (paramètre obligatoire). Indiquez une ou plusieurs sources. Kaspersky Embedded Systems Security contactera chacune des sources dans l'ordre de la liste. Séparez les sources par un espace.	
<chemin au format UNC>	Source de mise à jour définie par l'utilisateur. Chemin d'accès au dossier de mise à jour réseau au format UNC.
<URL>	Source de mise à jour définie par l'utilisateur. adresse du serveur FTP ou HTTP sur lequel se trouve le dossier contenant les mises à jour.
<Dossier local>	Source de mise à jour définie par l'utilisateur. Dossier sur l'appareil protégé.
/AK	Utilisez le Serveur d'administration Kaspersky Security Center comme source des mises à jour.
/KL	Utilisez les serveur de mise à jour de Kaspersky en tant que source des mises à jour.
/NOUSEKL	N'utilise pas les serveurs de mise à jour de Kaspersky si les autres sources des mises à jour indiquées sont inaccessibles (utilisés par défaut).
Paramètres du serveur proxy	
/PROXY:<adresse>:<port>	Nom de réseau ou adresse IP du serveur proxy et son port. Si vous ne définissez pas ce paramètre, Kaspersky Embedded Systems Security identifiera automatiquement les paramètres du serveur proxy utilisé dans le réseau local.
/AUTHTYPE:<0-2>	Ce paramètre définit la méthode d'authentification pour l'accès au serveur proxy. Le paramètre peut prendre les valeurs suivantes : **0** : authentification de Microsoft Windows (NTLM-authentication) intégrée ; Kaspersky Embedded Systems Security contactera le serveur proxy sous le compte **Système local** (**SYSTÈME**) ; **1** : authentification de Microsoft Windows (NTLM-authentication) ; Kaspersky Embedded Systems Security contactera le serveur proxy sous le compte dont le nom d'utilisateur et le mot de passe sont définis par les paramètres /PROXYUSER et /PROXYPWD. **2** : authentification selon le nom et le mot de passe de l'utilisateur définis par les paramètres /PROXYUSER et /PROXYPWD (Basic authentication). Si le serveur proxy ne requiert pas l'authentification, il n'est pas nécessaire de définir ce paramètre.
/PROXYUSER:<nom d'utilisateur>	Nom d'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez /AUTHTYPE:0, les options /PROXYUSER:<nom d'utilisateur> et /PROXYPWD:<mot de passe> sont ignorées.
/PROXYPWD:<mot de passe>	Mot de passe de l'utilisateur qui sera utilisé pour accéder au serveur proxy. Si vous définissez /AUTHTYPE:0, les options /PROXYUSER:<nom d'utilisateur> et /PROXYPWD:<mot de passe> sont ignorées. Si le paramètre /PROXYUSER est défini et si le paramètre /PROXYPWD est oublié, le mot de passe sera considéré comme une chaîne vide.
/NOPROXYFORKL	N'utilise pas les paramètres de proxy désignés pour se connecter aux serveurs de mise à jour de Kaspersky (utilisés par défaut).
/USEPROXYFORCUSTOM	Utilise les paramètres du serveur proxy pour la connexion aux sources de mises à jour définies par l'utilisateur (non utilisées par défaut).
/USEPROXYFORLOCAL	Utilise les paramètres du serveur proxy pour la connexion aux sources locales des mises à jour. Si cette option n'est pas indiquée, la valeur **Ne pas utiliser le serveur proxy pour les adresses locales** est appliquée.
Paramètres généraux du serveur FTP ou HTTP	

/NOFTPPASSIVE	Si vous spécifiez cette clé, Kaspersky Embedded Systems Security utilisera le mode actif du serveur FTP pour se connecter au périphérique protégé. Si vous ne définissez pas cet argument, Kaspersky Embedded Systems Security utilisera le mode de serveur FTP passif si cela est possible.
/TIMEOUT:<nombre de secondes>	Délai d'attente lors de la connexion au serveur FTP ou HTTP. Si vous ne définissez pas ce paramètre, Kaspersky Embedded Systems Security utilisera la valeur par défaut de 10 secondes. La valeur doit être un nombre entier.
/REG:<code iso3166>	Paramètres régionaux. Ce paramètre intervient lors de la réception des mises à jour depuis les serveurs de mise à jour de Kaspersky. Kaspersky Embedded Systems Security réduit la charge du périphérique protégé en choisissant le serveur de mises à jour le plus proche. La valeur de ce paramètre doit être le code ISO 3166-1 alpha-2 du pays où se trouve l'appareil protégé, par exemple /REG: gr ou /REG:US. Si vous ignorez cette clé ou si vous indiquez un code de pays incorrect, Kaspersky Embedded Systems Security identifiera l'emplacement du périphérique protégé à l'aide des paramètres régionaux du périphérique protégé doté de la console de l'application.
/ALIAS:<nom alternatif de la tâche>	Ce paramètre permet d'attribuer un nom temporaire à la tâche afin de pouvoir faire référence à la tâche pendant son exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à la l'aide de la commande TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâche de tous les composants de Kaspersky Embedded Systems Security. Si cet argument n'est pas défini, la tâche reçoit le nom temporaire au format update_<kavshell_pid>, par exemple update_1234. Dans la Console de l'application, la tâche reçoit automatiquement le nom « Update-databases (<date heure>) », par exemple, Update-databases 16/8/2007 5:41:02 PM.
/W:<nom du fichier journal d'exécution de la tâche>	Si vous désignez ce paramètre, Kaspersky Embedded Systems Security enregistre le fichier du journal d'exécution de la tâche et lui donne le nom défini par le paramètre. Le fichier journal contient les statistiques sur l'exécution des tâches, l'heure de lancement et de fin (arrêt) ainsi que sur les événements survenus pendant la tâche. Le journal reprend les événements définis par les paramètres des journaux d'exécution de la tâche et le journal des événements de Kaspersky Embedded Systems Security dans la console « Observateur d'événements ». Vous pouvez indiquer un chemin absolu ou relatif au fichier journal. Si vous indiquez uniquement le nom du fichier sans le chemin d'accès, le fichier journal sera créé dans le répertoire en cours. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant. Vous pouvez consulter le fichier journal durant l'exécution de la tâche d'analyse à la demande. Le journal est affiché dans le nœud **Journaux d'exécution de la tâche** de la console de l'application. Si Kaspersky Embedded Systems Security ne parvient pas à créer le fichier journal, il affiche un message d'erreur, mais exécute malgré tout la commande.

Codes de retour de l'instruction KAVSHELL UPDATE.

Annulation des mises à jour des bases de l'application Kaspersky Embedded Systems Security : KAVSHELL ROLLBACK

La commande `KAVSHELL ROLLBACK` vous permet d'exécuter la tâche locale du système d'annulation de la mise à jour des bases de l'application Kaspersky Embedded Systems Security (rétablissement des bases de Kaspersky Embedded Systems Security à la version installée antérieurement). La commande est exécutée en mode synchrone.

Syntaxe de la commande

```
KAVSHELL ROLLBACK
```

Codes de retour de l'instruction KAVSHELL ROLLBACK

Administration de l'inspection des journaux : KAVSHELL TASK LOG-INSPECTOR

La commande `KAVSHELL TASK LOG-INSPECTOR` permet de surveiller l'intégrité de l'environnement sur la base de l'analyse du journal des événements Windows.

Syntaxe de la commande

```
KAVSHELL TASK LOG-INSPECTOR
```

Exemples de commandes

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Options pour la commande KAVSHELL TASK LOG-INSPECTOR

Option	Description
/START	Lance la tâche indiquée en mode asynchrone.
/STOP	Arrête la tâche indiquée.
/STATE	Récupère l'état actuel de la tâche (par exemple, *Exécution en cours*, *Complétée*, *En pause*, *Arrêtée*, *Échec*, *Lancement en cours*, *Reprise en cours*)
/STATISTICS	Récupère les statistiques de la tâche : renseignements sur le nombre d'objets traités depuis le lancement de la tâche.

Codes de retour de la commande KAVSHELL TASK LOG-INSPECTOR.

Activation de l'application : KAVSHELL LICENSE

La commande `KAVSHELL LICENSE` permet de gérer les clés et les codes d'activation de Kaspersky Embedded Systems Security.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<fichier clé | code d'activation> [/R] | /DEL:<clé | numéro du code d'activation>]
```

Exemples d'instruction KAVSHELL LICENSE

Pour activer l'application, exécutez la commande :

```
KAVSHELL.EXE LICENSE / ADD: <code d'activation code ou clé>
```

Pour obtenir les informations sur les clés ajoutées, exécutez l'instruction suivante :

```
KAVSHELL LICENSE
```

Pour supprimer la clé ajoutée avec le numéro de série 0000-000000-00000001, exécutez l'instruction suivante :

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

La commande `KAVSHELL LICENSE` peut être exécutée avec ou sans arguments (cf. tableau ci-dessous).

Options/paramètres de la ligne de commande KAVSHELL LICENSE

Paramètre	Description
Sans argument	L'instruction affiche les informations suivantes sur les clés ajoutées : • Clé. • Type de licence (commerciale). • Durée de validité de la licence associée à la clé. • État de la clé (active ou complémentaire). Si l'état est *, la clé ajoutée est une clé additionnelle.
/ADD:<nom du fichier clé ou code d'activation>	Ajoute la clé à l'aide du fichier ou du code d'activation indiqué. Pour désigner le chemin d'accès au fichier clé, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
/R	Le code d'activation ou la clé /R vient compléter le code d'activation ou la clé /ADD et signale que ce code d'activation ou cette clé est ajouté en tant que clé ou code complémentaire.
/DEL:<clé ou du code d'activation>	Supprime la clé portant le numéro ou le code d'activation indiqués.

Codes de retour de la commande KAVSHELL LICENSE.

Activation, configuration et désactivation d'un journal de traçage : KAVSHELL TRACE

L'instruction `KAVSHELL TRACE` vous permet d'activer ou de désactiver la création d'un journal de traçage pour tous les sous-systèmes de Kaspersky Embedded Systems Security ainsi que de définir le niveau de détail des informations reprises dans le journal.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump en clair.

Syntaxe de la commande KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:< dossier contenant les fichiers journaux de traçage> [/S:<taille maximale du fichier de traçage en mégaoctets>] [/LVL:debug|info|warning|error|critical] [/r:<nombre maximum de fichiers de traçage pour la rotation>] | /OFF>
```

Si le journal de traçage est activé et si vous voulez modifier ses paramètres, saisissez la commande `KAVSHELL TRACE` avec l'option /ON et utilisez les paramètres /S et /LVL pour définir les paramètres du journal de traçage (cf. tableau ci-dessous).

Arguments de la commande KAVSHELL TRACE

Clé	Description
`/ON`	Active la constitution du journal de traçage.
`/F:< dossier contenant les fichiers journaux de traçage>`	Ce paramètre indique le chemin d'accès complet au dossier dans lequel les fichiers journaux de traçage seront conservés (argument obligatoire). Si vous saisissez un chemin d'accès à un répertoire inexistant, le journal ne sera pas créé. Les chemins d'accès aux dossiers sur les lecteurs réseau d'autres appareils protégés ne peuvent pas être précisés. Si le chemin d'accès défini par le paramètre contient un espace, il faut le saisir entre guillemets, par exemple /F:"C:\Trace Folder". Pour désigner le chemin d'accès au dossier contenant les fichiers journaux de traçage, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur
`/S: <taille maximale du fichier journal en mégaoctets>`	Cet argument définit la taille maximale d'un fichier journal de traçage. Dès que la taille du fichier journal atteint la valeur maximale, Kaspersky Embedded Systems Security consigne les informations dans un nouveau fichier ; le fichier journal antérieur est enregistré. Si vous ne définissez pas ce paramètre, la taille maximale d'un fichier journal sera limitée à 50 Mo.
`/LVL:debug|info|warning|error|critical`	Ce paramètre définit le niveau de détail du journal depuis le niveau le plus détaillé (**Toutes les informations de débogage**) où tous les événements sont enregistrés dans le journal jusqu'au niveau minimum (**Événements critiques**) où seuls les événements critiques sont enregistrés. Si vous ne définissez pas cette clé, le journal de trace contiendra les événements correspondant au niveau de détail **Toutes les informations de débogage**.
`/r:< nombre maximum de fichiers de traçage pour la rotation>`	Ce paramètre active la rotation des fichiers de traçage. Si la rotation des fichiers de traçage est activée et que la valeur du paramètre `<nombre maximum de`

	`fichiers de traçage pour la rotation>` est atteint, le fichier le plus ancien est supprimé avant la création d'un nouveau fichier. Valeurs disponibles : de 1 à 999. Si la valeur n'est pas définie, la rotation des fichiers de traçage n'est pas activée et l'application renvoie une erreur.
/OFF	Cette option désactive la constitution du journal de trace.

Exemples d'instruction KAVSHELL TRACE

*Pour activer le journal de trace avec le niveau de détail **Toutes les informations de débogage** et une taille maximale de 200 Mo et enregistrer le fichier journal dans le dossier "C:\Trace Folder", exécutez la commande suivante :*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*Pour activer le journal de trace avec le niveau de détail **Événements importants** et enregistrer le fichier journal dans le dossier "C:\Trace Folder", exécutez la commande :*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

*Pour activer le journal de traçage au niveau de détail **Événements importants** et avec enregistrement du fichier journal dans le dossier « C:\Trace Folder », et pour activer la rotation des fichiers de traçage après qu'un nombre maximum de 50 fichiers de traçage est atteint, exécutez la commande :*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

Pour désactiver le contenu du journal de traçage, exécutez l'instruction suivante :

```
KAVSHELL TRACE OFF
```

Codes de retour de l'instruction KAVSHELL TRACE

Défragmentation des fichiers journaux de Kaspersky Embedded Systems Security : KAVSHELL VACUUM

La commande `KAVSHELL VACUUM` permet de défragmenter les fichiers journaux de l'application. Ceci permet d'éviter les erreurs système et d'application provoquées par le stockage d'un nombre important de fichiers journal contenant les événements de l'application.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Nous conseillons d'appliquer la commande `KAVSHELL VACUUM` pour optimiser le stockage du fichier journal en cas d'exécution fréquente des tâches d'analyse à la demande et de mise à jour. Cette commande amène Kaspersky Embedded Systems Security à mettre à jour la structure logique des fichiers journal de l'application stockés sur un périphérique protégé au chemin indiqué.

Par défaut, les fichiers journaux de l'application sont conservés à l'emplacement "C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.2\Reports". Si vous avez désigné un autre chemin d'accès manuellement pour le stockage des journaux, la commande `KAVSHELL VACUUM` exécute une défragmentation des fichiers dans le dossier que vous aurez désigné dans les paramètres des journaux de Kaspersky Embedded Systems Security.

La taille importante des fichiers augmente la durée de l'opération de défragmentation lancée via la commande `KAVSHELL VACUUM`.

Pendant l'exécution de la commande `KAVSHELL VACUUM`, les tâches Protection en temps réel et de Contrôle de l'ordinateur ne sont pas disponibles. La procédure de défragmentation limite l'accès au journal de Kaspersky Embedded Systems Security et empêche l'enregistrement des événements dans le journal. Pour éviter une réduction de la protection, nous vous conseillons de bien planifier le moment où vous allez exécuter la commande `KAVSHELL VACUUM`.

Pour défragmenter les fichiers journaux créés suite aux événements survenus pendant l'utilisation de Kaspersky Embedded Systems Security, exécutez la commande :

```
KAVSHELL VACUUM
```

Cette commande nécessite des autorisations du compte Système local.

Nettoyage de la base iSwift : KAVSHELL FBRESET

Kaspersky Embedded Systems Security utilise la technologie iSwift qui permet de ne pas devoir analyser à nouveau un fichier si celui-ci n'a pas été modifié depuis l'analyse antérieure (**Utiliser la technologie iSwift**).

Kaspersky Embedded Systems Security crée les fichiers klamfb.dat et klamfb2.dat dans le dossier "%SYSTEMDRIVE%\System Volume Information". Ces fichiers contiennent des informations sur les objets sains qui ont déjà été analysés. Plus le nombre de fichiers différents analysés par Kaspersky Embedded Systems Security est élevé, plus la taille du fichier klamfb.dat (klamfb2.dat) augmente. Ce fichier contient uniquement les informations actuelles sur les fichiers existant dans le système : si un fichier quelconque est supprimé, Kaspersky Embedded Systems Security Server supprime les informations qui le concerne dans le fichier klamfb.dat.

Pour purger un fichier, utilisez la commande `KAVSHELL FBRESET`.

Tenez compte des particularités suivantes de la commande `KAVSHELL FBRESET` :

- En cas d'utilisation de la commande KAVSHELL FBRESET pour effacer le fichier klamfb.dat, Kaspersky Embedded Systems Security ne suspend pas la protection (à la différence de ce qui se passe lors de la suppression manuelle de klamfb.dat).

- Après la purge du fichier klamfb.dat, Kaspersky Embedded Systems Security peut augmenter la charge sur le périphérique protégé. Dans ce cas, Kaspersky Embedded Systems Security analyse tous les fichiers consultés pour la première fois après la suppression de klamfb.dat. Après l'analyse, Kaspersky Embedded Systems Security replace les informations relatives à chaque objet analysé dans klamfb.dat. En cas de nouvelle tentative d'accès à un objet, la technologie iSwift évite la nouvelle analyse d'un fichier si celui-ci n'a pas été modifié.

L'exécution de la commande `KAVSHELL FBRESET` requiert le lancement de l'interpréteur de ligne de commande sous le compte utilisateur SYSTEM.

Activation et désactivation de la création de fichiers dump : KAVSHELL DUMP

La commande `KAVSHELL DUMP` permet d'activer ou de désactiver la création d'instantanés (fichiers dump) des processus de Kaspersky Embedded Systems Security si ceux-ci s'arrêtent de manière anormale (cf. tableau suivant). De plus, vous pouvez créer à tout moment un fichier dump des processus de Kaspersky Embedded Systems Security en exécution.

Pour créer un fichier dump, la commande `KAVSHELL DUMP` doit être lancée sous le compte système local (SYSTEM).

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump en clair.

La commande KAVSHELL DUMP ne peut pas être utilisée pour les processus x64.

Syntaxe de la commande KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<dossier contenant le fichier dump>|/SNAPSHOT /F:<dossier contenant le fichier dump> / P:<pid> | /OFF>
```

Options/paramètres de la commande KAVSHELL DUMP

Clé	Description
/ON	Autorise la création d'un fichier dump en cas d'arrêt anormal d'un processus.
/F:<dossier contenant les fichiers dump>	Ce paramètre est obligatoire. Il indique le chemin d'accès au dossier où le fichier dump sera enregistré. Les chemins d'accès aux dossiers sur les lecteurs réseau d'autres appareils sans protection ne sont pas autorisés. Pour désigner le chemin d'accès au dossier contenant le fichier dump, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.
/SNAPSHOT	Prend un instantané de la mémoire du processus en cours d'exécution avec le PID indiqué et enregistre le fichier dump dans le dossier défini par le paramètre /F.
/P	Identificateur du processus (PID) ; repris dans le gestionnaire des tâches de Microsoft Windows.
/OFF	Désactive la création d'un fichier dump en cas d'arrêt anormal d'un processus.

Codes de retour de l'instruction KAVSHELL DUMP.

Exemples d'instruction KAVSHELL DUMP

Pour activer la création d'un fichier dump ; enregistrer le fichier dump dans le dossier "C:\Dump", exécutez la commande suivante :

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Pour enregistrer une image de la mémoire du processus avec l'identifiant 1234 dans le dossier "C:/Dumps", exécutez l'instruction suivante :

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

Pour désactiver la création de fichiers dump, exécutez la commande suivante :

```
KAVSHELL DUMP OFF
```

Importation des paramètres : KAVSHELL IMPORT

La commande `KAVSHELL IMPORT` permet d'importer les paramètres de Kaspersky Embedded Systems Security, de ses fonctions et de ses tâches depuis un fichier de configuration dans une copie de Kaspersky Embedded Systems Security sur le périphérique protégé. Vous pouvez créer le fichier de configuration à l'aide de l'instruction `KAVSHELL EXPORT`.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL IMPORT

```
KAVSHELL IMPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples d'instruction KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Paramètre de la commande KAVSHELL IMPORT

Paramètre	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration d'où les paramètres vont être importés. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL IMPORT.

Exportation des paramètres : KAVSHELL EXPORT

L'instruction `KAVSHELL EXPORT` permet d'exporter tous les paramètres de Kaspersky Embedded Systems Security et des tâches existantes dans un fichier de configuration afin de pouvoir les importer par la suite dans Kaspersky Embedded Systems Security sur d'autres périphériques protégés.

Syntaxe de la commande KAVSHELL EXPORT

```
KAVSHELL EXPORT <nom du fichier de configuration et chemin d'accès>
```

Exemples d'instruction KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Paramètre de la commande KAVSHELL EXPORT

Paramètre	Description
<nom du fichier de configuration et chemin d'accès>	Nom du fichier de configuration dans lequel les paramètres vont être enregistrés. Vous pouvez attribuer n'importe quelle extension au fichier de configuration. Pour désigner le chemin d'accès au fichier, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

Codes de retour de l'instruction KAVSHELL EXPORT.

Intégration avec Microsoft Operation Management Suite : KAVSHELL OMSINFO

La commande KAVSHELL OMSINFO permet de réviser l'état de l'application et les informations sur les menaces détectées par les bases antivirus et le service KSN. Les données sur les menaces proviennent des journaux des événements disponibles.

Syntaxe de la commande KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <chemin et nom du fichier généré>
```

Exemples d'instruction KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Paramètre de la commande KAVSHELL OMSINFO

Paramètre	Description
<chemin et nom du fichier généré>	Nom du fichier généré qui contient des informations sur l'état de l'application et les menaces détectées.

Gestion de la tâche Surveillance de l'intégrité des fichiers : KAVSHELL FIM/BASELINE

À l'aide de la commande `KAVSHELL FIM /BASELINE`, vous pouvez configurer le mode de fonctionnement de la tâche Surveillance de l'intégrité des fichiers et de contrôle du chargement des modules DLL.

L'exécution de la commande requiert la saisie du mot de passe. Pour saisir le mot de passe actif, utilisez `[/pwd:<mot de passe>]`.

Syntaxe de la commande KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<zone de surveillance> | /L:<chemin d'accès au fichier TXT contenant la liste des zones de surveillance>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<ID de la ligne de référence> | /ALIAS:<alias existant>]] | [/EXPORT:<chemin d'accès au fichier TXT> [/BL:<ID de la ligne de référence> | /ALIAS:<alias existant>]] | [/SHOW [/BL:<ID de la ligne de référence> | /ALIAS:<alias existant>]] | [/SCAN [/BL:<ID de la ligne de référence> | /ALIAS:<alias existant>]] | [/PWD:<mot de passe>]
```

Exemples de commande KAVSHELL FIM /BASELINE

Pour supprimer une ligne de référence, exécutez la commande suivante :

```
KAVSHELL FIM / BASELINE / CLEAR / BL: <ID de la ligne de référence>
```

Vous pouvez configurer les paramètres de la tâche Surveillance de l'intégrité des fichiers à l'aide de clés (cf. tableau ci-dessous).

Options/paramètres de la commande `KAVSHELL FIM/ BASELINE`

Paramètre/option	Description
`/CREATE`	Créez une nouvelle tâche Surveillance de l'intégrité des fichiers. Kaspersky Embedded Systems Security démarre la nouvelle tâche Surveillance de l'intégrité des fichiers afin de créer une ligne de référence.
`/L`	Désignez le chemin d'accès au fichier TXT contenant la liste des zones de surveillance.
`/MD5`	Désignez l'algorithme MD5 pour calculer une somme de contrôle (paramètre facultatif). Le paramètre `/MD5` ne peut pas être utilisé avec `/SHA256`. L'algorithme MD5 est utilisé par défaut.
`/SHA256`	Désignez l'algorithme SHA256 pour calculer une somme de contrôle (paramètre facultatif). Le paramètre `/SHA256` ne peut pas être utilisé avec `/MD5`. L'algorithme MD5 est utilisé par défaut.
`/SF`	Inclut tous les sous-dossiers dans la zone de la tâche Surveillance de l'intégrité des fichiers (paramètre facultatif). Par défaut, tous les sous-dossiers sont exclus de la zone de la tâche Surveillance de l'intégrité des fichiers.
`/CLEAR`	Supprimez la ligne de référence avec `<ID de ligne de référence>` désigné ou la ligne de référence de la tâche avec `<l'alias existant>` désigné. Supprimez toutes les lignes de référence si ni `<ID de la ligne de référence>` ni `<l'alias existant>` n'a été désigné. Paramètre facultatif.
`/BL`	Désignez l'ID unique d'une ligne de référence (paramètre facultatif).
`/EXPORT`	Exportez les données de toutes les lignes de référence dans un

	fichier TXT.
/SHOW	Affichez les données sur toutes les lignes de référence.
/SCAN	Démarrez la nouvelle tâche Surveillance de l'intégrité des fichiers avec <ID de la ligne de référence> ou <l'alias existant> désigné.
/ALIAS	Désignez le nom d'une tâche existante ou le nom d'une nouvelle tâche.
<zone de surveillance>	Désignez le fichier ou le dossier que vous souhaitez inclure dans la zone de la tâche Contrôle de l'intégrité des fichiers. Ce paramètre permet de désigner une seule zone.
<chemin d'accès au fichier TXT contenant la liste des zones de surveillance>	Désignez le chemin d'accès au fichier TXT contenant la liste des zones de surveillance. Le fichier doit être codé en UTF-8 et chaque chemin vers une zone de surveillance doit être désigné dans une ligne séparée.
<chemin d'accès au fichier TXT>	Désignez le chemin d'accès au fichier dans lequel vous souhaitez exporter les données sur toutes les lignes de référence.
<ID de la ligne de référence>	Désignez l'ID unique d'une ligne de référence. Vous pouvez utiliser le paramètre /SHOW pour apprendre l'ID d'une ligne de référence.
<alias existant>	Désignez le nom d'une tâche existante.
<nouvel alias>	Désignez le nom d'une nouvelle tâche.

Codes de retour de la commande

Codes de retour des commandes KAVSHELL START et KAVSHELL STOP

Codes de retour des commandes KAVSHELL START et KAVSHELL STOP

Code de retour	Description
0	L'opération a réussi
-3	Erreur de privilèges d'accès
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (par exemple, le service Kaspersky Security est déjà exécuté ou est déjà arrêté)
-7	Le service n'est pas enregistré
-8	Le lancement automatique du service est désactivé
-9	La tentative de démarrage de l'appareil protégé sous un autre compte utilisateur a échoué (par défaut, le service Kaspersky Security fonctionne sous le compte utilisateur Système local).
-99	Erreur inconnue

Codes de retour des instructions KAVSHELL SCAN et KAVSHELL SCANCRITICAL

Codes de retour des commandes KAVSHELL SCAN et KAVSHELL SCANCRITICAL

Code de retour	Description
0	L'opération a réussi (Aucune menace n'a été découverte)
1	L'opération a été annulée
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le fichier avec la liste des zones d'analyse est introuvable).
-5	Syntaxe de la commande incorrecte ou zone d'analyse non définie.
-80	Objets infectés et autres détectés
-81	Objets probablement infectés détectés
-82	Des erreurs de traitement ont été découvertes
-83	Des objets non analysés ont été découverts
-84	Objets endommagés détectés
-85	Échec de la création d'un journal d'exécution de la tâche
-99	Erreur inconnue
-301	Clé non valide

Codes de retour de la commande KAVSHELL TASK LOG-INSPECTOR

Code de retour de la commande KAVSHELL TASK LOG-INSPECTOR

Code de retour	Description
0	L'opération a réussi
-6	Opération invalide (par exemple, le service Kaspersky Security est déjà exécuté ou est déjà arrêté)
402	La tâche est déjà lancée (pour l'option /STATE)

Codes de retour de l'instruction KAVSHELL TASK

Codes de retour de l'instruction KAVSHELL TASK

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé

-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (la tâche est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (par exemple, la tâche n'est pas lancée, est déjà lancée ou ne peut être arrêtée)
-99	Erreur inconnue
-301	Clé non valide
401	La tâche n'est pas lancée (pour l'option /STATE)
402	La tâche est déjà lancée (pour l'option /STATE)
403	La tâche est déjà arrêtée (pour l'options/STATE)
-404	Échec de l'opération (une modification de l'état de la tâche a provoqué un plantage)

Codes de retour de l'instruction KAVSHELL RTP

Codes de retour de l'instruction KAVSHELL RTP

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	Objet introuvable (une ou plusieurs tâches de Protection en temps réel de l'ordinateur sont introuvables)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (par exemple, la tâche est déjà exécutée ou est déjà arrêtée)
-99	Erreur inconnue
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL UPDATE

Codes de retour de l'instruction KAVSHELL UPDATE

Code de retour	Description
0	L'opération a réussi
200	Tous les objets sont d'actualité (les bases ou les modules logiciels sont d'actualité)
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe de la commande incorrecte
-99	Erreur inconnue

-206	Les fichiers d'extension ne sont pas présents dans la source indiquée ou leur format est inconnu
-209	Erreur de connexion à la source des mises à jour
-232	Erreur d'authentification lors de la connexion au serveur proxy
-234	Erreur de connexion à Kaspersky Security Center
-235	Kaspersky Embedded Systems Security n'a pas subi d'authentification lors de la connexion à la source des mises à jour
-236	Les bases de Kaspersky Embedded Systems Security sont endommagées
-301	Clé non valide

Codes de retour de l'instruction KAVSHELL ROLLBACK

Codes de retour de l'instruction KAVSHELL ROLLBACK

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-99	Erreur inconnue
-221	La copie de sauvegarde des bases est introuvable
-222	La copie de sauvegarde des bases est corrompue

Codes de retour de l'instruction KAVSHELL LICENSE

Codes de retour de l'instruction KAVSHELL LICENSE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Privilèges insuffisants pour l'administration des clés
-4	Clé portant le numéro indiqué introuvable
-5	Syntaxe de la commande incorrecte
-6	Opération incorrecte (la clé a déjà été ajoutée)
-99	Erreur inconnue
-301	Clé non valide
-303	Licence destinée à une autre application

Codes de retour de l'instruction KAVSHELL TRACE

Codes de retour de l'instruction KAVSHELL TRACE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin d'accès indiqué pour le dossier contenant les fichiers journaux de traçage est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération non valide (tentative d'exécution de la commande KAVSHELL TRACE /OFF quand les journaux de trace sont déjà désactivés)
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL FBRESET

Codes de retour de l'instruction KAVSHELL FBRESET

Code de retour	Description
0	L'opération a réussi
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL DUMP

Codes de retour de l'instruction KAVSHELL DUMP

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (le chemin indiqué pour le dossier contenant le fichier dump est introuvable ; le processus avec le PID indiqué est introuvable)
-5	Syntaxe de la commande incorrecte
-6	Opération invalide (tentative d'exécution de la commande KAVSHELL DUMP /OFF si la création des fichiers dump a déjà été désactivée)
-99	Erreur inconnue

Codes de retour de l'instruction KAVSHELL IMPORT

Codes de retour de l'instruction KAVSHELL IMPORT

Code de	Description

retour	
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	Objet introuvable (impossible de trouver un fichier de configuration qui peut être importé)
-5	Syntaxe incorrecte
-99	Erreur inconnue
501	L'opération a réussi, mais avec une erreur/un commentaire, par exemple, Kaspersky Embedded Systems Security n'a pas importé les paramètres d'un composant fonctionnel quelconque
-502	Le format du fichier à importer est inconnu ou le fichier manque
-503	Paramètres incompatibles (le fichier de configuration provient d'une autre application ou d'une version de Kaspersky Embedded Systems Security postérieure ou incompatible)

Codes de retour de l'instruction KAVSHELL EXPORT

Codes de retour de l'instruction KAVSHELL EXPORT

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-5	Syntaxe incorrecte
-10	Impossible de créer le fichier de configuration (par exemple, accès interdit au répertoire indiqué dans le chemin d'accès au fichier)
-99	Erreur inconnue
501	L'opération a réussi, mais avec une erreur/un commentaire, par exemple, Kaspersky Embedded Systems Security n'a pas exporté les paramètres d'un composant fonctionnel quelconque

Codes de retour de la commande KAVSHELL FIM /BASELINE

Codes de retour de la commande KAVSHELL FIM /BASELINE

Code de retour	Description
0	L'opération a réussi
-2	Le service n'est pas lancé
-3	Erreur de privilèges d'accès
-4	L'objet est introuvable (la tâche est introuvable)
-5	Syntaxe de la commande incorrecte

-6	Opération non valide (par exemple, la ligne de référence a déjà été supprimée)
-10	Impossible de créer le fichier de configuration (par exemple, accès interdit au répertoire indiqué dans le chemin d'accès au fichier)
-12	Mot de passe incorrect
-80	Incohérent avec les objets de référence détectés
-85	Échec de la création d'un journal d'exécution de la tâche
-99	Erreur interne
-303	Clé de licence non valide
-502	Tâche non exécutée
200	Tous les objets sont cohérents avec la ligne de référence
501	Tâche terminée avec succès avec une erreur/un commentaire

Contacter le Support Technique

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

Modes d'obtention de l'assistance technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des sources d'informations relatives à l'application, contactez le Support Technique. Les employés du Support Technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Le Support Technique n'est pas proposé aux utilisateurs d'une version d'essai.

La prise en charge des applications est fournie en fonction de leur cycle de vie (voir la page relative au cycle de vie des applications).

Avant de contacter le Support Technique, veuillez lire les règles d'octroi de l'assistance technique.

Vous pouvez contacter le Support Technique en envoyant une requête au Support Technique de Kaspersky via le portail Kaspersky CompanyAccount.

Assistance technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail à disposition des entreprises qui utilisent les applications de Kaspersky. Le portail Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky via des requêtes électroniques. Le portail Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte utilisateur Kaspersky CompanyAccount. À l'aide d'un seul compte, vous pouvez centraliser l'administration des demandes électroniques envoyées par les employés à Kaspersky et gérer les droits d'accès de ces employés à 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.

Utilisation du fichier de trace et du script AVZ

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Embedded Systems Security à envoyer au Support Technique de Kaspersky. Les experts du Support Technique de Kaspersky peuvent également vous demander de créer un fichier de trace. Le fichier de trace permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

L'analyse des données que vous envoyez permet aux experts du Support technique de Kaspersky de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus actifs, de rechercher la présence éventuelle de menaces sur le périphérique protégé, de désinfecter ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

Glossaire

Analyse heuristique

Technologie de détection des menaces dont les informations ne figurent pas encore dans les bases de Kaspersky. L'analyse heuristique permet de détecter des objets dont le comportement dans le système d'exploitation peut constituer une menace pour la sécurité. Les objets identifiés à l'aide de l'analyse heuristique sont considérés comme probablement infectés. Par exemple, un objet qui contient une succession de commandes propres à des objets malveillants (ouverture d'un fichier, écriture dans le fichier) pourrait être considéré comme probablement infecté.

Archive

Un ou plusieurs fichiers repris dans un fichier compressé. Une application dédiée, appelée archiveur, est requise pour le compactage et le décompactage des données.

Bases antivirus

Bases de données qui contiennent les informations relatives aux menaces informatiques connues de Kaspersky au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les bases antivirus sont composées par les experts de Kaspersky et sont mises à jour toutes les heures.

Clé active

Une clé actuellement utilisée par l'application.

Désinfection

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être désinfectés.

Données relatives à la licence ;

Période de temps pendant laquelle vous avez accès aux fonctions de l'application et aux droits d'utiliser des services supplémentaires. Les services utilisables dépendent du type de licence.

État de la protection

État actuel de la protection, qui reflète le niveau de sécurité de l'ordinateur.

Faux positifs

Situation où un objet non infecté est considéré comme infecté par une application de Kaspersky car son code évoque celui d'un virus.

Fichier probablement infectable

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'insertion de code malveillant est assez élevé pour ces fichiers.

Kaspersky Security Network (KSN)

Infrastructure de services cloud donnant accès à la base de données de Kaspersky avec des informations constamment mises à jour sur la réputation des fichiers, les ressources Internet et le logiciel. Kaspersky Security Network assure une vitesse de réaction plus élevée que les applications de Kaspersky face aux nouvelles menaces, augmente l'efficacité de certains composants de la protection et réduit la possibilité de faux positifs.

Masque de fichier

Représentation d'un nom de fichier à l'aide de caractères génériques. Les caractères génériques standard utilisés dans les masques de fichier sont * et ?, où * représente n'importe quel nombre de n'importe quels caractères et ? représente n'importe quel caractère unique.

Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mise à jour de Kaspersky.

Niveau de sécurité

Le niveau de sécurité est décrit comme un ensemble pré-configuré de paramètres de composants de l'application.

Objet OLE

Objet lié à un autre fichier ou imbriqué dans un autre fichier via la technologie Object Linking and Embedding (OLE). Exemple d'objet OLE : feuille de calcul Microsoft Office Excel® imbriquée dans un document Microsoft Office Word.

Objets de démarrage

Ensemble d'applications nécessaires au démarrage et au fonctionnement corrects du système d'exploitation et au logiciel installé sur l'ordinateur. Objets de démarrage : objets que le système d'exploitation charge au démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

Quarantaine

Dossier dans lequel l'application de Kaspersky déplace les objets probablement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

Sauvegarde

Stockage spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur désinfection ou leur suppression.

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction de centralisation des informations relatives aux applications de Kaspersky installées sur le réseau de la société et qui permet de les administrer. Il permet également de gérer ces applications.

SIEM

Technologie qui analyse les événements de sécurité provenant de plusieurs périphériques réseau et applications.

Stratégie

Une stratégie définit les paramètres d'une application et administre la possibilité de configurer cette application sur les ordinateurs au sein d'un groupe d'administration. Une stratégie individuelle doit être créée pour chaque application. Vous pouvez créer plusieurs stratégies pour les applications installées sur les ordinateurs dans chaque groupe d'administration, mais une seule stratégie à la fois peut être appliquée à chaque application dans un groupe d'administration.

Tâche

Les fonctions de l'application de Kaspersky sont mises en œuvre sous la forme de tâches, comme : protection des fichiers en temps réel, Analyse complète de l'ordinateur et Mise à jour des bases de l'application.

Tâche locale

Tâche définie et exécutée sur un ordinateur client unique.

Témoin du niveau d'importance de l'événement

Propriété d'un événement rencontré pendant le fonctionnement d'une application Kaspersky. Il existe les niveaux de gravité suivants :

- Événement critique
- Panne de fonction
- Avertissement
- Info

Les événements du même type peuvent avoir différents niveaux de gravité en fonction de la situation de survenue de l'événement.

Un objet infecté a été découvert

Objet dont une portion de code correspond parfaitement à une partie du code d'une application malveillante connue. Kaspersky ne recommande pas d'accéder à ces objets.

Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs d'applications malveillantes pour pénétrer dans un système ou une application et nuire son intégrité. Un grand nombre de vulnérabilités dans un système rend son fonctionnement peu fiable car les virus, installés dans le système, peuvent entraîner des erreurs du système d'exploitation ou des applications installées.

Information sur le code tiers

Les informations sur le code tiers se trouvent dans le fichier legal_notices.txt, situé dans le dossier d'installation de l'application.

Avis de marques déposées

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Dell Technologies, Dell, EMC, Celerra et VNX et les autres marques commerciales sont des marques commerciales de Dell Inc. ou de ses filiales.

Domino, Lotus et Lotus Notes sont des marques commerciales d'International Business Machines Corporation, déposées dans de nombreuses juridictions dans le monde.

Intel et Pentium sont des marques d'Intel Corporation aux États-Unis et dans d'autres pays.

Linux est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

Microsoft, Active Directory, Forefront, Excel, Hyper-V, Internet Explorer, Lync, Outlook, SharePoint, SQL Server, Windows, Windows Server, Windows Vista, Windows XP sont des marques commerciales du groupe Microsoft.

NetApp est une marque commerciale ou une marque déposée de NetApp, Inc. aux États-Unis et/ou dans d'autres pays.

Schneider Electric est une marque commerciale de Schneider Electric.

Siemens, WinCC et Simatic sont des marques déposées de Siemens AG.

CVE est une marque déposé de The MITRE Corporation.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, licenciée exclusivement via X/Open Company Limited.