KASPERSKY lab

Kaspersky Embedded Systems Security

Manuel de l'utilisateur

Version de l'application : 2.0

Chers utilisateurs !

Nous vous remercions de votre confiance. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Date d'édition : 25/05/2017

https://www.kaspersky.fr
http://support.kaspersky.com/fr

Table des matières

Présentation du guide

Le Manuel de l'utilisateur de Kaspersky Embedded Systems Security 1.6 s'adresse aux spécialistes chargés de l'administration de la Console de Kaspersky Embedded Systems Security sur le périphérique protégé.

Ce guide reprend les informations relatives à la configuration et à l'utilisation de la Console de gestion de Kaspersky Embedded Systems Security.

Dans cette section

Dans ce document

Le Manuel de l'utilisateur de Kaspersky Embedded Systems Security contient les sections suivantes :

Kaspersky Embedded Systems Security

Cette section fournit des informations sur la fonction, les possibilités principales et la composition de l'application.

Interface de Kaspersky Embedded Systems Security

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

Lancement et arrêt de Kaspersky Embedded Systems Security

Cette section fournit des informations sur le lancement de la Console de Kaspersky Embedded Systems Security, ainsi que sur le lancement et l'arrêt du service Kaspersky Security.

Consultation de l'état de la protection et des informations sur Kaspersky Embedded Systems Security

Cette section fournit des informations sur l'état de la protection de l'ordinateur et des informations sur Kaspersky Embedded Systems Security.

Autorisations d'accès aux fonctions de Kaspersky Embedded Systems Security

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Embedded Systems Security et des services Windows® qui enregistrer l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

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 Kaspersky Embedded Systems Security installée sur l'ordinateur protégé ou sur un autre ordinateur.

Configuration de la zone de confiance

Cette section contient des informations sur la zone de confiance de Kaspersky Embedded Systems Security, sur les instructions pour ajouter des objets à la zone de confiance et sur l'application de la zone de confiance aux tâches de Kaspersky Embedded Systems Security.

Gestion des tâches de Kaspersky Embedded Systems Security

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.

Protection en temps réel

Cette section contient les informations sur les tâches de protection en temps réel : Protection des fichiers en temps réel des fichiers et Utilisation du KSN. Elle explique également comment configurer les paramètres des tâches de protection en temps réel et de la sécurité de l'ordinateur protégé.

Contrôle de l'ordinateur

Cette section contient des informations sur la fonction de Kaspersky Embedded Systems Security qui permet de contrôler le lancement des applications, la connexion de disques flash et autres périphériques externes USB. Elle traite également du contrôle du fonctionnement du pare-feu Windows.

Diagnostic du système

Cette section contient des informations sur la tâche de contrôle des opérations sur les fichiers et les possibilités d'inspection du journal système du système d'exploitation.

Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande et explique la configuration des paramètres des tâches d'analyse à la demande ainsi que la configuration des paramètres de la sécurité de l'ordinateur protégé.

Mise à jour des bases de données et des modules de Kaspersky Embedded Systems Security

Cette section présente les tâches de mises à jour des bases de données et des modules logiciels de Kaspersky Embedded Systems Security, la copie des mises à jour des bases 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 des bases de données et des modules de l'application.

L'isolement et les sauvegardes des objets

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur l'isolement des fichiers probablement infectés.

Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security

Cette section contient des informations sur l'utilisation des journaux de Kaspersky Embedded Systems Security : journal d'audit système, journaux d'exécution des tâches de Kaspersky Embedded Systems Security et journal des événements de Kaspersky Embedded Systems Security.

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 serveur, ainsi que les instructions relatives à la configuration des notifications.

Contacter le Support Technique

Cette section explique comment obtenir l'assistance technique et les conditions à remplir pour en profiter.

Glossaire

Cette section reprend les termes utilisés dans ce document et leur définition.

AO Kaspersky Lab

Cette section contient des informations sur AO Kaspersky Lab.

Informations sur le code tiers

Cette section contient des informations sur le code tiers utilisé dans l'application.

Avis de marques déposées

Cette section reprend les marques de commerce citées dans le document et leurs détenteurs respectifs.

Index

Cette section permet de trouver rapidement les informations que vous cherchez dans le document.

Conventions

Ce document utilise des conventions de style (cf. tableau ci-dessous).

Tableau 1. Conventions

Exemple de texte	Description de la convention
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions qui pourraient avoir des conséquences fâcheuses.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires et des conseils.

Exemple de texte	Description de la convention
Exemple : …	Les exemples sont présentés sur un fond bleu sous le titre « Exemple ».
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments suivants sont en italique dans le texte : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère « + » représentent une combinaison de touches. Ces touches doivent être enfoncées simultanément.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
▶ *Pour programmer une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et possèdent l'icône « flèche ».
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : Indiquez la date au format `JJ:MM:AA`.	Les types de texte suivants apparaissent dans un style spécial : • Texte de la ligne de commande ; • Texte des messages affichés sur l'écran par l'application ; • Données à saisir via le clavier.
<Nom d'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les chevrons sont omis.

A propos de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security 1.6 protège les ordinateurs et autres systèmes embarqués tournant sous les systèmes d'exploitation Microsoft® Windows® contre les virus et autres menaces contre la sécurité informatique. Les utilisateurs de Kaspersky Embedded Systems Security sont les administrateurs du réseau de l'organisation et les personnes chargées de la protection antivirus de ce réseau.

Vous pouvez installer Kaspersky Embedded Systems Security sur n'importe quel type de système embarqué tournant sous Windows, dont les catégories de périphériques suivantes :

- les GAB (guichets automatiques bancaires) ;
- les TPV (terminaux de point de vente).

Vous pouvez administrer Kaspersky Embedded Systems Security d'une des manières suivantes :

- Via la console de Kaspersky Embedded Systems Security installée sur un ordinateur doté de Kaspersky Embedded Systems Security ou sur un autre ordinateur ;
- Via la ligne de commande ;
- Via le plug-in Kaspersky Embedded Systems Security pour Kaspersky Security Center (pour la protection centralisée du groupe d'ordinateurs dotés chacun 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 les fonctions de Kaspersky Embedded Systems Security

L'application intègre les modules suivants :

- **Protection en temps réel**. Kaspersky Embedded Systems Security analyse les objets lorsqu'ils sont sollicités. Kaspersky Embedded Systems Security analyse les objets suivants :
  - Les fichiers ;
  - Les flux alternatifs des systèmes de fichiers (flux NTFS) ;
  - L'enregistrement 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 du périphérique protégé, ainsi que les objets de démarrage.
- **Contrôle du lancement des applications**. Ce composant surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus.
- **Contrôle des périphériques**. Ce composant contrôle l'enregistrement et l'utilisation des dispositifs de stockage de masse et des lecteurs CD/DVD-ROM afin de protéger l'ordinateur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec le disque flash ou les périphériques externes d'un autre type connectés par USB.
- **Administration 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 autre possibilité de configurer les paramètres du pare-feu par d'autres moyens.
- **Moniteur d'intégrité des fichiers**. Kaspersky Embedded Systems Security détecte les modifications des fichiers, dans les zones de monitoring définies au sein des paramètres de la tâche, qui peuvent indiquer une violation de la sécurité sur l'ordinateur 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 et des modules de l'application**. Kaspersky Embedded Systems Security télécharge la mise à jour des bases de données et des modules de l'application depuis des serveurs FTP ou HTTP de mise à jour de Kaspersky Lab, depuis le serveur d'administration 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 la *quarantaine*. Pour des raisons de sécurité, une fois en quarantaine, les objets sont chiffrés.

- **Sauvegarde**. Kaspersky Embedded Systems Security enregistre une copie chiffrée des objets dont le statut est *Infecté ou détecté* et *Probablement infecté* dans la *sauvegarde* avant de procéder à la désinfection ou à la suppression de ces objets.

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

- **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 de l'entrée dans l'arborescence des ressources fichier du serveur 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.

- **Administration des autorisations d'accès aux 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 dans le journal de l'application**. Kaspersky Embedded Systems Security consigne dans les journaux les informations relatives aux paramètres des modules de l'application, à l'état actuel des tâches, aux événements survenus pendant l'exécution de celles-ci, ainsi que les renseignements sur les événements liés à l'administration de Kaspersky Embedded Systems Security et les informations indispensables au diagnostic des échecs dans le fonctionnement de l'application.

- **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 des fichiers en temps réel.

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

Interface de Kaspersky Embedded Systems Security

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

Dans cette section

Interface de la 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 sous l'entrée **Kaspersky Embedded Systems Security**.

Après la connexion à la copie de Kaspersky Embedded Systems Security installée sur un autre ordinateur, le nom de l'entrée reprend le nom de l'ordinateur 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 de l'ordinateur> sous <nom du compte utilisateur>**. En cas de connexion à une copie de Kaspersky Embedded Systems Security installée sur le même ordinateur que la Console, le nom de l'entrée prend la forme : **Kaspersky Embedded Systems Security**.

Par défaut, la fenêtre de la console de Kaspersky Embedded Systems Security contient les éléments suivants :

- Arborescence de la Console ;

- Volet résultats ;
- Panneau de tâche ;
- Barre d'outils.

Vous pouvez également activer l'affichage de la zone de description et du panneau des actions dans la console.

Arborescence de la Console

L'arborescence de la Console affiche l'entrée **Kaspersky Embedded Systems Security** et ses sous-entrées correspondant aux modules opérationnels de l'application.

Dans le cas de **Kaspersky Embedded Systems Security**, il s'agit des nœuds enfants suivants :

- **Protection en temps réel** : administration de la protection des fichiers en temps réel et des paramètres d'utilisation des services du KSN. L'entrée **Protection en temps réel** permet d'administrer les tâches suivantes :
  - **Protection des fichiers en temps réel**.
  - **Utilisation du KSN**.
- **Contrôle de l'ordinateur** : contrôle des périphériques connectés, ainsi que le contrôle des applications lancées sur l'ordinateur protégé. L'entrée **Contrôle de l'ordinateur** permet d'administrer les tâches suivantes :
  - **Contrôle du lancement des applications**.
  - **Contrôle des périphériques**.
  - **Administration 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**.
  - **Génération des règles pour le Contrôle des périphériques**.
  - Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).

    Les tâches de groupe (cf. section « Catégories des tâches de Kaspersky Embedded Systems Security » à la page 73) sont créées à l'aide de Kaspersky Security Center. Il

est impossible d'administrer les tâches de groupe via la Console de Kaspersky Embedded Systems Security.

- **Diagnostic du système** : administration des paramètres du contrôle des opérations réalisées sur les fichiers et la configuration de l'inspection du journal des événements Windows.
  - **Moniteur d'intégrité des fichiers**.
  - **Inspection des journaux**.
- **Analyse à la demande** : gère les tâches d'analyse antivirus à la demande. Une entrée séparée existe pour chacune des tâches :
  - **Analyse au démarrage du système d'exploitation**.
  - **Analyse des zones critiques**.
  - **Analyse des objets en quarantaine**.
  - **Vérification de l'intégrité de l'application**.
  - Tâches définies par l'utilisateur **<Nom des tâches>** (le cas échéant).

  L'entrée affiche les tâches système (cf. section « Catégories des tâches de Kaspersky Embedded Systems Security » à la page 73) créées lors de l'installation de l'application, les tâches définies par l'utilisateur ajoutées ainsi que les tâches de groupe d'analyse à la demande créées et transmises à l'ordinateur 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. L'entrée contient des entrées secondaires permettant d'administrer chacune des tâches de mise à jour ou d'annulation de la dernière 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**.

L'entrée affiche toutes les tâches définies par l'utilisateur et les tâches de groupe (cf. section « Catégories des tâches de Kaspersky Embedded Systems Security » à la page 73) de mise à jour créées et transmises à l'ordinateur via Kaspersky Security Center.

- **Stockages** : administration des paramètres de la quarantaine et de la sauvegarde.
  - **Quarantaine**.
  - **Sauvegarde**.
- **Journaux** : gestion des journaux d'exécution de la tâche de protection en temps réel, d'analyse à la demande, du contrôle de l'ordinateur et des tâches de mise à jour ; gestion du journal des événements de sécurité et du journal d'audit système de Kaspersky Embedded Systems Security.
  - **Journal des événements de sécurité**.
  - **Journal d'audit système**.
  - **Journaux d'exécution des tâches**.
- **Licence** : ajout et suppression de clés et de codes d'activation pour Kaspersky Embedded Systems Security, consultation des informations relatives aux licences.

Volet résultats

Le volet résultats reprend les informations relatives au nœud sélectionné. Si vous avez choisi l'entrée **Kaspersky Embedded Systems Security**, le volet résultats affichent les informations relatives à l'état actuel de la protection de l'ordinateur (cf. section « Consultation de l'état de la protection et des informations sur Kaspersky Embedded Systems Security » à la page 31), les informations relatives à Kaspersky Embedded Systems Security, l'état de ses composants fonctionnels et l'état de la licence ou la clé.

Menu contextuel de l'entrée Kaspersky Embedded Systems Security

A l'aide des options du menu contextuel de l'entrée **Kaspersky Embedded Systems Security**, vous pouvez exécuter les opérations suivantes :

- **Se connecter à un autre ordinateur**. Se connecter à un autre ordinateur pour administrer la copie de Kaspersky Embedded Systems Security installée sur cet ordinateur. Pour effectuer cette opération, vous pouvez également utiliser le lien situé dans le coin inférieur droit du volet résultats de l'entrée **Kaspersky Embedded Systems Security**.

- **Lancer Kaspersky Embedded Systems Security** / **Arrêter Kaspersky Embedded Systems Security** (**Démarrer** / **Arrêter**). Lancer ou arrêter l'application ou la tâche sélectionnée (cf. section « Lancement / suspension / rétablissement / arrêt manuel d'une tâche » à la page 75). 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**. Consulter et configurer l'analyse des disques amovibles (cf. section « Analyse des disques amovibles » à la page 280) à la connexion.

- **Protection contre les exploits : paramètres généraux de la protection**. Choisir le mode de protection de l'ordinateur contre les exploits (cf. section « Configuration des paramètres de protection de la mémoire des processus » à la page 141) et les actions de réduction de l'impact.

- **Protection contre les exploits : paramètres de protection des processus**. Ajouter des processus à la liste des processus protégés (cf. section « Ajout d'un processus protégé » à la page 143) et configurer les paramètres de leur protection.

- Configurer les paramètres de la zone de confiance. Consulter et configurer les paramètres de la zone de confiance (cf. section « A propos de la zone de confiance de Kaspersky Embedded Systems Security » à la page 62).

- **Modifier les permissions utilisateur pour l'administration de l'application**. Consulter et configurer les privilèges d'accès aux fonctions de Kaspersky Embedded Systems Security (cf. section « A propos des autorisations d'administration de Kaspersky Embedded Systems Security » à la page 41).

- **Modifier les autorisations des utilisateurs pour l'administration du service Kaspersky Security**. Consulter et configurer les privilèges d'accès à l'administration du Service Kaspersky Security.
- **Exporter les paramètres**. Enregistrer les paramètres de l'application dans un fichier de configuration au format XML (cf. section « Exportation des paramètres » à la page 84). L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Importer les paramètres**. Importer les paramètres de l'application depuis le fichier de configuration au format XML (cf. section « Importation des paramètres » à la page 85). L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Données sur l'application et les mises à jour disponibles**. Affiche les informations relatives à Kaspersky Embedded Systems Security et aux mises à jour des modules de l'application disponibles.
- **A propos du logiciel**. Accéder à la consultation des informations sur Kaspersky Embedded Systems Security.
- **Nouvelle fenêtre**. Ouvrir une nouvelle fenêtre dans la Console de Kaspersky Embedded Systems Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Mettre à jour**. Actualiser le contenu de la fenêtre de la Console de Kaspersky Embedded Systems Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Propriétés**. Consulter et configurer 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 volet résultats de l'entrée **Kaspersky Embedded Systems Security** ou le bouton dans la barre d'outils.

- **Aide**. Accéder à la consultation de l'aide de Kaspersky Embedded Systems Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Volet d'accès rapide et menu contextuel des tâches de Kaspersky Embedded Systems Security

Vous pouvez administrer les tâches Kaspersky Embedded Systems Security à l'aide des options du menu contextuel de chaque tâche dans l'arborescence de la Console.

A l'aide des options du menu contextuel de la tâche sélectionnée, vous pouvez exécuter les opérations suivantes :

- **Reprendre / Suspendre**. Rétablir ou suspendre l'exécution d'une tâche (cf. section « Lancement / suspension / rétablissement / arrêt manuel d'une tâche » à la page 75). Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches de protection en temps réel et d'analyse à la demande.

- **Ajouter une tâche**. Créer une tâche définie par l'utilisateur (cf. section « Création d'une tâche d'analyse à la demande » à la page 282). L'opération est disponible pour les tâches d'analyse à la demande.

- **Ouvrir le journal d'exécution**. Accéder à la consultation et à l'utilisation du journal d'exécution de la tâche. (cf. section « A propos des journaux d'exécution des tâches » à la page 342) L'opération est disponible pour toutes les tâches.

- **Enregistrer la tâche**. Enregistrer et appliquer les modifications apportées aux paramètres de la tâche (cf. section « Enregistrement de la tâche après modification de ses paramètres » à la page 74). Cette action est disponible pour les tâches de protection des fichiers en temps réel et d'analyse à la demande.

- **Supprimer la tâche**. Supprimer une tâche définie par l'utilisateur (cf. section « Suppression d'une tâche » à la page 286). L'opération est disponible pour les tâches d'analyse à la demande.

- **Statistiques**. Accéder à la consultation des statistiques de la tâche. L'opération est disponible pour la tâche de vérification de l'intégrité de l'application.

- **Modèles des paramètres**. Accéder à l'utilisation des modèles. Cette opération est disponible pour les tâches de protection des fichiers en temps réel et d'analyse à la demande.

Icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches

Chaque fois que Kaspersky Embedded Systems Security se lance automatiquement après le redémarrage de l'ordinateur, l'icône de Kaspersky Embedded Systems Security apparaît dans la zone de notification de la barre des tâches. L'icône est affichée par défaut si vous avez installé le composant **Icône de zone de notification Kaspersky Embedded Systems Security** lors de l'installation de l'application.

L'aspect de l'icône de la zone de notifications de Kaspersky Embedded Systems Security indique le statut de la protection actuelle de l'ordinateur. L'icône peut avoir un des états suivants :

- actif (en couleur) si au moins une des tâches suivantes est actuellement en cours d'exécution : Protection des fichiers en temps réel, Contrôle du lancement des applications ou Contrôle des périphériques ;

- inactif (en noir et blanc) si aucune des tâches suivantes n'est actuellement en cours d'exécution : Protection des fichiers en temps réel, Contrôle du lancement des applications ou Contrôle des périphériques.

Le menu contextuel de l'icône s'ouvre d'un clic droit de la souris.

Le menu contextuel contient plusieurs commandes d'affichage de fenêtre de l'application (cf. tableau ci-après).

Tableau 2. Commandes du menu contextuel de l'icône de la zone de notifications de Kaspersky Embedded Systems Security

Instruction	Description
Ouvrir la console de Kaspersky Embedded Systems Security	Ouvre la console de Kaspersky Embedded Systems Security (si celle-ci est installée).
A propos du logiciel	Ouvre la fenêtre **A propos du logiciel** qui contient des informations sur Kaspersky Embedded Systems Security. Si vous êtes un utilisateur enregistré de Kaspersky Embedded Systems Security, alors la fenêtre **A propos du logiciel** contient des informations sur les mises à jour urgentes installées.
Fermer	Masque l'icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.

Vous pouvez à tout moment restaurer l'icône de Kaspersky Embedded Systems Security masquée.

► *Pour afficher à nouveau l'icône de l'application,*

Dans le menu **Démarrer** de Microsoft Windows, choisissez **Programmes → Kaspersky Embedded Systems Security 1.6 → Icône de Kaspersky Embedded Systems Security**.

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

Dans les paramètres de l'application, vous pouvez activer et désactiver l'affichage de l'icône de Kaspersky Embedded Systems Security dans la zone de notification lors du lancement automatique de l'application après le redémarrage de l'ordinateur.

Lancement et arrêt de Kaspersky Embedded Systems Security

Cette section fournit des informations sur le lancement de la Console de Kaspersky Embedded Systems Security, ainsi que sur le lancement et l'arrêt du service Kaspersky Security.

Dans cette section

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 lancer la console de l'application depuis le menu « Démarrer », procédez comme suit :*

  Dans le menu **Démarrer**, choisissez **Programmes → Kaspersky Embedded Systems Security → Outils d'administration → Console de Kaspersky Embedded Systems Security**.

Si vous avez l'intention d'ajouter d'autres composants logiciels enfichables à la Console de l'application, lancez la Console en mode auteur.

► *Pour lancer la Console de l'application en mode auteur, procédez comme suit :*

1. Dans le menu **Démarrer** sélectionnez **Programmes** → **Kaspersky Embedded Systems Security** → **Outils d'administration**.

2. Dans le menu contextuel de l'application **Console de Kaspersky Embedded Systems Security**, choisissez la commande **Auteur**.

La Console de Kaspersky Embedded Systems Security sera lancée en mode auteur.

Si vous avez lancé la console de Kaspersky Embedded Systems Security sur l'ordinateur à protéger, la fenêtre de la console s'ouvre (cf. section « Interface de la fenêtre de la console de Kaspersky Embedded Systems Security » à la page 20).

Si vous aviez lancé la Console de Kaspersky Embedded Systems Security non pas sur l'ordinateur à protéger, mais sur un autre périphérique, connectez-vous à l'ordinateur à protéger.

► *Pour vous connecter à l'ordinateur à protéger, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.

2. Sélectionnez la commande **Se connecter à un autre ordinateur**.

   La fenêtre **Sélection d'ordinateur** s'ouvre.

3. Dans la fenêtre qui s'ouvre, sélectionnez **Autre ordinateur**.

4. Dans le champ de saisie de droite, indiquez le nom réseau de l'ordinateur à protéger.

5. Cliquez sur **OK**.

La console de Kaspersky Embedded Systems Security sera connectée à l'ordinateur protégé.

Si le compte utilisateur employé pour accéder à Microsoft Windows ne dispose pas des privilèges d'accès au service d'administration de Kaspersky Embedded Systems Security sur l'ordinateur, cochez la case **Se connecter sous le compte utilisateur** et indiquez un autre compte qui dispose de tels privilèges.

Lancement et arrêt du service Kaspersky Security

Le service Kaspersky Security est lancé automatiquement par défaut au démarrage du système d'exploitation. Le service Kaspersky Security gère les processus de travail chargés de la protection en temps réel, du contrôle de l'ordinateur, de la protection des stockages réseau, de l'analyse à la demande et de la mise à jour.

Le lancement du service Kaspersky Security marque par défaut le lancement des tâches Protection des fichiers en temps réel, Analyse au démarrage du système d'exploitation, Vérification de l'intégrité de l'application 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 lancé à nouveau le service Kaspersky Security, l'application lance automatiquement uniquement les tâches dont la planification reprend la fréquence **Au lancement de l'application**, les autres tâches sont lancées manuellement.

Vous pouvez lancer et arrêter le service Kaspersky Security à l'aide du menu contextuel de l'entrée **Kaspersky Embedded Systems Security** ou via le composant logiciel enfichable **Services** de Microsoft Windows.

Vous pouvez lancer et arrêter Kaspersky Embedded Systems Security si vous faites partie du groupe d'administrateurs sur le serveur protégé.

► *Pour arrêter ou lancer l'application via la console de gestion, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.
2. Choisissez une des commandes suivantes :
   - **Arrêter Kaspersky Embedded Systems Security** pour arrêter le service Kaspersky Security Service ;
   - **Lancer Kaspersky Embedded Systems Security** pour lancer le service Kaspersky Security Service.

Le service Kaspersky Security sera lancé ou arrêté.

Consultation de l'état de la protection et des informations sur Kaspersky Embedded Systems Security

► *Pour voir les informations sur le statut de la protection de l'ordinateur et les informations sur Kaspersky Embedded Systems Security,*

Ouvrez le nœud **Kaspersky Embedded Systems Security** dans l'arborescence de la Console.

Par défaut, les informations du volet résultats de la Console de Kaspersky Embedded Systems Security 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 **Mettre à jour** dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

Le volet résultats de la Console affiche les informations suivantes sur l'application :

- État de la protection de l'ordinateur ;
- Données sur la mise à jour des bases de données et des modules de l'application ;
- Données relatives à la licence ;
- Données relatives aux tâches de contrôle de l'ordinateur ;
- État de l'intégration à Kaspersky Security Center : données de l'ordinateur doté de Kaspersky Security Center auquel l'application est connectée ; données sur le contrôle des tâches de l'application par la stratégie active.

Les couleurs suivantes sont utilisées pour désigner l'état de la protection :

- *Vert*. La tâche est exécutée conformément aux paramètres définis. La protection est garantie.
- *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 à l'entrée de la tâche correspondante ou d'ouvrir le journal de son exécution.

Le groupe **Protection** (cf. tableau ci-après) affiche les informations sur l'état actuel de la protection de l'ordinateur.

Tableau 3. Informations sur l'état de la protection de l'ordinateur

Groupe Protection	Conseil
Indicateur d'état de la protection de l'ordinateur	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que les tâches de protection en temps réel sont en cours d'exécution et que la tâche d'analyse rapide a été exécutée il y a moins de 30 jours (par défaut). • Volet de couleur jaune : une ou plusieurs tâches de protection en temps réel ne sont pas en cours d'exécution ou ont été arrêtées et la tâche d'analyse rapide n'a pas été exécutée depuis longtemps. • Volet de couleur rouge : la tâche de protection des fichiers en temps réel n'a pas pu être exécutée.
Protection des fichiers en temps réel	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **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.
Utilisation du KSN	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **Conclusions douteuses** : nombre d'objets identifiés comme douteux par les services du KSN. Par exemple, si au cours de l'analyse de cinq fichiers, le service du KSN renvoie un résultat établissant le caractère malveillant de l'un d'entre eux, la valeur de ce champ augmentera d'une unité. Si le nombre de conclusions douteuses dépasse 0, la valeur de la ligne est mise en évidence en rouge.

Groupe Protection	Conseil
Analyse des zones critiques	**Date de la dernière analyse** : date et heure de la dernière analyse rapide à la recherche de virus et autres menaces informatiques dans les zones critiques de l'ordinateur. *N'a pas été réalisée :* événement qui survient quand la tâche d'analyse des zones critiques a été effectuée il y a 30 jours ou plus (par défaut). Vous pouvez modifier le seuil de déclenchement de l'événement.
Nombre d'objets dans la sauvegarde	*Dépassement du seuil d'espace disponible dans la sauvegarde* : événement qui se produit si le seuil d'espace disponible dans la sauvegarde atteint la valeur indiquée. Kaspersky Embedded Systems Security continue malgré tout à placer les objets en sauvegarde. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en jaune. *Dépassement de la taille maximale de sauvegarde* : événement qui se produit si la taille de la Sauvegarde atteint la valeur indiquée. Kaspersky Embedded Systems Security continue malgré tout à placer les objets en sauvegarde. Dans ce cas, la valeur du champ **Espace utilisé** est mise en évidence en rouge. **Nombre d'objets dans la sauvegarde** : nombre d'objets présents actuellement dans la sauvegarde. **Espace utilisé** : volume d'espace occupé dans la sauvegarde.
Protection de la mémoire	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). Le mode de fonctionnement est un des deux modes à sélectionner lors de la configuration de la protection de la mémoire des processus : • Prévenir l'exploitation des vulnérabilités dans les processus. • Signaler uniquement l'intrusion suspecte dans les processus. **Processus dans la liste de protection** : total des processus protégés et traité selon le mode sélectionné.

Le groupe **Mise à jour** (cf. tableau ci-dessous) affiche les informations sur l'actualité des bases antivirus et des modules de l'application.

Tableau 4. Informations sur l'état des bases et des modules de Kaspersky Embedded Systems Security

Le bloc Mise à jour	Conseil
Témoin de l'état des bases et des modules de l'application	La couleur du volet portant le nom du groupe indique l'état des bases et des modules de l'application. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que les bases de l'application sont à jour et qu'aucune mise à jour critique des modules de l'application n'est disponible. • Volet de couleur jaune : un des événements suivants s'est produit : *Les bases de l'application sont dépassées* ; *Une mise à jour critique des modules de l'application est disponible* ; *Le rappel de la mise à jour critique des modules de l'application a été annoncé* ; *Afin de terminer la mise à jour des modules de l'application, l'ordinateur doit être redémarré.* • Volet de couleur rouge : l'événement *Les bases de l'application sont fortement dépassées* ou *Les bases de l'application sont endommagées* s'est produit.
Mise à jour des bases et des modules de l'application	**État des bases de l'application** : évaluation de l'actualité des bases de l'application. Le paramètre peut prendre les valeurs suivantes : • **Les bases de l'application sont à jour** : les bases de l'application ont été mises à jour il y a 7 jours maximum (par défaut). • **Les bases de l'application sont dépassées** : les bases de l'application ont été mises à jour il y a 7 à 14 jours. • **Les bases de l'application sont 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 *Les bases de l'application sont dépassées* et *Les bases de l'application sont 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 installée. La date et l'heure sont exprimées en TU. **Nombre d'enregistrements dans les bases de l'application** : nombre d'enregistrements relatifs aux menaces dans les bases de données de l'application installées. **Etat de la tâche de mise à jour des bases de l'application lancée** : 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'ordinateur à protéger. La valeur du champ prend la couleur rouge si l'événement *Echec* 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.

Le groupe **Contrôle** (cf. tableau ci-dessous) affiche les informations sur l'état des tâches Contrôle du lancement des applications, Contrôle des périphériques et Administration du pare-feu.

Tableau 5. Informations sur l'état du contrôle de l'ordinateur

Groupe Contrôle	Conseil
Indicateur d'état du contrôle de l'ordinateur	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que toutes les tâches de contrôle de l'ordinateur sont en cours d'exécution. • Volet de couleur jaune : une ou plusieurs tâches de protection de l'ordinateur n'ont pas été exécutées ; l'événement *Non exécuté* se produit. • La couleur rouge du volet indique l'échec du lancement de la tâche du Contrôle du lancement des applications ou du contrôle des périphériques externes ; l'événement *Échec*.
Contrôle du lancement des applications	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **Mode de fonctionnement** : un des deux modes de fonctionnement disponibles pour la tâche Contrôle du lancement des applications : • Appliquer les règles du Contrôle du lancement des applications. • Statistiques uniquement. **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 de contrôle du lancement des applications. Si le nombre de lancements d'applications bloqués dépasse 0, la valeur du champ prend la couleur rouge. **Durée de traitement moyenne (en ms)** : temps qui a été nécessaire à Kaspersky Embedded Systems Security pour le traitement des tentatives de lancement d'applications sur l'ordinateur à protéger.

Groupe Contrôle	Conseil
Contrôle des périphériques	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **Mode de fonctionnement** : un des deux modes de fonctionnement disponibles pour la tâche Contrôle du lancement des applications : • Appliquer le blocage par défaut. • Statistiques uniquement. **Périphériques bloqués** : nombre de périphériques connectés avec tentative d'utilisation en tant que dispositif de stockage de masse bloqués par Kaspersky Embedded Systems Security au cours de l'exécution de la tâche de contrôle des périphériques. Si le nombre de périphériques bloqués dépasse 0, la valeur du champ prend la couleur rouge.
Administration du pare-feu	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). Connexions bloquées : nombre de connexions au périphérique protégé qui n'ont pas été autorisées par les règles du pare-feu définies.

Le groupe **Diagnostic** (cf. tableau ci-après) affiche les informations relatives à l'état des tâches Monitoring d'intégrité des fichiers et Inspection des journaux.

Tableau 6. Informations sur l'état du diagnostic du système

Groupe Diagnostic	Conseil
Indicateur de l'état de la sécurité sur le réseau	La couleur du volet portant le nom du groupe indique l'état des tâches exécutées dans le groupe. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : s'affiche par défaut et indique que toutes les tâches de diagnostic du système sont en cours d'exécution. • Volet de couleur jaune : une ou plusieurs tâches de diagnostic du système n'ont pas été exécutées ; l'événement *Non exécuté* se produit. • La couleur rouge du volet indique l'échec du lancement de la tâche Moniteur d'intégrité des fichiers ou Inspection des journaux ; l'événement *Échec* est enregistré.
Moniteur d'intégrité des fichiers	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **Opérations non autorisées** : total des modifications dans des fichiers de la zone de monitoring qui pourraient indiquer une violation de la sécurité du périphérique protégé.
Inspection des journaux	**Etat de la tâche** : état actuel de la tâche (par exemple, *Exécution en cours* ou *Stoppée*). **Violations potentielles** : total des violations enregistrées d'après les données du journal des événements Windows et détectées sur la base des règles définies de la tâche ou de l'application de l'analyse heuristique.

Les informations sur l'état de la licence de Kaspersky Embedded Systems Security sont affichées dans la ligne dans le coin inférieur gauche du volet résultats de l'entrée **Kaspersky Embedded Systems Security**.

Vous pouvez configurer les propriétés de Kaspersky Embedded Systems Security via le lien **Propriétés de l'application** (cf. section « **Paramètres de fonctionnement de Kaspersky Embedded Systems Security dans la Console »** à la page 51).

Vous pouvez établir une connexion sur un autre ordinateur via le lien **Se connecter à un autre ordinateur** (voir la section « **Administration de Kaspersky Embedded Systems Security via une Console sur un autre ordinateur »** à la page 60).

Autorisations d'accès aux fonctions de Kaspersky Embedded Systems Security

Cette section fournit des informations sur les autorisations d'administration de Kaspersky Embedded Systems Security et des services Windows qu'enregistre l'application. Elle fournit également des instructions sur la configuration de ces autorisations.

Dans cette section

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 l'ordinateur protégé et aux utilisateurs du groupe ESS Administrators créé sur l'ordinateur protégé lors de l'installation de Kaspersky Embedded Systems Security et aussi aux utilisateurs du groupe SYSTEM.

La suppression du compte utilisateur SYSTEM et la modification des privilèges de ce dernier sont impossibles. Si des modifications sont introduites dans le compte utilisateur SYSTEM, les privilèges maximum de ce compte utilisateur sont restaurés.

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 l'ordinateur 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 Kaspersky Embedded Systems Security.

Vous pouvez attribuer à l'utilisateur ou au groupe d'utilisateurs de Kaspersky Embedded Systems Security un des niveaux prédéfinis d'accès aux fonctions de Kaspersky Embedded Systems Security :

- **Contrôle complet** : accès à toutes les fonctions de l'application ; consultation et modifications des paramètres généraux de fonctionnement de Kaspersky Embedded Systems Security, des paramètres de fonctionnement des modules de Kaspersky Embedded Systems Security, des autorisations des utilisateurs de Kaspersky Embedded Systems Security ainsi que la consultation des statistiques de fonctionnement 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 du fonctionnement de Kaspersky Embedded Systems Security, les paramètres de fonctionnement des composants de Kaspersky Embedded Systems Security.

- **Lire** : lecture et modification des paramètres généraux de fonctionnement de Kaspersky Embedded Systems Security, des paramètres de fonctionnement des modules de Kaspersky Embedded Systems Security, des statistiques de fonctionnement de Kaspersky Embedded Systems Security et des autorisations des utilisateurs de l'application.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès (cf. section « Configuration des autorisations d'accès aux fonctions de Kaspersky Embedded Systems Security et à l'administration du service Kaspersky Security » à la page 45) : autoriser ou interdire l'accès aux fonctions individuelles 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**.

Tableau 7. Autorisations d'accès aux 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 de tâches	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilité d'importer les paramètres de fonctionnement de Kaspersky Embedded Systems Security depuis un fichier de configuration.
Lire les paramètres	Possibilités : • Consultation des paramètres généraux de fonctionnement de Kaspersky Embedded Systems Security et des paramètres des tâches ; • Exportation des paramètres de fonctionnement de Kaspersky Embedded Systems Security dans un fichier de configuration ; • Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Gérer les stockages	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	Possibilité de consulter les statistiques de fonctionnement de chaque tâche de Kaspersky Embedded Systems Security.

Autorisations d'accès	Description
Licence de l'application	Possibilité d'activer ou de désactiver Kaspersky Embedded Systems Security.
Suppression de l'application	Possibilité de supprimer Kaspersky Embedded Systems Security
Lecture des privilèges	Consultation de la liste des utilisateurs de Kaspersky Embedded Systems Security et des privilèges d'accès de chacun d'entre eux.
Modification des privilèges	Possibilités : • Modifier la liste des utilisateurs qui ont accès à l'administration de l'application ; • Modification des autorisations d'accès des utilisateurs aux fonctions de Kaspersky Embedded Systems Security.

A propos des autorisations d'administration des services enregistrés

Les informations détaillées sur les services Windows enregistrés et la configuration de l'accès aux services enregistrés figurent dans le *Manuel de l'administrateur de Kaspersky Embedded Systems Security.*

Lors de l'installation, Kaspersky Embedded Systems Security enregistre dans Windows le service Kaspersky Security (KAVFS) et le service d'administration de l'application Kaspersky Security Management (KAVFSGT).

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'ordinateur à protéger, 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 (cf. section « A propos des autorisations d'administration de Kaspersky Embedded Systems Security » à la page 41) peuvent octroyer l'accès à l'administration du service Kaspersky Security à d'autres utilisateurs enregistrés sur l'ordinateur à protéger ou appartenant au domaine.

Service Kaspersky Security Management Service

Pour administrer l'application via la console de Kaspersky Embedded Systems Security installée sur un autre ordinateur, il faut que le compte utilisateur sous les autorisations duquel la connexion à Kaspersky Embedded Systems Security s'opère possède un accès complet à Kaspersky Security Management Service sur l'ordinateur protégé.

Par défaut, l'accès à l'administration de Kaspersky Security Management Service est octroyé aux utilisateurs du groupe Administrateurs sur l'ordinateur protégé et aux utilisateurs du groupe ESS Administrators créé sur l'ordinateur protégé lors de l'installation de Kaspersky Embedded Systems Security.

Vous pouvez administrer Kaspersky Security Management Service uniquement via le composant logiciel enfichable Services de Microsoft Windows.

Configuration des autorisations d'accès à l'administration de Kaspersky Embedded Systems Security et du service Kaspersky Security

Vous pouvez modifier la liste des utilisateurs et groupes d'utilisateurs ayant accès aux fonctions de Kaspersky Embedded Systems Security et à l'administration du service Kaspersky Security, ainsi que modifier les privilèges d'accès des utilisateurs et groupes d'utilisateurs.

► *Pour ajouter un utilisateur ou un groupe à la liste ou pour l'en supprimer, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security** et réalisez une des actions suivantes :

   - Choisissez l'option **Modifier les permissions utilisateur pour l'administration de l'application** si vous souhaitez modifier la liste des utilisateurs ayant accès à l'administration des fonctions de Kaspersky Embedded Systems Security.

   - Choisissez l'option **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service** 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 **Autorisations pour le groupe « Kaspersky Embedded Systems Security »** s'ouvre.

2. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

   - Pour ajouter un utilisateur (un groupe) à la liste, cliquez sur le bouton **Ajouter** puis, sélectionnez l'utilisateur ou le groupe auquel vous souhaitez octroyez des autorisations.

   - Pour supprimer un utilisateur (un groupe) de la liste, sélectionnez les utilisateurs (les groupes) pour lesquels vous souhaitez restreindre l'accès, puis cliquez sur le bouton **Supprimer**.

3. 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 d'un utilisateur (ou d'un groupe d'utilisateurs), procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security** et réalisez une des actions suivantes :

- Choisissez l'option **Modifier les permissions utilisateur pour l'administration de l'application** si vous souhaitez configurer les autorisations d'accès aux fonctions de Kaspersky Embedded Systems Security.

- Choisissez l'option **Modifier les autorisations des utilisateurs pour l'administration de Kaspersky Security Service** si vous souhaitez configurer les autorisations d'accès au service Kaspersky Security.

  La fenêtre **Autorisations pour le groupe « Kaspersky Embedded Systems Security »** s'ouvre.

2. Dans la fenêtre qui s'ouvre sélectionnez dans la liste **Groupes ou utilisateurs** l'utilisateur ou le groupe d'utilisateurs dont vous souhaitez modifier les autorisations.

3. Dans le groupe **Autorisation pour le groupe "<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 : **Lecture des statistiques**, **Lire les paramètres**, **Lire les journaux** et **Lire les privilèges** ;

     - Autorisations suivantes pour l'administration du service Kaspersky Security : **Lecture des paramètres du service**, **Requête concernant le statut du service auprès du Gestionnaire d'administration des services**, **Requête concernant le statut auprès du service**, **Lecture de la liste des services dépendants, Lire les privilèges**.

- **Modifier** :
  - Toutes les autorisations d'administration de Kaspersky Embedded Systems Security, sauf **Modifier les privilèges** ;
  - Autorisations suivantes sur l'administration du service Kaspersky Security : **Modification des paramètres du service, Lire les privilèges**.
- **Exécution** : autorisations suivantes sur l'administration du service Kaspersky Security : **Lancement du service**, **Arrêt du service**, **Suspension/reprise du service**, **Lire les privilèges**, **Requêtes de l'utilisateur au service**.

4. 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 avancés pour Kaspersky Embedded Systems Security** qui s'ouvre, sélectionnez l'utilisateur ou le groupe requis.
   b. Cliquez sur le bouton **Modifier**.
   c. Dans la fenêtre qui s'ouvre, cliquez sur le lien **Afficher les autorisations spéciales**.
   d. Dans la liste déroulante de la partie supérieure de la fenêtre, sélectionnez le type de contrôle d'accès (**Autoriser** ou **Interdire**).
   e. Cochez la case en regard des fonctions pour lesquelles vous souhaitez octroyer ou non un accès à un utilisateur ou un groupe d'utilisateurs sélectionnés.
   f. Cliquez sur **OK**.
   g. Dans la fenêtre **Paramètres de sécurité avancé pour Kaspersky Embedded Systems Security**, cliquez sur **OK**.
5. Dans la fenêtre **Autorisations pour le groupe "Kaspersky Embedded Systems Security"**, cliquez sur le bouton **Appliquer**.

Les autorisations d'administration de Kaspersky Embedded Systems Security ou du service Kaspersky Security configurées seront enregistrées.

Utilisation de la Console de Kaspersky Embedded Systems Security

Cette section fournit des informations sur la Console de Kaspersky Embedded Systems Security (ci-après, la « Console ») et sur l'administration de l'application via la Console de Kaspersky Embedded Systems Security installée sur l'ordinateur protégé ou sur un autre ordinateur.

Dans cette section

Présentation de la console de Kaspersky Embedded Systems Security

La console de Kaspersky Embedded Systems Security est un composant logiciel enfichable isolé qui est ajouté à la console Microsoft Management Console.

Il est possible d'administrer l'application via la console installée sur l'ordinateur protégé ou sur un autre ordinateur du réseau. Une fois que la Console de Kaspersky Embedded Systems Security a été installée sur un autre ordinateur, vous devez effectuer la configuration avancée (cf. section « Administration de Kaspersky Embedded Systems Security via une Console sur un autre ordinateur » à la page 60).

Si la console de Kaspersky Embedded Systems Security et l'application sont installées sur différents ordinateurs appartenant à différents domaines, il se peut qu'il y ait des restrictions au niveau de la remise des informations de Kaspersky Embedded Systems Security à la console. Par exemple, après le démarrage d'une tâche quelconque de Kaspersky Embedded Systems Security, il se peut que l'état de cette tâche ne soit pas actualisé dans la console.

Une fois l'installation de la console de l'application terminée, le programme d'installation conserve le fichier kavfs.msc dans le répertoire d'installation et ajoute le composant logiciel enfichable à la liste des composants logiciel enfichables isolés de Microsoft Windows.

Vous pouvez ouvrir la console de Kaspersky Embedded Systems Security depuis le menu **Démarrer.** Vous pouvez également, sur le périphérique protégé, ouvrir la console à l'aide de l'icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches.

Vous pouvez lancer le fichier msc du composant logiciel enfichable de Kaspersky Embedded Systems Security ou ajouter ce composant logiciel enfichable à la console Microsoft Management Console existante en tant que nouvel élément de son arborescence (cf. section « Interface de la fenêtre de la Console de Kaspersky Embedded Systems Security » à la page 20).

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 ce faire, tapez la commande mmc.exe/32 dans la ligne de commande pour ouvrir la Microsoft Management Console.

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

Paramètres de fonctionnement de Kaspersky Embedded Systems Security dans la Console

Les paramètres généraux et les paramètres du diagnostic des pannes de Kaspersky Embedded Systems Security définissent les conditions générales de fonctionnement de l'application. Ils déterminent le nombre de processus utilisés par Kaspersky Embedded Systems Security, ils permettent d'activer la reprise des tâches de Kaspersky Embedded Systems Security après un arrêt inopiné de leur fonctionnement, de tenir un journal de traçage, 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 Kaspersky Embedded Systems Security 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 fonctionnement de Kaspersky Embedded Systems Security, procédez comme suit :*

1. Dans l'arborescence de la Console de l'application, sélectionnez l'entrée **Kaspersky Embedded Systems Security** et réalisez l'une des actions suivantes :

   - Dans le volet résultats de l'entrée, suivez le lien **Propriétés de l'application**.
   - Dans le menu contextuel de l'entrée, sélectionnez l'option **Propriétés**.

   La fenêtre **Paramètres de l'application** s'ouvre.

2. Dans la fenêtre qui s'ouvre, configurez les paramètres de fonctionnement de Kaspersky Embedded Systems Security en fonction de vos exigences :

   - L'onglet **Montée en puissance et interface** permet de configurer les paramètres suivants :
     - Dans le groupe **Paramètres d'optimisation** :
       - Nombre maximum de processus de travail actifs que Kaspersky Embedded Systems Security peut lancer.

Tableau 8. Quantité maximale de processus actifs

<table>
<tr><td>Paramètre</td><td>Quantité maximale de processus actifs.</td></tr>
<tr><td>Description</td><td>Ce paramètre appartient au groupe Paramètres d'optimisation de Kaspersky Embedded Systems Security. Il définit le nombre maximum de processus de travail qui peuvent être exécutés simultanément par l'application.

L'augmentation du nombre de processus de travail exécutés en parallèle accélère la vitesse d'analyse des fichiers et la résistance de Kaspersky Embedded Systems Security aux échecs. Toutefois, si cette valeur est trop élevée, les performances globales de l'ordinateur peuvent chuter et la mémoire vive requise peut augmenter.

N'oubliez pas que la console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre Quantité maximale de processus actifs uniquement pour Kaspersky Embedded Systems Security sur un ordinateur séparé (dans la boîte de dialogue Paramètres de l'application) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe d'ordinateurs.</td></tr>
<tr><td>Valeurs possibles</td><td>1 – 8</td></tr>
<tr><td>Valeur par défaut</td><td>Kaspersky Embedded Systems Security réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :
<table><tr><th>Nombre de processeurs</th><th>Quantité maximale de processus actifs</th></tr><tr><td>1</td><td>1</td></tr><tr><td>1< nbre de processeurs < 4</td><td>2</td></tr><tr><td>4 et plus</td><td>4</td></tr></table></td></tr>
</table>

- Nombre de processus de protection en temps réel.

Tableau 9. Nombre de processus de protection en temps réel

Paramètre	Nombre de processus pour la protection en temps réel.
Description	Ce paramètre appartient au groupe **Paramètres d'optimisation** de Kaspersky Embedded Systems Security. Grâce à ce paramètre, vous pouvez définir un nombre fixe de processus qui serviront à Kaspersky Embedded Systems Security pour l'exécution de la protection en temps réel. La valeur plus élevée de ce paramètre accélère l'analyse des objets dans les tâches liées à la protection en temps réel. Toutefois, plus le nombre de processus de travail affectés à Kaspersky Embedded Systems Security est élevé, plus grand sera l'impact sur les performances globales de l'ordinateur protégé et sur son utilisation de la mémoire vive. N'oubliez pas que la console d'administration de l'application Kaspersky Security Center vous permet de définir le paramètre **Nombre de processus de protection en temps réel** uniquement pour Kaspersky Embedded Systems Security sur un ordinateur distinct (dans la boîte de dialogue **Paramètres de l'application**) ; vous ne pouvez pas modifier ce paramètre dans les propriétés de la stratégie pour le groupe d'ordinateurs.
Valeurs possibles	Valeurs possibles : 1-N, où N est la valeur définie par le paramètre **Quantité maximale de processus actifs**. Si vous attribuez au paramètre **Nombre de processus de protection en temps réel** une valeur égale au nombre maximum de processus actifs, vous diminuez l'impact de Kaspersky Embedded Systems Security sur la vitesse de l'échange de fichiers entre les postes de travail et l'ordinateur, tout en augmentant sa vitesse de réaction pendant la protection en temps réel. Toutefois, les tâches de mise à jour et les tâches d'analyse à la demande avec la priorité de base **Moyenne** (**Normal**) seront exécutées dans les processus de Kaspersky Embedded Systems Security déjà lancés. Les tâches d'analyse à la demande seront exécutées plus lentement. Si l'exécution de la tâche entraîne un échec, son relancement prendra plus de temps. Les tâches d'analyse à la demande avec la priorité de base **faible** (**Low**) seront toujours exécutées dans un processus ou dans des processus séparés.

<table>
<tr><td>Valeur par défaut</td><td>Kaspersky Embedded Systems Security réalise une montée en capacité automatique en fonction du nombre de processeurs sur le serveur :<table><tr><th>Nombre de processeurs</th><th>Nombre de processus pour la protection en temps réel</th></tr><tr><td>=1</td><td>1</td></tr><tr><td>>1</td><td>2</td></tr></table></td></tr>
</table>

- nombre de processus de travail pour les tâches d'analyse à la demande en mode arrière-plan.

Tableau 10. Nombre de processus pour les tâches d'analyse à la demande en mode arrière-plan.

Paramètre	Nombre de processus pour les tâches d'analyse à la demande en mode arrière-plan.
Description	Ce paramètre appartient au groupe **Paramètres d'optimisation** de Kaspersky Embedded Systems Security. Grâce à ce paramètre, vous pouvez définir le nombre maximum de processus que Kaspersky Embedded Systems Security utilisera pour l'exécution de l'analyse à la demande en mode arrière-plan. Le nombre de processus que vous définissez à l'aide de ce paramètre ne fait pas partie du total des processus de travail de Kaspersky Embedded Systems Security défini à l'aide du paramètre **Quantité maximale de processus actifs**. Par exemple, si vous spécifiez les valeurs des paramètres comme ci-dessous : • Nombre maximum de processus actifs – 3 ; • Nombre de processus pour les tâches de protection en temps réel – 3 ; • Nombre de processeurs pour les tâches d'analyse à la demande en mode arrière-plan – 1 ; Et puis que vous lancez la tâche de protection en temps réel et une tâche d'analyse à la demande en mode arrière-plan, le nombre total de processus de

	travail de kavfswp.exe de Kaspersky Embedded Systems Security est de 4. Un processus de travail de faible priorité peut exécuter plusieurs tâches d'analyse à la demande. Vous pouvez augmenter le nombre de processus de travail, par exemple si vous lancez simultanément plusieurs tâches en mode arrière-plan, afin d'attribuer des processus distincts à chaque tâche. L'attribution de processus distincts aux tâches augmente la fiabilité de l'exécution de ces tâches ainsi que la vitesse.
Valeurs possibles	1-4
Valeur par défaut	1

- Dans le groupe **Interaction avec l'utilisateur**, configurez l'affichage de l'icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches (cf. section « Icône de Kaspersky Embedded Systems Security dans la zone de notification de la barre des tâches » à la page 27) à chaque lancement de l'application.

- L'onglet **Sécurité et fiabilité** permet de configurer les paramètres suivants :

  - Dans le groupe **Paramètres de restauration**, indiquez le nombre de tentatives de restauration des tâches d'analyse à la demande en cas d'échec suite à une erreur.

Tableau 11. Récupération automatique

Paramètre	Restauration des tâches (**Réaliser la restauration des tâches**).
Description	Ce paramètre appartient au groupe **Paramètres de restauration** de Kaspersky Embedded Systems Security. Il active la restauration des tâches lorsque celles-ci se solde par une erreur et définit le nombre de tentatives de restauration des tâches d'analyse à la demande. Lorsqu'une tâche se solde par un échec, le processus kavfs.exe de Kaspersky Embedded Systems Security tente de relancer le processus dans lequel cette tâche était exécutée au moment de l'arrêt. Si la restauration des tâches est désactivée, Kaspersky Embedded Systems Security ne restaure pas les tâches d'analyse à la demande et de

	protection en temps réel. Si la restauration des tâches est activée, Kaspersky Embedded Systems Security tente de restaurer les tâches de protection en temps réel jusqu'à la réussite de l'opération et tente de restaurer les tâches d'analyse à la demande autant de fois que le précise le paramètre.
Valeurs possibles	Activée / désactivée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 1-10.
Valeur par défaut	La restauration des tâches est activée. Nombre de tentatives de restauration des tâches d'analyse à la demande : 2.

- Le groupe **Action lors du passage à une source d'alimentation continue** permet de choisir les actions de Kaspersky Embedded Systems Security dans le cadre de l'alimentation de secours.

Tableau 12. Utilisation de la source d'alimentation de secours

Paramètre	Actions à exécuter en cas d'alimentation via la batterie.
Description	Ce paramètre définit les actions exécutées par Kaspersky Embedded Systems Security lorsque l'ordinateur fonctionne sur l'alimentation électrique de secours.
Valeurs possibles	Lancer ou pas les tâches d'analyse à la demande qui ont été programmées. Exécuter ou arrêter toutes les tâches d'analyse à la demande lancées.
Valeur par défaut	Par défaut, lorsque l'ordinateur utilise une source d'alimentation de secours, Kaspersky Embedded Systems Security fonctionne selon le mode suivant : • N'exécute pas les tâches d'analyse à la demande qui ont été programmées ; • Arrête automatiquement toutes les tâches d'analyse à la demande lancées.

- Le groupe **Paramètres d'application du mot de passe** permet de configurer les paramètres de protection par mot de passe lors de l'accès aux fonctions de l'application.

- Sous l'onglet **Paramètres de connexion** :
  - Définissez les paramètres d'utilisation du serveur proxy dans le groupe **Paramètres du serveur proxy**.
  - Dans le groupe **Paramètres d'authentification du serveur proxy**, indiquez le type d'authentification et les données requises pour l'authentification sur le serveur proxy.
  - Dans le groupe **Licence**, indiquez si Kaspersky Security Center doit être utilisé en guise de serveur proxy pour l'activation de l'application.
- Sur l'onglet **Diagnostic des échecs** :
  - Si vous souhaitez enregistrer les informations de débogage dans un fichier, cochez la case **Consigner les informations de débogage dans le fichier de trace**.
    - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de trace.
    - Configurez le niveau de détail des informations de débogage.

    La liste déroulante permet de sélectionner le niveau de détail des informations de débogage que Kaspersky Embedded Systems Security consigne dans le fichier de trace.

    Vous avez le choix parmi les niveaux de détail suivants :

    - **Evénements critiques** : Kaspersky Embedded Systems Security enregistre dans le fichier de trace uniquement les informations relatives aux événements critiques.
    - **Erreurs** : Kaspersky Embedded Systems Security enregistre dans le fichier de trace les informations relatives aux événements critiques et aux erreurs.
    - **Evénements importants** : Kaspersky Embedded Systems Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs et aux événements importants.

- **Evénements d'information** : Kaspersky Embedded Systems Security enregistre dans le fichier de trace les informations relatives aux événements critiques, aux erreurs, aux événements importants et aux événements d'information.
- **Toutes les informations de débogage** : Kaspersky Embedded Systems Security enregistre dans le fichier de trace toutes les informations de débogage.

Le niveau de détail à définir pour résoudre le problème qui se pose est déterminé par l'expert du Support Technique.

Le niveau de détail sélectionné par défaut est **Toutes les informations de débogage**.

La liste déroulante est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée.

- Indiquez la taille maximale du fichier de trace.
- Indiquez les modules à déboguer.

Liste des codes de sous-systèmes de Kaspersky Embedded Systems Security dont les informations de débogage sont enregistrées dans le fichier de trace. Les codes des sous-systèmes doivent être séparés par une virgule et en respectant la distinction entre majuscules et minuscules (cf. tableau ci-dessous).

Tableau 13. Les codes des sous-systèmes Kaspersky Embedded Systems Security

Code de sous-système	Nom du sous-système
*	Tous les composants.
gui	Sous-système de l'interface utilisateur, composant logiciel enfichable de Kaspersky Embedded Systems Security dans Microsoft Management Console.
ak_conn	Sous-système d'intégration à l'agent d'administration de Kaspersky Security Center.
bl	Processus directeur ; exécute la tâche d'administration de Kaspersky Embedded Systems Security.
wp	Processus de travail ; exécute la tâche de protection antivirus.
blgate	Processus d'administration à distance de Kaspersky Embedded Systems Security.
ods	Sous-système d'analyse à la demande.
oas	Sous-système de protection des fichiers en temps réel.
qb	Sous-système de la quarantaine et des sauvegardés.
scandll	Module auxiliaire de recherche de virus.
core	Sous-système des fonctions de base du programme antivirus.
avscan	Sous-système de traitement du programme antivirus.
avserv	Sous-système de contrôle du noyau du programme antivirus.
prague	Sous-système des fonctions de base.
updater	Sous-système de mise à jour des bases de données et des modules du programme.
snmp	Sous-système de prise en charge du protocole SNMP.
perfcount	Sous-système des compteurs de performance.

Les paramètres de traçage du composant logiciel enfichable de Kaspersky Embedded Systems Security (gui) et du plug-in d'administration de Kaspersky Embedded Systems Security pour Kaspersky Security Center (ak_conn) sont appliqués après le relancement de ces composants. Les paramètres de traçage des sous-systèmes de prise en charge du protocole

SNMP (snmp) sont appliqués après le relancement du service SNMP. Les paramètres de traçage du sous-système des compteurs de performances (perfcount) sont appliqués après le relancement de tous les processus qui utilisent des compteurs de performance. Les paramètres de traçage des autres sous-systèmes de Kaspersky Embedded Systems Security sont appliqués directement après l'enregistrement des paramètres de diagnostic des échecs.

Kaspersky Embedded Systems Security enregistre par défaut les informations de débogage du fonctionnement de tous les sous-systèmes de Kaspersky Embedded Systems Security (recommandé).

Le champ est accessible si la case **Consigner les informations de débogage dans le fichier de trace** est cochée.

- Si vous souhaitez créer un fichier dump, cochez la case **Créer un fichier dump lors d'un incident**.
  - Dans le champ en dessous, désignez le dossier dans lequel Kaspersky Embedded Systems Security enregistrera le fichier dump.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump de mémoire en clair.

3. Cliquez sur **OK**.

Les paramètres de fonctionnement de Kaspersky Embedded Systems Security seront enregistrés.

Administration de Kaspersky Embedded Systems Security via une Console sur un autre ordinateur

Il est possible d'administrer Kaspersky Embedded Systems Security depuis une Console installée sur un ordinateur distant.

Pour administrer l'application via la console de Kaspersky Embedded Systems Security sur un ordinateur distant, confirmez que :

- Les utilisateurs de la console de Kaspersky Embedded Systems Security sur l'ordinateur distant sont ajoutés au groupe ESS Administrators sur l'ordinateur à protéger.
- Les connexions réseau sont autorisées pour le processus du service Kaspersky Security Management kavfsgt.exe, si le Pare-feu Windows est activé sur l'ordinateur à protéger.
- 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 l'ordinateur distant est protégé par un mot de passe, vous devez l'introduire pour accéder à l'administration de l'application via la Console.

Configuration de la zone de confiance

Cette section contient des informations sur la zone de confiance de Kaspersky Embedded Systems Security, sur les instructions pour ajouter des objets à la zone de confiance et sur l'application de la zone de confiance aux tâches de Kaspersky Embedded Systems Security.

Dans cette section

Présentation de la zone de confiance de Kaspersky Embedded Systems Security

La zone de confiance est la liste des exclusions de la zone de protection ou d'analyse que vous pouvez créer et utiliser dans les tâches d'analyse à la demande, de protection des fichiers en temps réel.

Si lors de l'installation de Kaspersky Embedded Systems Security, vous aviez cochez les cases **Ajouter les exclusions recommandées par Microsoft** et **Ajouter les fichiers recommandés par Kaspersky Lab aux exclusions**, Kaspersky Embedded Systems Security ajoute à la zone de confiance les fichiers recommandés par Microsoft et Kaspersky Lab pour les tâches de protection en temps réel.

Vous pouvez créer une zone de confiance de Kaspersky Embedded Systems Security selon les règles suivantes :

- **Processus de confiance**. La zone de confiance contient les objets sollicités par les processus des applications sensibles aux interceptions de fichier.
- **Opérations de sauvegarde**. La zone de confiance reprend les objets sollicités lors des opérations des systèmes de sauvegarde des disques durs sur des périphériques externes.
- **Exclusions**. La zone de confiance reprend les objets, indiqués par leur emplacement et/ou l'objet détectés dans ceux-ci.

Vous pouvez utiliser la zone de confiance dans les tâches Protection des fichiers en temps réel, dans les tâches d'analyse à la demande définies par l'utilisateur nouvellement créées et dans toutes les tâches système d'analyse à la demande, à l'exception de la tâche Analyse des objets en quarantaine.

Par défaut, la zone de confiance est appliquée dans les tâches de protection des fichiers en temps réel et dans les tâches d'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 ordinateur.

Processus de confiance

Applicable aux tâches de protection des fichiers en temps réel.

Certaines applications de l'ordinateur peuvent fonctionner de manière instable si les fichiers qu'elles utilisent sont interceptés par l'application 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 en temps réel des objets sollicités 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 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 http://www.microsoft.com/fr-fr (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 s'il est actualisé, Kaspersky Embedded Systems Security l'exclura de la liste des processus de confiance.

Kaspersky Embedded Systems Security n'utilise pas la valeur du chemin vers le fichier sur l'ordinateur local pour l'identification un processus comme étant de confiance. Le chemin d'accès au fichier sur l'ordinateur local 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.

Pendant la sauvegarde des données des disques durs sur des périphériques externes, vous pouvez désactiver la fonction de protection en temps réel 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

Intervient dans les tâches de protection des fichiers en temps réel et d'analyse à la demande.

Vous pouvez sélectionner les tâches dans lesquelles vous souhaitez appliquer chacune des exclusions ajoutées à la zone de confiance. Vous pouvez également exclure des objets de l'analyse séparément dans le cadre de la configuration des paramètres du niveau de sécurité de chaque tâche de Kaspersky Embedded Systems Security.

Vous pouvez ajouter à la zone de confiance des objets en fonction de leur emplacement sur l'ordinateur ou en fonction du nom ou du masque de nom de l'objet détecté dans ces objets. Vous pouvez également utiliser les deux paramètres.

Sur la base de l'exclusion, Kaspersky Embedded Systems Security peut ignorer des objets dans les tâches indiquées en fonction des paramètres suivants :

- Objets à détecter désignés selon le nom ou le masque du nom dans les zones désignées de l'ordinateur ;
- Tous les objets détectés dans les zones indiquées de l'ordinateur ;
- Objets à détecter désignés selon le nom ou le masque de nom dans toute la zone de protection ou d'analyse.

Activation et désactivation de l'application de la zone de confiance dans les tâches de Kaspersky Embedded Systems Security

La zone de confiance est appliquée par défaut dans les tâches Protection des fichiers en temps réel, dans les tâches d'analyse à la demande définies par l'utilisateur recréées et dans toutes les tâches système d'analyse à la demande, sauf la tâche Analyse des objets en 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 Kaspersky Embedded Systems Security, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer l'application 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 dans le groupe correspondant, 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. Si vous voulez configurer les paramètres de la zone de confiance, cliquez sur le lien placé dans le nom de la case **Appliquer la zone de confiance** (cf. section « **Ajout des exclusions à la zone de confiance** » à la page 66).
5. Cliquez sur **OK**.

Les modifications seront enregistrées.

Ajout d'exclusions à la zone de confiance

Cette section fournit des instructions sur l'ajout d'exclusions uniques à la zone de confiance de Kaspersky Embedded Systems Security.

Dans cette section

Ajout de processus à la liste des 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'ordinateur protégé.
- Sélectionner le fichier exécutable du processus sans savoir si ce processus est exécuté ou non en ce moment.

  Si le fichier exécutable du processus change, Kaspersky Embedded Systems Security l'exclut de la liste des processus de confiance.

► *Pour ajouter un processus à la liste des processus de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Processus de confiance** et cochez la case **Ne pas surveiller les actions sur les fichiers des processus spécifiés**.
4. Cliquez sur **Ajouter**.

   La fenêtre **Ajout d'un processus de confiance** s'ouvre.
5. Ajoutez un processus de confiance à l'aide d'une des méthodes suivantes :

   - Pour ajouter un processus de la liste des processus exécutés, procédez comme suit :

     a. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **Processus**.

     La fenêtre **Processus actifs** s'ouvre.

     b. Dans la fenêtre **Processus actifs**, sélectionnez le processus souhaité dans la liste des processus en exécution et cliquez sur **OK**.

     Les données du processus indiqué sont ajoutées automatiquement au groupe **Critères de confiance**.

     > Le compte utilisateur sous les privilèges duquel la tâche de protection des fichiers en temps réel est lancée doit posséder les autorisations d'administrateur sur l'ordinateur 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, le PID ou le chemin d'accès au fichier exécutable du processus sur l'ordinateur local.

- Si vous souhaitez indiquer le fichier exécutable du processus, procédez comme suit :

    a. Dans la fenêtre **Ajout d'un processus de confiance**, cliquez sur le bouton **Parcourir**.

    Une fenêtre standard de sélection de fichier Microsoft Windows s'ouvre.

    b. Sélectionnez le fichier exécutable du processus, puis cliquez sur le bouton **OK**.

    Les données du fichier indiqué sont ajoutées automatiquement au groupe **Critères de confiance**.

    > Kaspersky Embedded Systems Security n'utilise pas la valeur du chemin vers le fichier sur l'ordinateur local pour l'identification un processus comme étant de confiance. Le chemin d'accès au fichier sur l'ordinateur local 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.

6. Choisissez les critères de confiance dont il faut tenir compte pour le fichier exécutable ou le processus sélectionnés :

    - Utiliser le chemin d'accès complet pour déterminer la confiance du processus.

        Si la case est cochée, Kaspersky Embedded Systems Security détermine l'état de confiance du processus sur la base du fichier d'accès complet au dossier.

        Si la case n'est pas cochée, le chemin d'accès au dossier contenant le fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

        Cette case est cochée par défaut.

    - Utiliser le hash du fichier pour déterminer la confiance du processus.

        Si la case est cochée, Kaspersky Embedded Systems Security détermine l'état de confiance du processus sur la base du hash du fichier sélectionné.

        Si la case n'est pas cochée, le hash du fichier n'est pas pris en compte en tant que critère de définition de l'état de confiance du processus.

Cette case est cochée par défaut.

> Pour ajouter le processus ou le fichier exécutable à la liste des processus de confiance, il faut choisir au moins un critère de confiance.

7. Dans la fenêtre **Ajout d'un processus 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**.

Suppression d'un processus de la liste des processus de confiance

► *Pour désactiver l'application d'un processus de confiance dans la zone de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.

2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.

3. Dans la fenêtre **Zone de confiance**, choisissez l'onglet **Processus de confiance** et dans la liste des processus de confiance proposée, décochez la case en regard du nom du fichier exécutable que vous souhaitez exclure temporairement de la zone de confiance.

4. Cliquez sur **OK**.

La fenêtre **Zone de confiance** se ferme ; les processus sélectionnés seront supprimés de la liste des processus de confiance.

Désactivation de la protection des fichiers en temps réel pendant la copie de sauvegarde

► *Pour désactiver la protection des fichiers en temps réel pendant la copie de sauvegarde depuis les disques durs, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Processus de confiance** et cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers**.
4. Cliquez sur **OK**.

La fenêtre **Zone de confiance** se ferme ; la protection des fichiers en temps réel sera suspendue pendant la copie de sauvegarde.

Ajout d'une exclusion à la zone de confiance

► *Pour ajouter une exclusion à la zone de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**.
2. Choisissez l'option **Configurer les paramètres de la zone de confiance**.

   La fenêtre **Zone de confiance** s'ouvre.
3. Sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Exclusion** s'ouvre.
4. Dans le groupe **L'objet ne sera pas analysé lorsque les conditions suivantes seront remplies**, indiquez les objets que vous souhaitez exclure de la zone de protection / d'analyse et les objets que vous souhaitez exclure de la liste des objets à détecter (par exemple, un utilitaire d'administration à distance) :

   - Si vous souhaitez exclure un objet de la zone de protection / d'analyse, procédez comme suit :

     a. Cochez la case **Objet à analyser**.

        Ajout d'un fichier, d'un dossier, d'un disque ou d'un fichier de script à l'exclusion.

        Quand la case est cochée, Kaspersky Embedded Systems Security ignore la zone définie, le fichier, le dossier, le disque ou le fichier de script désigné lors de l'analyse à l'aide du composant de Kaspersky Embedded Systems Security sélectionné dans le groupe **Zone d'application de la règle**.

        Cette case est cochée par défaut.

     b. Cliquez sur le bouton **Modifier**.

     La fenêtre **Sélection de l'objet** s'ouvre.

     c. Dans la fenêtre qui s'ouvre, indiquez l'objet que vous souhaitez exclure

de la zone d'analyse.

> Vous pouvez utiliser pour ce faire les caractères génériques ? et *.

- Si vous souhaitez indiquer le nom de l'objet à détecter, procédez comme suit :

  a. Cochez la case **Objets à détecter**.

     Exclusion des objets à détecter de l'analyse selon le nom ou le masque de nom de l'objet à détecter. La liste des noms des objets à détecter est disponible sur le site de l'Encyclopédie des virus (https://securelist.fr).

     Si la case est cochée, Kaspersky Embedded Systems Security ignore les objets à détecter indiqués pendant l'analyse.

     Si la case est décochée, Kaspersky Embedded Systems Security détecte tous les objets indiqués par défaut dans l'application.

     Cette case est décochée par défaut.

  b. Cliquez sur le bouton **Modifier**.

  La fenêtre **Liste des objets à détecter** s'ouvre.

  c. Dans la fenêtre qui s'ouvre, indiquez le nom ou le masque du nom de l'objet à détecter conformément à la classification de l'Encyclopédie des virus (https://securelist.fr).

- Dans le groupe **Zone d'application de l'exclusion**, cochez les cases en regard du nom des tâches qui appliqueront l'exclusion.

5. Cliquez sur **OK**.

L'exclusion ajoutée apparaît dans la liste sous l'onglet **Exclusions** de la fenêtre **Zone de confiance**.

Gestion des tâches de Kaspersky Embedded Systems Security

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.

Dans cette section

Catégories des tâches de Kaspersky Embedded Systems Security

Les fonctions de la protection en temps réel, du contrôle de l'ordinateur, de l'analyse à la demande et de la mise à jour de Kaspersky Embedded Systems Security sont réalisées sous la 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 la barre d'outils ou du volet 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 dans Kaspersky Embedded Systems Security : *locales* et *de groupe*.

Tâches locales

Les tâches locales sont uniquement exécutées sur l'ordinateur protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- **Tâches système locales**. Ces tâches sont créées automatiquement lors de l'installation de Kaspersky Embedded Systems Security. Vous pouvez modifier les paramètres de toutes les tâches système à l'exception des tâches Analyse des objets en quarantaine et Annulation de la mise à jour des bases de l'application. Il est impossible de renommer ou de supprimer les tâches système. Vous pouvez lancer les tâches d'analyse à la demande système en même temps que les tâches définies par l'utilisateur.
- **Tâches locales définies par l'utilisateur**. Vous pouvez créer une tâche d'analyse à la demande dans la console de Kaspersky Embedded Systems Security. 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. C'est ce qu'on appelle les tâches définies par l'utilisateur. 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

Les tâches de groupe et les tâches pour les sélections d'ordinateurs créées via Kaspersky Security Center sont affichées dans la Console de Kaspersky Embedded Systems Security. Ces tâches sont les tâches de groupe. Vous pouvez administrer les tâches de groupe et les configurer au départ de Kaspersky Security Center. La console de Kaspersky Embedded Systems Security permet uniquement de consulter l'état des tâches de groupe.

Enregistrement d'une tâche après modification de ses paramètres

Vous pouvez modifier les paramètres d'une tâche, qu'elle soit en cours d'exécution ou arrêtée (suspendue). Les nouvelles valeurs des paramètres seront appliquées si les conditions suivantes sont remplies :

- Si vous avez modifié les paramètres d'une tâche à exécuter : les nouvelles valeurs des paramètres seront appliquées directement après l'enregistrement de la tâche ;
- Si vous avez modifié les paramètres d'une tâche arrêtée (suspendue), les nouvelles valeurs seront appliquées à la prochaine exécution de la tâche.

► *Pour enregistrer les paramètres modifiés d'une tâche :*

Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer la tâche**.

Si, après la modification des paramètres de la tâche, vous sélectionnez un autre nœud dans l'arborescence de la console sans avoir sélectionné la commande **Enregistrer la tâche**, la fenêtre d'enregistrement des paramètres s'ouvre.

► *Pour enregistrer les paramètres modifiés au moment de passer à une autre entrée de la console :*

Dans la fenêtre d'enregistrement des paramètres, cliquez sur **Oui**.

Lancement / suspension / rétablissement / arrêt manuel d'une tâche

Vous ne pouvez suspendre et reprendre que les tâches de protection en temps réel et d'analyse à la demande.

► *Pour lancer / suspendre / reprendre / arrêter une tâche, procédez comme suit :*

1. Ouvrez le menu contextuel du nom de la tâche dans la console de Kaspersky Embedded Systems Security.

2. Sélectionnez une des options : **Démarrer**, **Suspendre**, **Reprendre** ou **Arrêter**.

L'opération sera exécutée et enregistrée dans le journal d'audit système (cf. section « Journal d'audit système » à la page 338).

Quand vous suspendez, puis relancez une tâche d'analyse à la demande, Kaspersky Embedded Systems Security reprend l'analyse à l'objet qui était traité au moment de l'interruption.

Programmation des tâches

Vous pouvez planifier l'exécution des tâches de Kaspersky Embedded Systems Security et configurer les paramètres de la planification.

Dans cette section

Configuration des paramètres de planification du lancement des tâches

La console de Kaspersky Embedded Systems Security vous permet de planifier le lancement des tâches système et des tâches définies par l'utilisateur locales (cf. page 73). Vous ne pouvez pas configurer la planification du lancement des tâches de groupe.

► *Pour configurer les paramètres de planification du lancement de la tâche,* procédez comme suit *:*

1. Ouvrez le menu contextuel du nom de la tâche dont vous souhaitez configurer la planification du lancement.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Planification**, activez le lancement planifié de la tâche en cochant la case **Activé selon la programmation**.

   Les champs contenant les paramètres de planification de la tâche d'analyse à la demande et de la tâche de mise à jour ne sont pas accessibles si le lancement planifié de la tâche est interdit par une stratégie de Kaspersky Security Center.

4. Configurez l'horaire en fonction de vos besoins. Pour ce faire, procédez comme suit *:*

   a. Choisissez une des options suivantes dans la liste **Fréquence** :

   - **Chaque heure** si vous souhaitez que la tâche soit exécutée selon la fréquence horaire que vous aurez définie à l'aide du champ **Une fois toutes les <nombre> heures** ;
   - **Chaque jour** si vous souhaitez que la tâche soit exécutée selon la fréquence journalière que vous aurez définie dans le champ **Une fois tous les <nombre> jour** ;
   - **Chaque semaine** si vous souhaitez que la tâche soit exécutée selon une fréquence hebdomadaire que vous aurez définie dans le champ **Une fois toutes les <nombre> semaines**. 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 ;
   - **A 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 **Démarrer à**, l'heure de la première exécution de la tâche.

   c. Indiquez, dans le champ **A partir de**, la date d'entrée en vigueur de la programmation.

   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, dans la partie supérieure dans la fenêtre, le champ **Prochain démarrage** affiche des informations relatives au temps restant avant la nouvelle exécution de la tâche. Des informations actualisées sur le temps restant seront proposées à chaque ouverture de la fenêtre **Paramètres de la tâche** sous l'onglet **Planification**.

   La valeur **Interdit par la stratégie** dans le champ **Prochain démarrage** s'affiche si le lancement des tâches système planifiées est interdit par les paramètres d'une stratégie en vigueur de Kaspersky Security Center.

5. Sous l'onglet **Avancé**, configurez le reste des paramètres en fonction de vos besoins.

   - Dans le groupe **Paramètres d'arrêt de la tâche** :

     a. Cochez la case **Durée** et saisissez la quantité requise d'heures et de minutes dans les champs de droite afin de définir la durée maximale d'exécution de la carte.

     b. Cochez la case **Suspendre entre … et …**, puis saisissez le début et la fin de l'intervalle de temps au cours de la journée pendant lequel l'exécution de la tâche sera suspendue.

   - Dans le groupe **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 l'exécution des 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 **Appliquer**.

Les paramètres de la planification de la tâche sélectionnées seront enregistrés.

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, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security ; ouvrez le menu contextuel du nom de la tâche dont vous souhaitez planifier le lancement.

2. Choisissez l'option **Propriétés**.

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

3. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes sous l'onglet **Planification** :

   - Cochez la case **Exécuter de manière planifiée** si vous souhaitez activer l'exécution planifiée d'une tâche ;
   - Décochez la case **Exécuter de manière planifiée** si vous souhaitez désactiver l'exécution planifiée d'une tâche.

   > Les paramètres de la planification du lancement de la tâche ne seront pas supprimés. Ils seront toujours valides à la prochaine activation de l'exécution planifiée de la tâche.

4. Cliquez sur le bouton **Appliquer**.

Les paramètres configurés de l'exécution planifiée de la tâche seront 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.

Dans cette section

A propos de l'utilisation des comptes utilisateur pour l'exécution des tâches

Vous pouvez indiquer le compte utilisateur sous les autorisations duquel vous souhaitez exécuter la tâche sélectionnée pour les modules suivants de Kaspersky Embedded Systems Security :

- Tâches de génération automatique des règles du contrôle des périphériques et du contrôle du lancement des applications ;
- Tâches d'analyse à la demande ;
- Tâches de mise à jour.

Par défaut, les tâches désignées sont exécutées avec les autorisations du compte système.

Il est conseillé de définir un autre compte utilisateur avec les privilèges suffisants dans les cas suivants :

- Pour la tâche de mise à jour, si la source de mise à jour est un dossier partagé sur un autre ordinateur du réseau.
- Pour la 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).
- Pour les tâches d'analyse à la demande, si le compte système ne possède pas les autorisations d'accès à un des objets à analyser (par exemple, aux fichiers dans les dossiers réseaux partagés de l'ordinateur).
- Pour la tâche de génération automatique des règles, si à l'issue de l'exécution de la tâche, les règles générées sont importées dans un fichier de configuration situé dans un emplacement inaccessible au compte système (par exemple, dans un des dossiers réseau partagés de l'ordinateur).

Vous pouvez lancer les tâches de mise à jour, d'analyse à la demande et de génération automatique des règles du contrôle du lancement des applications avec les autorisations du compte système. Lors de l'exécution de ces tâches, Kaspersky Embedded Systems Security contacte les dossiers partagés sur l'autre ordinateur du réseau si cet ordinateur est enregistré dans le même domaine que l'ordinateur protégé. Dans ce cas, le compte système doit posséder les autorisations d'accès à ces dossiers. Kaspersky Embedded Systems Security contactera cet ordinateur avec les privilèges du compte utilisateur **<Nom_de_domaine\nom_d'ordinateur>**.

Définition du compte utilisateur pour l'exécution de la tâche

► *Pour sélectionner le compte utilisateur sous lequel la tâche sera exécutée, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de la tâche pour laquelle vous souhaitez configurer le lancement sous un autre compte utilisateur.
2. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
3. Dans la fenêtre qui s'ouvre, réalisez les opérations suivantes sous l'onglet **Exécuter en tant que** :
   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'ordinateur protégé ou dans le même domaine.

   c. Confirmez le mot de passe saisi.
4. Cliquez sur le bouton **Appliquer**.

Les paramètres modifiés d'exécution des tâches sous les autorisations du compte utilisateur sont enregistrés.

Importation et exportation des paramètres

Cette section aborde l'exportation des valeurs des paramètres de fonctionnement de Kaspersky Embedded Systems Security ou des paramètres de fonctionnement de composants distincts de l'application dans un fichier de configuration au format XML et l'importation de ces valeurs depuis le fichier de configuration dans l'application.

Dans cette section

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.

- Génération des règles pour le Contrôle des périphériques.
- Génération des règles du Contrôle du lancement des applications.
- Analyse à la demande.
- Mise à jour des bases de données et des modules de Kaspersky Embedded Systems Security.
- Quarantaine.
- Sauvegarde.
- Journaux.
- Notifications de l'administrateur et des utilisateurs.
- Zone de confiance.

Vous pouvez également exporter dans un fichier les paramètres généraux de Kaspersky Embedded Systems Security et 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 identifiants pour l'exécution des tâches ou la connexion au serveur proxy. 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 le même ordinateur où l'application a 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 ordinateur. Après l'importation des paramètres sur un autre ordinateur, vous devrez 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 dans Kaspersky Embedded Systems Security, seuls les paramètres repris dans le fichier de configuration sont modifiés. Les autres paramètres demeurent inchangés.

Les paramètres importés des tâches ne sont pas appliqués lors de l'exécution de la tâche. Pour appliquer les paramètres importés, il faut relancer la tâche.

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 dans un fichier de configuration, procédez comme suit :*

1. Dans la console de Kaspersky Embedded Systems Security, réalisez une des opérations suivantes :

   - Dans le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**, choisissez l'option **Exporter les paramètres** afin d'exporter tous les paramètres de Kaspersky Embedded Systems Security.

   - Dans le menu contextuel du nom de la tâche dont vous souhaitez exporter les paramètres, choisissez l'option **Exporter les paramètres** afin d'exporter les paramètres d'un module individuel de l'application.

   - Pour exporter les paramètres du composant Zone de confiance :

     a. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **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**.

     La fenêtre de bienvenue de l'Assistant d'exportation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : indiquez le nom du fichier de configuration dans lequel vous souhaitez enregistrer les paramètres ainsi que le chemin d'accès à celui-ci.

   Pour désigner le chemin d'accès, vous pouvez utiliser des variables système ; vous ne pouvez pas utiliser des variables utilisateur.

   > Si une stratégie de Kaspersky Security Center est active au moment de l'exportation des paramètres, l'application exporte les valeurs des paramètres de la stratégie.

3. Dans la fenêtre **L'exportation des paramètres de l'application est terminée**, cliquez sur **OK**.

L'Assistant d'exportation des paramètres se fermera et l'exportation des paramètres sera terminée.

Importation des paramètres

► *Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :*

1. Dans la console de Kaspersky Embedded Systems Security, réalisez une des opérations suivantes :

   - Dans le menu contextuel de l'entrée **Kaspersky Embedded Systems Security**, choisissez l'option **Importer les paramètres** afin d'importer tous les paramètres de Kaspersky Embedded Systems Security.
   - Dans le menu contextuel du nom de la tâche dont vous souhaitez importer les paramètres, choisissez l'option **Importer les paramètres**, afin d'importer les paramètres d'un module individuel.
   - Pour importer les paramètres du composant Zone de confiance :

     a. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **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**.

La fenêtre de bienvenue de l'Assistant d'importation des paramètres s'ouvre.

2. Suivez les instructions affichées dans les fenêtres de l'Assistant : identifiez le fichier de configuration que vous souhaitez importer.

   Une fois que les paramètres de Kaspersky Embedded Systems Security et de ses composants auront été importés sur l'ordinateur, vous ne pourrez plus revenir à leurs valeurs antérieures.

3. Dans la fenêtre **L'importation des paramètres de l'application est terminée**, cliquez sur **OK**.

   L'Assistant d'importation des paramètres se ferme ; les paramètres importés sont enregistrés.

4. Cliquez sur le bouton **Mettre à jour** dans la barre d'outils de la console de Kaspersky Embedded Systems Security.

Les paramètres importés apparaissent dans la fenêtre de la console.

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 ordinateur ou sur ce même ordinateur après une réinstallation ou de mise à jour de Kaspersky Embedded Systems Security. Après la fin de l'importation, vous devrez saisir les mots de passe manuellement.

Utilisation des modèles de paramètres de sécurité

Cette section explique l'utilisation des modèles des paramètres de sécurité dans les tâches de protection et d'analyse de Kaspersky Embedded Systems Security.

Dans cette section

Présentation des modèles des paramètres de sécurité

Vous pouvez configurer manuellement les paramètres de sécurité de l'entrée dans l'arborescence des ressources fichier du serveur 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.

L'utilisation de modèles est accessible lors de la configuration des paramètres de sécurité des 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 valeurs des paramètres de sécurité du modèle appliqué à l'entrée principale dans l'arborescence des ressources fichier du serveur sont appliquées à toutes les sous-entrées. Le modèle de l'entrée principale n'est pas appliqué aux sous-entrées dans les cas suivants :

- Si les paramètres de sécurité des sous-entrées ont été configurés séparément (cf. section « Application du modèle de paramètres de sécurité » à la page 89).
- Si les sous-entrées sont virtuelles. Il faudra alors appliquer le modèle pour chaque entrée virtuelle séparément.

Création d'un modèle de paramètres de sécurité

► *Pour enregistrer manuellement les paramètres de sécurité de l'entrée et les enregistrer dans le modèle, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
2. Dans le volet résultats 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 fichiers de l'ordinateur, sélectionnez l'entrée dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.
4. Dans la partie inférieure de la fenêtre, 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 toute information complémentaire relative au modèle.
7. Cliquez sur **OK**.

Le modèle avec la sélection de paramètres de sécurité sera conservé.

Vous pouvez également passer à la création d'un modèle de paramètres pour les tâches d'analyse à la demande depuis le volet résultats de l'entrée principale **Analyse à la demande**.

Consultation des paramètres de sécurité du modèle

► *Pour consulter les valeurs des paramètres de sécurité dans le modèle créé, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, sélectionnez la tâche dont vous souhaitez consulter le modèle de sécurité.

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 qui s'ouvre, sélectionnez le modèle que vous souhaitez consulter.

4. Cliquez sur le bouton **Voir**.

La fenêtre **<Nom du modèle>** s'ouvre. L'onglet **Général** reprend les noms des modèles et les informations complémentaires sur le modèle ; l'onglet **Paramètres** reprend la liste des valeurs des paramètres de sécurité enregistrés dans le modèle.

Application du modèle de paramètres de sécurité

► *Pour appliquer les modèles de sécurité du modèle à l'entrée sélectionnée, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.

2. Dans le volet résultats de la tâche sélectionnée, cliquez sur le lien **Configurer la zone de protection** ou **Configurer la zone d'analyse**.

3. Dans l'arborescence des ressources fichiers de l'ordinateur, ouvrez le menu contextuel de l'entrée à laquelle vous souhaitez appliquer le modèle.

4. Sélectionnez **Appliquer un modèle** → **<Nom du modèle>**.

5. Dans l'arborescence de la console, ouvrez le menu contextuel du nom de la tâche à configurer.

6. Sélectionnez l'option **Enregistrer la tâche**.

Le modèle des paramètres de sécurité sera appliqué à l'entrée sélectionnée dans l'arborescence des ressources fichier de l'ordinateur. Sous l'onglet **Niveau de sécurité** de l'entrée sélectionnée, la valeur **Personnalisé** apparaîtra.

Les valeurs des paramètres de sécurité du modèle appliqué à l'entrée principale dans l'arborescence des ressources fichier du serveur sont appliquées à toutes les sous-entrées.

Si la zone de protection ou d'analyse des sous-entrées dans l'arborescence des ressources de fichiers de l'ordinateur a été configurée séparément, les paramètres de sécurité du modèle appliqué à l'entrée principale ne sont pas appliqués automatiquement aux sous-entrées.

► *Pour définir les paramètres de sécurité du modèle pour toutes les sous-entrées, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, sélectionnez la tâche dont vous souhaitez enregistrer les paramètres de sécurité dans un modèle.

2. Dans le volet résultats 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 fichiers de l'ordinateur, choisissez l'entrée parent pour appliquer le modèle à cette entrée et à toutes les sous-entrées.

4. Sélectionnez **Appliquer un modèle** → **<Nom du modèle>**.

5. Dans l'arborescence de la console, ouvrez le menu contextuel de la tâche à configurer.

6. Sélectionnez l'option **Enregistrer la tâche**.

Le modèle des paramètres de sécurité sera appliqué à l'entrée principale et à toutes les sous-entrées dans l'arborescence des ressources fichier de l'ordinateur. Sous l'onglet **Niveau de sécurité** de l'entrée sélectionnée, la valeur **Personnalisé** apparaîtra.

Suppression du modèle de paramètres de sécurité

► *Pour supprimer un modèle de paramètres de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, sélectionnez la tâche pour la configuration de laquelle vous ne souhaitez plus utiliser un modèle de paramètres de sécurité.

2. Dans le menu contextuel de la tâche sélectionnée, sélectionnez **Modèles des paramètres**.

   Vous pouvez passer à la création d'un modèle de paramètres pour les tâches d'analyse à la demande depuis le volet résultats de l'entrée principale **Analyse à la demande**.

   La fenêtre **Modèles** s'ouvre.

3. Dans la liste des modèles de la fenêtre qui s'ouvre, sélectionnez le modèle que vous souhaitez supprimer.

4. Cliquez sur le bouton **Supprimer**.

   La fenêtre de confirmation de la suppression s'ouvre.

5. Dans la fenêtre de confirmation, cliquez sur **Oui**.

Le modèle sélectionné sera supprimé.

Si le modèle de paramètres de sécurité a été appliqué à la protection ou à l'analyse d'entrées des ressources fichiers de l'ordinateur, les paramètres de sécurité configurés pour ces entrées seront conservés après la suppression du modèle.

Protection en temps réel

Cette section contient les informations sur les tâches de protection en temps réel : Protection des fichiers en temps réel des fichiers et Utilisation du KSN. Elle explique également comment configurer les paramètres des tâches de protection en temps réel et de la sécurité de l'ordinateur protégé.

Dans cette section

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.

Dans cette section

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 de l'ordinateur protégé suivants lorsqu'ils sont sollicités :

- Les fichiers ;
- Les flux alternatifs des systèmes de fichiers (flux NTFS) ;
- L'enregistrement principal de démarrage et les secteurs d'amorçage des disques durs locaux ou des périphériques externes.

Lorsqu'un programme quelconque enregistre un fichier sur l'ordinateur ou tente de le lire, Kaspersky Embedded Systems Security intercepte le fichier, y recherche la présence éventuelle de menaces et s'il identifie une menace contre la sécurité informatique, il exécute les actions que vous avez définies dans les paramètres de la tâche ou par défaut : il tente de désinfecter le fichier, le place en quarantaine ou il le supprime. Kaspersky Embedded Systems Security rend le fichier à l'application uniquement s'il est sain ou si sa réparation a réussi.

Statistiques de la tâche Protection des fichiers en temps réel

Pendant que la tâche Protection des fichiers en temps réel est exécutée, 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 jusqu'à maintenant.

► *Pour consulter les statistiques de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

   Le volet résultats de l'entrée sélectionnée reprend les statistiques actuelles de la tâche dans le groupe **Statistiques**.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Embedded Systems Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 14. 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 application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	La quantité d'objets considérés comme infectés par Kaspersky Embedded Systems Security ou d'objets détectés qui sont des applications légitimes qui n'ont pas été exclues de la zone d'action des tâches de la protection en temps réel ou d'analyse.
Objets probablement infectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Embedded Systems Security.
Objets non désinfectés	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu désinfecter pour les raisons suivantes : • Le type d'objet détecté 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 un autre programme.
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.

Champ	Description
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 total 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** dans le groupe **Administration** du volet résultats.

Si la valeur dans le champ **Total des événements** dans la fenêtre du journal d'exécution de la tâche de la 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 **Evénements**.

Configuration des paramètres de la tâche Protection des fichiers en temps réel

Par défaut, la tâche système Protection des fichiers en temps réel contient les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 15. Paramètres par défaut de la tâche Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
Zone de protection	L'ensemble de l'ordinateur, à l'exception des disques virtuels.	Vous pouvez limiter la zone de protection.
Niveau de sécurité	Identique pour toutes les zones de protection ; correspond au niveau de sécurité **Recommandé**.	Pour les entrées sélectionnées dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez : • Appliquer un autre niveau de sécurité prédéfini ; • Modifier manuellement le niveau de sécurité ; • Enregistrer la configuration des paramètres de sécurité de l'entrée sélectionnée dans un modèle en vue de l'appliquer par la suite à n'importe quelle autre entrée.
Mode de protection	A l'accès et à la modification.	Vous pouvez sélectionner le mode de protection des objets et indiquer dans quel type d'accès aux objets Kaspersky Embedded Systems Security les analyse.
Analyseur 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.

Paramètre	Valeur par défaut	Description
Zone de confiance	Appliquée. Exclusions des fichiers recommandées par Microsoft Corporation si vous aviez choisi l'option **Ajouter les exclusions recommandées par Microsoft** lors de l'installation de Kaspersky Embedded Systems Security.	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.
Utilisation des services du KSN	Appliquée	Vous pouvez améliorer l'efficacité de la protection de l'ordinateur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Planification du lancement de la tâche	Au lancement de l'application	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

► *Pour configurer les paramètres de la tâche Protection des fichiers en temps réel, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats, passez au lien **Propriétés**.

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

4. Configurez les paramètres de la tâche suivants :

    - Sous l'onglet **Général** :

        - Mode de protection d'objets (cf. section « Sélection du mode de protection des objets » à la page 99) ;

        - Application de l'analyseur heuristique (à la page 100) ;

        - Paramètres d'intégration aux autres modules de Kaspersky Embedded Systems Security (cf. section « Intégration de la tâche aux autres modules de Kaspersky Embedded Systems Security » à la page 101).

    - Sous les onglets **Planification** et **Avancé** :

        - Paramètres de lancement de la tâche selon la planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

    Les modifications apportées aux paramètres seront enregistrées.

6. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

7. Exécutez les actions suivantes :

    - Dans l'arborescence ou dans la liste des ressources de fichiers de l'ordinateur, sélectionnez les entrées que vous souhaitez inclure dans la zone de protection de la tâche (cf. section « A propos de la zone de protection de la tâche Protection des fichiers en temps réel » à la page 108).

    - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section « Sélection des niveaux de sécurité prédéfinis » à la page 119) ou configurez manuellement les paramètres de protection des objets (cf. section « Configuration manuelle des paramètres de sécurité » à la page 122).

8. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer**.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution de la tâche.

Sélection du mode de protection des objets

La tâche Protection des fichiers en temps réel vous permet de sélectionner le mode de protection des objets. Le groupe **Mode de protection d'objets** permet de définir le type d'accès aux objets déclenchant une analyse par Kaspersky Embedded Systems Security.

Le paramètre **Mode de protection d'objets** possède une valeur unique pour toutes les zones de protection reprises dans la tâche. Vous ne pouvez pas définir différentes valeurs pour les nœuds particuliers de la zone de protection.

► *Pour sélectionner le mode de protection des objets, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, sélectionnez le mode de protection des objets que vous souhaitez définir :

   - **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 un processus contacte et modifie plusieurs fois un objet pendant son exécution, Kaspersky Embedded Systems Security analysera à nouveau cet objet uniquement après la dernière sauvegarde effectuée par ce processus.

   - **A l'accès et à la modification**.

     Kaspersky Embedded Systems Security analyse l'objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié.

     Cette option est sélectionnée par défaut.

- **A l'accès**.

  Kaspersky Embedded Systems Security analyse tous les objets lors de leur ouverture, aussi bien en lecture qu'en exécution ou en modification.

- **A l'exécution**.

  Kaspersky Embedded Systems Security analyse le fichier uniquement en cas d'ouverture pour exécution.

5. Cliquez sur **OK**.

Le mode de protection des objets sélectionné sera adopté.

Application de l'analyseur heuristique

Vous pouvez, dans la tâche Protection des fichiers en temps réel, appliquer l'analyse heuristique et configurer le niveau de l'analyse.

► *Pour configurer l'analyse heuristique, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Utiliser l'analyse heuristique**.
5. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

   Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse 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 détail pour l'analyse :

- **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. 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 dans le fichier exécutable conforme aux recommandations des experts de Kaspersky Lab.

  Il s'agit du niveau par défaut.
- **Minutieuse**. L'analyseur 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 de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

6. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Intégration de la tâche aux autres modules de Kaspersky Embedded Systems Security

La tâche Protection des fichiers en temps réel vous permet de configurer les paramètres d'intégration de la tâche aux autres modules opérationnels de Kaspersky Embedded Systems Security.

Il est indispensable d'accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

> Si vous avez accepté la Déclaration de Kaspersky Security Network pendant l'installation de l'application, la tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer une tâche manuellement (cf. section « Lancement et arrêt d'une tâche Utilisation du KSN » à la page 132) ou planifier son exécution (cf. section « Configuration des paramètres d'une tâche Utilisation du KSN » à la page 134).

► *Pour configurer les interactions entre la tâche Protection des fichiers en temps réel et les autres modules de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Configurez les paramètres suivants dans le groupe **Intégration aux autres composants** :
   - Cochez ou décochez la case **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 de fichiers des processus de confiance aux exclusions de l'analyse définies dans la configuration des paramètres de la tâche.

     Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte les opérations de fichiers des processus de confiance lors de la création de la zone de protection dans la tâche Protection des fichiers en temps réel.

     Cette case est cochée par défaut.
   - Cochez ou décochez la case **Utiliser KSN pour la protection**.

     La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

     Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

     Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

     Cette case est cochée par défaut.
5. Cliquez sur **OK**.

Les paramètres de la tâche définis seront appliqués.

Liste des 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?*

Zone de protection dans la tâche Protection des fichiers en temps réel

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.

Dans cette section

Présentation de la zone de protection dans la tâche Protection des fichiers en temps réel

Par défaut, la tâche Protection des fichiers en temps réel protège tous les objets du système de fichiers de l'ordinateur. 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 Kaspersky Embedded Systems Security, la zone de protection se présente sous la forme d'une arborescence ou d'une liste de ressources de fichiers de l'ordinateur que l'application peut contrôler. Par défaut les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de la liste.

► *Pour insérer l'affichage des ressources fichiers de l'ordinateur sous la forme de l'arborescence,*

Dans la liste déroulante du coin supérieur gauche de la fenêtre **Configuration de la zone de protection**, choisissez l'option **Afficher sous forme d'arbre**.

Les entrées de l'arborescence des ressources de fichiers de l'ordinateur sont illustrées de la manière suivante :

☑ Nœud repris dans la zone de protection.

☐ Nœud exclu de la zone de protection.

☑ Au moins une des entrées intégrées à cette entrée est exclue de la zone de protection ou les paramètres de sécurité de ces entrées diffèrent des paramètres de sécurité de cette entrée (uniquement pour mode d'affichage en arborescence).

L'icône ☑ s'affiche si toutes les sous-entrées ont été sélectionnées mais pas l'entrée principale. Dans ce cas, les modifications du contenu des fichiers et dossiers de l'entrée principale ne sont pas automatiquement prises en compte lors de la constitution de la zone de protection de la sous-entrée.

Le nom des nœuds virtuels de la zone de protection apparaît en lettres bleues.

Zones de protection prédéfinies

L'arborescence des ressources des fichiers de l'ordinateur est affichée dans le volet résultats de l'entrée **Protection des fichiers en temps réel** via le lien **Configuration de la zone de protection**. Vous pouvez configurer l'affichage des ressources fichiers sous la forme d'une liste ou d'une arborescence.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security prévoit les zones de protection prédéfinies suivantes :

- **Disques durs locaux**. Kaspersky Embedded Systems Security protège les fichiers sur les disques durs de l'ordinateur.
- **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.
- **Emplacements réseau**. Kaspersky Embedded Systems Security protège les fichiers qui sont enregistrés dans les répertoires réseau ou qui y sont lus par les applications exécutées sur l'ordinateur. Kaspersky Embedded Systems Security ne protège pas les fichiers dans les répertoires réseau lorsqu'ils sont sollicités par des applications d'autres ordinateurs.
- **Disques virtuels**. Vous pouvez inclure dans la zone de protection les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés temporairement sur l'ordinateur, par exemple les disques partagés d'une grappe.

Les zone d'analyse prédéfinies s'affichent par défaut dans l'arborescence des ressources de fichiers de l'ordinateur et acceptent l'ajout à la liste des ressources de fichiers 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 pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la Console de Kaspersky Embedded Systems Security. Pour inclure les objets d'un pseudo-disque dans la zone de protection, il faut inclure le répertoire de l'ordinateur auquel ce pseudo-disque est lié.

Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. 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).

Configuration des paramètres de l'affichage des ressources de fichiers de la zone de protection

► *Pour choisir le mode d'affichage des ressources de fichiers de l'ordinateur lors de la configuration des paramètres de la zone de protection, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.
4. Dans un gauche angle supérieur de la fenêtre ouverte déployez la liste déroulante. Exécutez une des actions suivantes :

   - Choisissez le point **Afficher sous forme d'arbre** si vous voulez que les ressources fichiers de l'ordinateur protégé s'affichent sous la forme d'une arborescence.
   - Choisissez le point **Afficher sous forme de liste** si vous voulez que les ressources fichiers de l'ordinateur protégé s'affichent sous la forme d'une liste.

   Par défaut les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de la liste.
5. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** sera fermée. Les paramètres de la tâche définis seront appliqués.

Constitution de la zone de protection

La procédure de constitution de la zone de protection dans la tâche Protection des fichiers en temps réel dépend du type d'affichage des ressources de fichiers de l'ordinateur protégé (cf. section « Configuration des paramètres de l'affichage des ressources de fichiers de la zone de protection » à la page 111). Vous pouvez configurer l'affichage des ressources fichiers sous la forme de la liste (est appliqué par défaut) ou sous la forme de l'arborescence.

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 composer la zone de protection, au départ l'arborescence des ressources de fichiers, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Cliquez sur le lien **Configurer la zone de protection** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone de protection** s'ouvre.
4. Dans la partie gauche de la fenêtre qui s'ouvre, déployez l'arborescence des ressources fichiers de l'ordinateur pour afficher tous les entrées.

5. 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 certaines entrées 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, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**) ;
     - Si vous souhaitez inclure un disque particulier du type requis, déployez 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:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:** ;
     - Si vous souhaitez inclure à la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case à côté de ce dossier ou de ce fichier.

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** sera fermée. Les paramètres de la tâche définis seront enregistrés.

► *Pour former la zone de protection, en travaillant avec la liste des ressources fichiers, exécutez les actions suivantes*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Cliquez sur le lien **Configurer la zone de protection** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone de protection** s'ouvre.

4. Pour inclure certaines entrées 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 avec le bouton droit de la souris.

    b. Dans le menu contextuel, sélectionnez l'option **Ajouter une zone de protection**.

    c. Dans la fenêtre **Ajout d'une zone de protection** qui s'ouvre, choisissez le type d'objet que vous voulez ajouter à la zone de protection :

    - **Zone prédéfinie**, si vous voulez insérer dans la zone de protection une des zones prédéfinies sur l'ordinateur protégé. Puis dans la liste déroulante choisissez la zone nécessaire.
    - **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 requise via le bouton **Parcourir**.
    - **Fichier**, si vous voulez insérer dans la zone de protection uniquement un fichier distinct sur le disque. Puis choisissez le fichier nécessaire via le bouton **Parcourir**.

    Vous ne pouvez pas ajouter un objet à la zone de protection s'il est déjà ajouté en tant qu'exclusion de la zone de protection.

5. 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 avec le bouton droit de la souris.

    b. Dans le menu contextuel choisissez le point **Ajouter une exclusion**.

    c. Dans la fenêtre **Ajouter une exclusion**, choisissez le type de l'objet que vous voulez ajouter à titre de l'exclusion de la zone de protection, de la même manière que l'ajout d'un objet à la zone de protection.

6. Pour modifier la zone de protection ou l'exclusion ajoutée, dans le menu contextuel de la zone que vous voulez modifier, choisissez l'option **Modifier la zone**.

7. Pour masquer l'affichage d'une zone de protection ou d'une exclusion ajoutée au préalable à la liste des ressources de fichiers, dans le menu contextuel de la zone que vous voulez masquer, choisissez l'option **Supprimer de la liste**.

   La 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 fichiers.

8. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** sera fermée. Les paramètres de la tâche définis 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'ordinateur est incluse dans la 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 de fichiers de l'ordinateur, cela pourrait ralentir quelque peu l'analyse des objets à l'accès.

A propos de la zone de protection virtuelle

Kaspersky Embedded Systems Security peut analyser non seulement les dossiers et les fichiers existants sur les disques durs et amovibles, mais également les dossiers et fichiers créés dynamiquement sur l'ordinateur par différents services et applications.

Si vous avez inclus tous les objets de l'ordinateur dans la zone de protection, ces entrées dynamiques seront automatiquement reprise dans la zone de protection. Toutefois, si vous souhaitez attribuer des valeurs particulières aux paramètres de protection de ces entrées dynamiques ou si vous avez sélectionné pour la protection en temps réel non pas tout l'ordinateur, mais uniquement quelques secteurs, alors pour pouvoir inclure les disques, les fichiers ou les répertoires dans la zone de protection, vous devrez d'abord les créer dans la Console de Kaspersky Embedded Systems Security ; c'est ce que l'on appelle la création d'une zone de protection virtuelle. Les disques, les fichiers ou les répertoires que vous créez existent uniquement dans la Console de Kaspersky Embedded Systems Security et non pas dans la structure du système de fichiers de l'ordinateur 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 dynamiques qui s'y trouvent ne seront pas repris automatiquement dans la zone de protection. Vous devez créer des « copies virtuelles » dans la Console de Kaspersky Embedded Systems Security et les ajouter à la zone de protection.

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 des ressources de fichiers (cf. section « Configuration des paramètres de l'affichage des ressources de fichiers de la zone de protection » à la page 111).

► *Pour ajouter à la zone de protection un disque virtuel, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Ouvrez le menu contextuel de l'entrée **Disques virtuels** et choisissez le nom du disque virtuel à créer dans la liste des noms disponibles.
6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone de protection.
7. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

► *Pour ajouter un dossier ou un fichier virtuel dans la zone de protection, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.

4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.

5. 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.

6. Dans le champ, saisissez le nom du dossier ou du fichier.

7. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone de protection.

8. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Paramètres de sécurité de l'entrée sélectionnée dans la tâche Protection des fichiers en temps réel

Dans la tâche Protection des fichiers en temps réel, 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 dans l'arborescence des ressources de fichiers de l'ordinateur.

Les paramètres de sécurité configurés pour l'entrée principale sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Vous pouvez configurer les paramètres 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 fichiers du serveur (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.

Sélection des niveaux de sécurité prédéfinis

Pour les entrées sélectionnées dans l'arborescence ou la liste des ressources de fichiers de l'ordinateur, 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

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Embedded Systems Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 16. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Paramètres	Niveau de sécurité		
	Performance maximale	**Recommandé**	**Protection maximale**
Protection des objets	Selon l'extension	En fonction du format	En fonction du format
Optimisation	Activée	Activée	Désactivée
Action à exécuter sur les objets infectés et autres détectés	Désinfecter, supprimer si la désinfection est impossible	Désinfecter, supprimer si la désinfection est impossible	Désinfecter, supprimer si la désinfection est impossible
Action à exécuter sur les objets probablement infectés	Placer en quarantaine	Placer en quarantaine	Placer en quarantaine
Exclure les objets	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 défini
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* • Objets OLE intégrés* • Uniquement les objets nouveaux et modifiés	• Archives SFX* • Objets compactés* • Objets OLE intégrés* *Tous les objets

Les paramètres **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Application de l'analyse heuristique** ne font pas partie des paramètres des niveaux de sécurité prédéfinis. Si, après avoir choisi un des niveaux de sécurité prédéfini, vous modifiez les paramètres de protection **Protection des objets**, **Utiliser la technologie iChecker**, **Utiliser la technologie iSwift**, **Utiliser l'analyse heuristique**, le niveau prédéfini que vous aviez choisi ne change pas.

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.
3. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.
4. Sélectionnez l'entrée pour laquelle vous souhaitez sélectionner un niveau de sécurité prédéfini.
5. Confirmez que ce nœud est repris dans la zone de protection.
6. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez dans la liste 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.
7. Dans le menu contextuel du nom de la tâche, sélectionnez **Enregistrer**.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution 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 toutes les zones de protection. Leurs valeurs correspondent aux valeurs du niveau de sécurité prédéfini **Recommandé** (cf. section « **Sélection des niveaux de sécurité prédéfinis** » à la page 119).

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 différentes entrées dans l'arborescence ou la liste des ressources de fichiers de l'ordinateur.

Lors de l'utilisation de l'arborescence des ressources fichiers, les paramètres de sécurité configurés pour l'entrée principale sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

► *Pour configurer manuellement les paramètres de sécurité du nœud sélectionné, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.

2. Sélectionnez le sous-nœud **Protection des fichiers en temps réel**.

3. Dans le volet résultats de l'entrée **Protection des fichiers en temps réel**, cliquez sur le lien **Configurer la zone de protection**.

   La fenêtre **Configuration de la zone de protection** s'ouvre.

4. Dans la partie gauche de la fenêtre, sélectionnez l'entrée dont vous souhaitez configurer les paramètres de sécurité.

   Pour la zone de protection sélectionnée, vous pouvez appliquer un modèle prédéfini contenant un ensemble de paramètres de sécurité (cf. section « A propos des modèles de paramètres de sécurité » à la page 87).

5. Configurez les paramètres de sécurité requis pour le nœud sélectionné en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, configurez les paramètres suivants, si nécessaire :

     Dans le groupe **Protection des objets**, indiquez les objets que vous souhaitez inclure à la zone de protection :

     - **Tous les objets**.

       Kaspersky Embedded Systems Security analyse tous les objets.

     - **Objets analysés en fonction du format**.

       Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base du format du fichier.

       La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Embedded Systems Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus**.

       Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

       La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée**.

       Kaspersky Embedded Systems Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

     - **Secteurs d'amorçage des disques MBR**.

       Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

       Quand la case est cochée, Kaspersky Embedded Systems Security analyse les secteurs et les enregistrements d'amorçage sur les disques durs et les disques amovibles du serveur.

       Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs**.

  Analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les flux complémentaires des fichiers et des dossiers.

  Cette case est cochée par défaut.

Dans le groupe **Optimisation**, cochez ou décochez la case :

- **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

  La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Embedded Systems Security a identifié comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse et protège tous les fichiers.

  La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Recommandé** ou **Protection maximale**, la case est décochée.

Dans le groupe **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone de protection :

- **Toutes les / uniquement les nouvelles archives**.

  Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les archives.

  Si la case est décochée, Kaspersky Embedded Systems Security ignore les archives lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Toutes les / Les nouvelles archives SFX**.

  Analyse des archives qui contiennent un module logiciel de décompactage.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les archives SFX.

  Si la case est décochée, Kaspersky Embedded Systems Security ignore les archives SFX lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données de messagerie**.

  Analyse des fichiers des bases de données de messagerie de Microsoft Office Outlook® et Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers des bases de données de messagerie.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers des bases de données de messagerie lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / les nouveaux objets compactés**.

  Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers exécutables compactés par des logiciels de compression.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux messages de texte plat**.

  Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers aux formats de messagerie.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers aux formats de messagerie lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés**.

  Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les objets intégrés au fichier.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les objets intégrés au fichier lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Vous pouvez choisir de protéger tous les objets composés ou uniquement les nouveaux si la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés** est cochée. Si la case **Protection uniquement des nouveaux fichiers et des fichiers modifiés** est décochée, Kaspersky Embedded Systems Security protège tous les objets composés désignés.

- Sous l'onglet **Actions**, configurez les paramètres suivants, si nécessaire :

  - Sélectionnez l'action à exécuter sur les objets infectés et autres détectés.
  - Sélectionnez l'action à exécuter sur les objets probablement infectés.
  - Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter.

- Choisissez les actions à exécuter sur les conteneurs non modifiables : cochez ou décochez la case **Forcer la suppression du fichier conteneur parent en cas de détection d'un objet infecté ou autre joint quand la modification du conteneur est impossible**.

  La case active ou désactive la suppression forcée du conteneur parent en cas de détection d'un objet intégré malveillant ou autre.

  Si la case est cochée et que **Supprimer** est l'action à exécuter sur les fichiers infectés et probablement infectés, Kaspersky Embedded Systems Security force la suppression de l'ensemble du conteneur parent en cas de détection d'un objet malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée du conteneur parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet détectable intégré (par exemple, si le conteneur parent ne peut pas être modifié).

  Si la case est décochée et que **Supprimer** est l'action à exécuter sur les fichiers infectés et probablement infectés, Kaspersky Embedded Systems Security n'exécute pas l'action indiquée pour le conteneur parent en cas de détection d'un objet malveillant ou d'un autre type d'objet à détecter intégré si ce conteneur parent n'est pas modifiable.

  La case est cochée par défaut pour le niveau de sécurité **Protection maximale**. La case est décochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- Sous l'onglet **Optimisation**, configurez les paramètres suivants, si nécessaire :

  Dans le groupe **Exclusions** :

  - **Exclure les fichiers**.

    Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

    Si la case est cochée, Kaspersky Embedded Systems Security ignore les objets indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Embedded Systems Security analyse tous les objets.

Cette case est décochée par défaut.

- **Ne pas détecter**.

  Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque de nom d'objet à détecter. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus (https://securelist.fr).

  Si la case est cochée, Kaspersky Embedded Systems Security ignore les objets à détecter indiqués pendant l'analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security détecte tous les objets indiqués par défaut dans l'application.

  Cette case est décochée par défaut.

Dans le groupe **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.)**.

  Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

  Si la case est cochée, la durée maximale de l'analyse d'un objet est égale à la valeur indiquée.

  Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

  Cette case est cochée par défaut.

- **Ne pas analyser les objets composés de plus de (Mo)**.

  Exclut de l'analyse les objets complexes dont la taille est supérieure à la valeur indiquée. La valeur par défaut est de 8 Mo.

  Si la case est cochée, Kaspersky Embedded Systems Security ne réalise pas la recherche de virus dans les objets complexes dont la taille est supérieure à la valeur indiquée.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les objets complexes sans tenir compte de la taille.

  La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- **Utiliser la technologie iChecker**.

  Analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les fichiers sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

- **Utiliser la technologie iSwift**.

  Analyse uniquement des nouveaux objets ou des fichiers objets depuis la dernière analyse dans le système de fichiers NTFS.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse du système de fichiers NTFS.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les objets du système de fichiers NTFS sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

6. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

Utilisation du KSN

Cette section contient des informations sur la tâche Utilisation du KSN et les instructions sur la configuration de cette tâche.

Dans cette section

A propos de la tâche Utilisation du KSN

Le *Kaspersky Security Network* (ci-après, KSN) est une infrastructure de services en ligne qui donne accès à la base opérationnelle des connaissances de Kaspersky Lab 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 de la protection et réduit la possibilité de faux positifs.

Il est indispensable d'accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Si vous avez accepté la Déclaration de Kaspersky Security Network pendant l'installation de l'application, la tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer une tâche manuellement (cf. section « Lancement et arrêt d'une tâche Utilisation du KSN » à la page 132) ou planifier son exécution (cf. section « Configuration des paramètres d'une tâche Utilisation du KSN » à la page 134).

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 Lab 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.

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour de plus amples informations sur la collecte, le traitement, la conservation et la destruction des informations sur l'utilisation de l'application, vous pouvez consulter le Règlement du KSN sous l'onglet **Règlement du KSN** dans la fenêtre des propriétés de la tâche Utilisation du KSN, et sur le site Internet de Kaspersky Lab https://www.kaspersky.fr/privacy.

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 participation au Kaspersky Security Network à n'importe quel moment (cf. section « Lancement et arrêt de la tâche Utilisation du KSN » à la page 132).

Kaspersky Security Network peut être utilisé dans les tâches suivantes de Kaspersky Embedded Systems Security :

- Protection des fichiers en temps réel (cf. section « Configuration des paramètres de la tâche Protection des fichiers en temps réel » à la page 96).
- Analyse à la demande (cf. section « Configuration des paramètres de la tâche d'analyse à la demande » à la page 246).
- Contrôle du lancement des applications (cf. section « Configuration des paramètres de la tâche Contrôle du lancement des applications » à la page 151).

Lancement et arrêt de la tâche Utilisation du KSN

Si vous avez accepté la Déclaration de Kaspersky Security Network pendant l'installation de l'application, la tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security.

Vous pouvez également lancer l'exécution de la tâche manuellement.

► *Pour lancer la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Sélectionnez l'onglet **Règlement du KSN**.
5. Cochez la case **J'accepte les conditions de prestation des services du KSN** si vous acceptez les conditions de la Déclaration de Kaspersky Security Network et souhaitez activer l'utilisation du KSN.

   Si la case **J'accepte les conditions de prestation des services du KSN** est décochée pendant le fonctionnement de la tâche Utilisation du KSN, cette tâche sera interrompue.
6. Cochez la case **Envoyer les statistiques sur les événements du fonctionnement de l'application** si vous souhaitez envoyer des statistiques complémentaires à KSN.

   La case active et désactive l'envoi de statistiques complémentaires à KSN. Si la case est cochée, l'application envoie les données sur les détections d'applications malveillantes, y compris les faux positifs, survenues pendant l'exécution des tâches de protection en temps réel et d'analyse à la

demande, ainsi que les informations de débogage relatives aux échecs survenus lors de l'analyse. Si la case est décochée, l'application envoie uniquement les valeurs des sommes de contrôle des fichiers analysés en vue d'obtenir les conclusions des services KSN, ainsi que des informations générales sur l'application et le système d'exploitation.

Cette case est cochée par défaut.

L'application envoie les statistiques si toutes les conditions reprises ci-dessous sont remplies :

1) La tâche Utilisation du KSN a été lancée.

2) La Déclaration de Kaspersky Security Network a été acceptée.

3) La case **Utiliser KSN pour la protection** a été cochée dans les propriétés de la tâche Protection des fichiers en temps réel ; la case **Utiliser KSN pour l'analyse** a été cochée dans les propriétés de la tâche Analyse à la demande.

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

   Les modifications des paramètres de la tâche sont enregistrées.

8. Dans le groupe **Administration** du volet résultats de l'entrée **Utilisation du KSN**, suivez le lien **Démarrer**.

La tâche Utilisation du KSN sera lancée.

Le lancement de la tâche Utilisation du KSN est impossible si le Règlement du KSN n'a pas été accepté. Avant de lancer la tâche, assurez-vous que la case **J'accepte les conditions de prestation des services du KSN** est cochée.

► *Pour arrêter la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le groupe **Administration** du volet résultats de l'entrée **Utilisation du KSN**, cliquez sur le lien **Arrêter**.

La tâche Utilisation du KSN sera arrêtée.

Configuration de la tâche Utilisation du KSN

La tâche Utilisation du KSN possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 17. Paramètres par défaut de la tâche Utilisation du KSN

Paramètre	Valeur par défaut	Description
Actions sur les objets considérés comme douteux par KSN	Supprimer	Vous pouvez préciser les actions que Kaspersky Embedded Systems Security exécutera sur les objets réputés comme étant infectés dans le KSN.
Envoi des données	La somme de contrôle (hash MD5) est calculée pour les fichiers dont la taille ne dépasse pas 2 Mo.	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 Embedded Systems Security calcule les hash MD5 pour les fichiers de n'importe quelle taille.
	La case **Envoyer les statistiques sur les événements du fonctionnement de l'application** est cochée.	Vous pouvez autoriser ou interdire l'envoi de statistiques supplémentaires sur les résultats du fonctionnement de Kaspersky Embedded Systems Security à KSN.
Règlement du KSN	La case **J'accepte les conditions de prestation des services du KSN** est décochée ou cochée.	Vous pouvez accepter la Déclaration du Kaspersky Security Network pendant l'installation de l'application. Vous pouvez modifier votre choix concernant l'utilisation du KSN à tout moment.
Planification du lancement de la tâche	Le prochain lancement n'est pas défini.	La tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security si vous avez acceptez la Déclaration du Kaspersky Embedded Systems Security pendant l'installation de l'application. Vous pouvez également lancer la tâche manuellement ou planifier son exécution.

► *Pour configurer les paramètres de la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Configurez les paramètres de la tâche :
   - Dans le groupe **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 réputé infecté dans le KSN :
     - **Supprimer**.

       Kaspersky Embedded Systems Security supprime l'objet considéré comme infecté selon les données du KSN et place une copie de celui-ci dans la sauvegarde.

       Cette option est sélectionnée par défaut.
     - **Consigner les informations dans le rapport**.

       Kaspersky Embedded Systems Security consigne dans le journal d'exécution des tâches les informations sur l'objet considéré comme infecté selon les données du KSN détecté. Kaspersky Embedded Systems Security ne supprime pas l'objet infecté.
   - Dans le groupe **Envoi des données**, limitez la taille des fichiers pour lesquels il faut calculer la somme de contrôle :
     a. Cochez ou décochez la case **Ne pas calculer la somme de contrôle pour l'envoi au KSN si la taille du fichier dépasse (Mo)**.

        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.

b. Le cas échéant, saisissez dans le champ de droite la taille maximale des fichiers pour lesquels Kaspersky Embedded Systems Security calculera la somme de contrôle.

c. Décochez ou cochez la case **Envoyer les statistiques sur les événements du fonctionnement de l'application** si vous voulez envoyer des statistiques complémentaires à KSN.

La case active et désactive l'envoi de statistiques complémentaires à KSN. Si la case est cochée, l'application envoie les données sur les détections d'applications malveillantes, y compris les faux positifs, survenues pendant l'exécution des tâches de protection en temps réel et d'analyse à la demande, ainsi que les informations de débogage relatives aux échecs survenus lors de l'analyse. Si la case est décochée, l'application envoie uniquement les valeurs des sommes de contrôle des fichiers analysés en vue d'obtenir les conclusions des services KSN, ainsi que des informations générales sur l'application et le système d'exploitation.

Cette case est cochée par défaut.

5. Si nécessaire, 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'ordinateur.

L'application lancera la tâche Utilisation du KSN selon la planification.

Le lancement de la tâche Utilisation du KSN est impossible si le Règlement du KSN n'a pas été accepté. Avant de lancer la tâche, assurez-vous que la case **J'accepte les conditions de prestation des services du KSN**, sous l'onglet **Règlement du KSN** est cochée.

6. Cliquez sur **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'exécution de la tâche.

Statistiques concernant la tâche Utilisation du KSN

Pendant que la tâche Utilisation du KSN est exécutée, 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 d'une tâche sont consignés dans le journal d'exécution de la tâche (cf. section « A propos des journaux d'exécution des tâches » à la page 342).

► *Pour consulter les statistiques de la tâche Utilisation du KSN, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Protection en temps réel**.
2. Sélectionnez la sous-entrée **Utilisation du KSN**.

Le volet résultats de l'entrée sélectionnée reprend les statistiques actuelles de la tâche dans le groupe **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).

Tableau 18. Statistiques concernant la tâche Utilisation du KSN

Champ	Description
Requêtes fichier envoyées	Nombre de requêtes sur la réputation de fichiers que Kaspersky Embedded Systems Security a envoyées aux services du KSN pour examen.
Conclusions suspectes reçues	Nombre d'objets identifiés comme douteux par les services du KSN.
Erreurs d'envoi des requêtes	Nombre de requêtes à KSN dont le traitement a entraîné une erreur de tâche.
Objets supprimés	Nombre d'objets que Kaspersky Embedded Systems Security a supprimé 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 enregistrées 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 répare pas et ne supprime pas les fichiers qui n'ont pas pu être placés dans la sauvegarde. Les informations relatives à ces objets sont enregistrées dans le journal d'exécution de la tâche.

Protection contre les exploits

Cette section contient les instructions de configuration des paramètres de la protection de la mémoire des processus contre l'exploitation des vulnérabilités.

Dans cette section

A propos de la protection contre les exploits

Kaspersky Embedded Systems Security donne la possibilité de protéger la mémoire des processus contre les Exploits via le composant Protection contre les exploits. Vous pouvez modifier l'état de l'activité du composant, ainsi que configurer les paramètres de protection des processus contre l'exploitation des vulnérabilités.

Le composant protège la mémoire des 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 externe 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.

Le déchargement de l'Agent des processus protégés implique qu'ils soient arrêtés : 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. Pour exécuter la suppression du composant en présence des processus protégés dans le système, le redémarrage de l'ordinateur protégé peut être requis.

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 du discrédit de la vulnérabilité dans le processus.

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.

Si lors de la suppression, l'Agent est intégré dans au moins un des processus protégés, le redémarrage de l'ordinateur protégé est requis.

Service Kaspersky Security Broker Host

Pour une efficacité maximale de l'exécution des fonctions, le composant Protection contre les exploits doit posséder le service Kaspersky Security Broker Host sur l'ordinateur protégé. Ce service fait partie de l'installation recommandée avec le composant Protection contre les exploits. Lors de l'installation du service sur l'ordinateur protégé, le processus kavfswh est créé et lancé ; il fournit à l'Agent de protection les informations sur les processus protégés contre le composant.

Après l'arrêt du service Kaspersky Security Broker Host, Kaspersky Embedded Systems Security continue de protéger les processus qui ont été ajoutés à la liste des processus protégés, puis est chargé dans les nouveaux processus ajoutés et applique toutes les techniques disponibles de réduction de l'impact pour protéger la mémoire des processus.

En cas d'arrêt du service Kaspersky Security 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, 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.

Modes 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 les processus exploités : 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 le processus protégé auquel un niveau critique est attribué dans le système d'exploitation, Kaspersky Embedded Systems Security ne termine pas ce processus quel que soit le mode indiqué dans les paramètres du composant Protection contre les exploits.

- Informer uniquement sur l'Exploit : appliquez ce mode pour recevoir les données d'exploitation des vulnérabilités dans les processus protégés à l'aide des événements dans le Journal des violations de la sécurité.

  Si ce mode est sélectionné, Kaspersky Embedded Systems Security consigne toutes les tentatives d'exploitation des vulnérabilités en créant des événements.

Configuration des paramètres de protection de la mémoire des processus

► *Pour ajouter un processus à la liste des processus protégés, procédez comme suit :*

1. Sélectionnez l'entrée principale **Kaspersky Embedded Systems Security** dans l'arborescence de la Console.

2. Dans le groupe **Protection** du volet résultats, cliquez sur le lien **Statistiques uniquement**.

   La fenêtre **Paramètres de protection contre l'exploitation de vulnérabilités** s'ouvre.

3. Configurez les paramètres de protection de la mémoire des processus :

   - **Protéger la mémoire des processus contre l'exploitation de vulnérabilités en mode**.

     Si la case est cochée, Kaspersky Embedded Systems Security réduit l'impact de l'exploitation des vulnérabilités des processus se trouvant dans la liste des processus protégés.

     Si la case est décochée, Kaspersky Embedded Systems Security ne protège pas les processus sur l'ordinateur contre l'exploitation des vulnérabilités.

     Cette case est décochée par défaut.

   - **Terminer les processus exploités**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security termine le processus protégé en cas de détection d'une tentative d'exploitation de la vulnérabilité à laquelle s'applique une technique active de réduction de l'impact.

   - **Statistiques uniquement**.

     Si ce mode est sélectionné, Kaspersky Embedded Systems Security signale l'exploitation d'une vulnérabilité en affichant la fenêtre de terminal à l'écran. Le processus exploité continue d'être exécuté.

     Si lors du fonctionnement de l'application sous le mode *Terminer les processus exploités*, Kaspersky Embedded Systems Security détecte un cas d'exploitation de vulnérabilité d'un processus critique, le composant passe forcément au mode *Communiquer uniquement sur l'Exploit*.

4. Configurez les paramètres suivants dans le groupe **Actions de réduction de l'impact** :

   - **Signaler les processus exploités via le service de terminal**

     Si la case est cochée, Kaspersky Embedded Systems Security affiche à l'écran la fenêtre de terminal en décrivant le motif de déclenchement de la protection et en indiquant le processus dans lequel la tentative d'exploitation de la vulnérabilité a été détectée.

     Si la case est décochée, Kaspersky Embedded Systems Security n'affiche pas à l'écran la fenêtre de terminal lors de la détection du cas de tentative d'exploitation de la vulnérabilité ou d'achèvement du processus exploités.

La fenêtre de terminal s'affiche quel que soit l'état de fonctionnement du service Kaspersky Security Broker Host.

Cette case est cochée par défaut.

- **Appliquer la protection contre l'exploitation de vulnérabilités quel que soit l'état du service Kaspersky Security**.

  Si la case est cochée, Kaspersky Embedded Systems Security réduit l'impact de l'exploitation des vulnérabilités des processus déjà lancés quel que soit l'état d'exécution du service Kaspersky Security. Kaspersky Embedded Systems Security ne protégera pas les processus ajoutés après l'arrêt du service Kaspersky Security. Une fois le service lancé, la réduction de l'impact de l'exploitation des vulnérabilités de tous les processus sera arrêtée.

  Si la case est décochée, Kaspersky Embedded Systems Security ne protège pas les processus contre l'exploitation des vulnérabilités à l'arrêt du service Kaspersky Security.

  Cette case est cochée par défaut.

5. Dans la fenêtre **Paramètres de protection contre l'exploitation de vulnérabilités**, cliquez sur le bouton **OK**.

   Kaspersky Embedded Systems Security enregistre les paramètres définis et les applique à la protection des processus.

Ajout d'un processus protégé

► *Pour ajouter un processus à la liste des processus protégés, procédez comme suit :*

1. Sélectionnez l'entrée principale **Kaspersky Embedded Systems Security** dans l'arborescence de la Console.

2. Dans le groupe **Protection** du volet résultats, cliquez sur le lien **Protection contre les exploits**.

   La fenêtre **Zone de protection** s'ouvre.

3. Ajoutez le processus à la liste des processus protégés en procédant 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.

4. Sélectionnez le processus ajouté dans la liste.

5. Les paramètres en vigueur apparaissent sous l'onglet **Paramètres de protection du processus** :

    - **Etat**.
    - **Chemin d'accès au fichier exécutable**.
    - **Techniques de réduction de l'impact**.

6. Pour modifier les techniques de réduction de l'impact appliquées à processus, sélectionnez l'onglet **Configurer l'application de la technique de réduction de l'impact**.

7. Choisissez une des options d'application de la technique de réduction de l'impact :

    - **Appliquer toutes les techniques de réduction de l'impact disponibles**.

      Si vous choisissez cette option, le contenu de la liste ne peut être modifié, toutes les techniques sont appliquées par défaut.

    - **Appliquer les techniques de réduction de l'impact indiquées**.

      Si vous avez choisi cette option, vous pouvez modifier la liste des techniques de réduction de l'impact à appliquer en cochant les cases en regarde des techniques en question.

8. Le groupe **Lancement de modules depuis un processus** permet de configurer les paramètres de fonctionnement de la technique de réduction de l'impact **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
        - Sites de confiance
        - Sites à accès restreint
        - Ordinateur

        > Ces données sont applicables uniquement à Internet Explorer.

9. Cliquez sur **OK**.

Techniques de réduction de l'impact

Tableau 19. Techniques de réduction de l'impact

Technique de réduction de l'impact	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 Exeption 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.
Export Adress Table Access Moitor (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
Heapspray Allocation	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 suspectes (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).

Technique de réduction de l'impact	Description
Attack Surface Reduction	Interdiction du lancement de modules vulnérables via le processus protégé.

Contrôle de l'ordinateur

Cette section contient des informations sur la fonction de Kaspersky Embedded Systems Security qui permet de contrôler le lancement des applications, la connexion de disques flash et autres périphériques externes USB. Elle traite également du contrôle du fonctionnement du pare-feu Windows.

Dans cette section

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.

Dans cette section

Présentation de la tâche Contrôle du lancement des applications

Au cours de l'exécution de la tâche Contrôle du lancement des applications, Kaspersky Embedded Systems Security surveille les tentatives de lancement des applications par les utilisateurs et autorise ou interdit l'opération. La tâche Contrôle du lancement des applications repose sur la technologie de blocage par défaut (Default Deny) qui suppose le blocage automatique du lancement de n'importe quelle application interdite dans les paramètres de la tâche.

Vous pouvez autoriser le lancement des applications d'une des manières suivantes :

- définir des règles d'autorisation pour les applications de confiance ;
- tenir compte de la réputation des applications de confiance dans KSN au moment de leur lancement.

  L'interdiction du lancement de l'application possède la priorité absolue : si le lancement de l'application est bloqué par un composant de la tâche Contrôle du lancement des applications, le lancement de cette application sera bloqué quelles que soient les conclusions des autres composants de la tâche. Par exemple, si l'application est considérée comme douteuse par les services KSN, mais qu'elle est couverte par une règle d'autorisation, le lancement de cette application sera interdit.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution des tâches (cf. section « A propos des journaux d'exécution des tâches » à la page 342).

La tâche Contrôle du lancement des applications est exécutée selon un des deux modes suivants :

- **Appliquer les règles du Contrôle du lancement des applications**. Kaspersky Embedded Systems Security contrôle, à l'aide de règles définies, le lancement des applications qui entrent dans la zone d'application des règles de la tâche Contrôle du lancement des applications. La zone d'application des règles de la tâche 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 de la tâche Contrôle du lancement des applications, et que ses paramètres ne respectent aucune des règles du Contrôle du lancement des applications, le lancement de cette application sera interdit.

Le lancement des applications n'entrant pas dans la zone d'application des règles, telle que définie dans les paramètres de la tâche Contrôle du lancement des applications, est autorisé, indépendamment des paramètres des règles du Contrôle du lancement des applications.

Le lancement de la tâche Contrôle du lancement des applications en mode **Appliquer les règles du Contrôle du lancement des applications** est impossible si aucune règle n'a été définie ou si le nombre de règles définies pour un seul ordinateur est supérieur à 65 535.

- **Statistiques uniquement**. Kaspersky Embedded Systems Security ne contrôle pas le lancement des applications à l'aide des règles du Contrôle du lancement des applications et consigne simplement dans le journal d'exécution des tâches les informations sur les lancements des applications et les règles du Contrôle du lancement des applications que respectent les applications exécutées. Le lancement de toutes les applications est autorisé. Il s'agit du mode par défaut.

  Ce mode permet de composer la liste des règles du Contrôle du lancement des applications sur la base des informations fixées dans le journal d'exécution des tâches (cf. section « Composition de la liste des règles sur la base des événements de la tâche Contrôle du lancement des applications » à la page 177).

Vous pouvez organisez le fonctionnement de la tâche Contrôle du lancement des applications conformément à un des scénarios suivants :

- Configuration étendue des règles et leur application au Contrôle du lancement des applications.
- Configuration minimale des règles et l'utilisation du KSN pour le contrôle du lancement des applications (cf. section « Utilisation du KSN dans la tâche Contrôle du lancement des applications » à la page 157).

Si les fichiers système tombent sous le coup de l'application de la tâche Contrôle du lancement des applications, assurez-vous lors de la création des règles du Contrôle du lancement des applications que le lancement de ces applications est autorisé par les règles créées. Dans le cas contraire, le système d'exploitation pourrait ne pas démarrer.

Configuration des paramètres de la tâche Contrôle du lancement des applications

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.

Tableau 20. Paramètres par défaut de la tâche Contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Mode de fonctionnement de la tâche	**Statistiques uniquement**. La tâche consigne dans le journal d'exécution tous les événements de blocage et de lancement des applications conformément aux règles définies. Le lancement des applications n'est pas vraiment bloqué.	Vous pouvez sélectionner **Appliquer les règles du Contrôle du lancement des applications** pour protéger l'ordinateur après la composition de la liste définitive des règles.
Zone d'application des règles dans la tâche	La tâche contrôle l'exécution des fichiers exécutables, des scripts et des paquets MSI.	Vous pouvez indiquer les types de fichier dont l'exécution sera contrôlée par les règles.
Utilisation du KSN	Les données sur la réputation des applications dans KSN ne sont pas utilisées.	Vous pouvez utiliser les conclusions de KSN sur la réputation des applications dans le fonctionnement de la tâche Contrôle du lancement des applications.
Autorisation de la diffusion des applications pour les paquets d'installation	Pas appliqué.	Vous pouvez autoriser automatiquement l'installation ou la mise à jour du logiciel via les paquets d'installation indiqués.

Paramètre	Valeur par défaut	Description
indiqués		
Autorisation de la diffusion des applications via Windows Installer	Appliquée.	Vous pouvez autoriser l'installation ou la mise à jour de n'importe quel logiciel si les opérations sont exécutées via Windows Installer.
Planification du 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.

► *Pour configurer les paramètres de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Configurez les paramètres de la tâche suivants :
   - Sous l'onglet **Général** :
     - Mode de fonctionnement de la tâche Contrôle du lancement des applications (cf. section « Sélection du mode de fonctionnement de la tâche Contrôle du lancement des applications » à la page 153).

- Zone d'application des règles dans la tâche (cf. section « Composition de la zone d'application de la tâche Contrôle du lancement des applications » à la page 155).
- Utilisation du KSN (cf. section « Utilisation du KSN dans la tâche Contrôle du lancement des applications » à la page 157).

- Sous l'onglet **Contrôle de distribution de logiciels** :
  - Paramètres du contrôle de la diffusion du logiciel (cf. section « Composition de la liste des distributions des paquets de confiance » à la page 160).
- Sous les onglets **Planification** et **Avancé** :
  - Paramètres de lancement de la tâche selon la planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

6. Dans la partie inférieure du volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Règles du contrôle du lancement des applications**.

7. Le cas échéant, modifiez la liste des règles du Contrôle du lancement des applications.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur l'heure de modification des paramètres, ainsi que les valeurs des paramètres avant et après leur modification, sont enregistrées dans le journal d'exécution de la tâche.

Sélection du mode de fonctionnement de la tâche Contrôle du lancement des applications

► *Pour configurer le mode de fonctionnement de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Dans le volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Sélectionnez le mode d'exécution de la tâche dans la liste **Mode de fonctionnement de la tâche Contrôle du lancement des applications**.

   La liste déroulante vous permet de sélectionner l'un des modes d'exécution de la tâche Contrôle du lancement des applications :

   - **Appliquer les règles du Contrôle du lancement des applications**. Kaspersky Embedded Systems Security contrôle le lancement des applications à l'aide des règles indiquées.
   - **Statistiques uniquement**. Kaspersky Embedded Systems Security ne contrôle pas le lancement des applications à l'aide des règles indiquées et consigne simplement dans le journal d'exécution des tâches les informations sur les lancements des applications. 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 consignées dans le journal d'exécution des tâches.

   Par défaut, la tâche Contrôle du lancement des applications s'exécute en mode **Statistiques uniquement**.

5. Décochez ou cochez la case **Traiter les lancements répétés des applications contrôlées selon le schéma de traitement du premier lancement**.

   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 interdit ou autorise l'exécution d'un nouveau lancement de l'application sur la base de la décision prise au premier lancement de l'application par la tâche de contrôle du lancement des applications. Par exemple, si le premier lancement de l'application avait été autorisé par les règles du Contrôle du lancement des applications, l'enregistrement relatif à cet événement est enregistré dans le

cache et le nouveau lancement de cette application sera autorisé, sans vérification additionnelle de la présence de règles d'autorisation.

Si la case est désactivée, Kaspersky Embedded Systems Security analyse l'application à chacun de ses lancements ultérieurs.

Cette case est cochée par défaut.

Kaspersky Embedded Systems Security dresse une nouvelle liste de précédents dans le cache à chaque modification des paramètres de la tâche Contrôle du lancement des applications. Ainsi, le lancement des applications est contrôlé conformément aux paramètres de sécurité actuels.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Toutes les tentatives de lancement des applications sont consignées dans le journal d'exécution des tâches.

Composition de la zone d'application de la tâche Contrôle du lancement des applications

► *Pour créer une zone d'application de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Définissez les valeurs des paramètres suivants dans le groupe **Zone d'application des règles** :

   - **Utiliser les règles pour les fichiers exécutables**.

     La case active/désactive le contrôle du lancement des fichiers exécutables

des applications.

Si la case est cochée, Kaspersky Embedded Systems Security autorise ou interdit le lancement des fichiers exécutables des applications à l'aide des règles indiquées et dont les paramètres prévoient la couverture des Fichiers exécutables par la zone d'application.

Si la case est décochée, Kaspersky Embedded Systems Security ne contrôle pas le lancement des fichiers exécutables des applications à l'aide des règles indiquées. Le lancement des fichiers exécutables des applications est autorisé.

Cette case est cochée par défaut.

- **Contrôle du chargement des modules DLL**.

  La case active/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 et dont les paramètres prévoient la couverture des Fichiers exécutables par la zone d'application.

  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 accessible si la case **Utiliser les règles pour les fichiers exécutables** est cochée.

  Cette case est décochée par défaut.

  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**.

  La case active ou désactive le contrôle du 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 et dont les paramètres prévoient la couverture des Scripts et paquets MSI par la zone d'application.

  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.

5. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Utilisation du KSN dans la tâche Contrôle du lancement des applications

Il est indispensable d'accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

> Si vous avez accepté la Déclaration de Kaspersky Security Network pendant l'installation de l'application, la tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer une tâche manuellement (cf. section « Lancement et arrêt d'une tâche Utilisation du KSN » à la page 132) ou planifier son exécution (cf. section « Configuration des paramètres d'une tâche Utilisation du KSN » à la page 134).

Lors de l'utilisation des données du KSN sur la réputation des applications dans la tâche Contrôle du lancement des applications, la réputation de l'application dans KSN est le critère d'autorisation ou d'interdiction du lancement de cette application. Kaspersky Embedded Systems Security obtient une conclusion douteuse de KSN lors de la tentative de lancement d'une application, le lancement de cette application est interdit. Kaspersky Embedded Systems Security obtient une conclusion de confiance de KSN lors de la tentative de lancement d'une application, le lancement de cette application est autorisé. Vous pouvez appliquer KSN avec les règles du Contrôle du lancement des applications ou à titre de critère indépendant pour le blocage du lancement des applications.

Application des conclusions du KSN en tant que critère indépendant du blocage du lancement des applications

Ce scénario permet de contrôler sans danger le lancement des applications sur l'ordinateur protégé sans configuration étendue de la liste des règles.

Vous pouvez appliquer les conclusions du KSN dans le fonctionnement de Kaspersky Embedded Systems Security avec la seule règle spécifiée. L'application autorise uniquement le lancement

des applications qui ont reçu un état de confiance du KSN ou qui sont autorisées par la 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 au principe de blocage par défaut. L'application du KSN en l'absence de règles permet de protéger l'ordinateur 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 du KSN avec les règles du Contrôle du lancement des applications, les scénarios suivants peuvent se dérouler :

- Kaspersky Embedded Systems Security bloque toujours le lancement de l'application si celle-ci tombe sous le coup d'au moins une règle d'interdiction. Si l'application est considérée comme une application de confiance par les services KSN, cette conclusion possède une priorité inférieure et n'est pas prise en compte ; l'application sera de toute manière bloquée. Cela permet d'enrichir manuellement la liste des applications indésirables.

- Kaspersky Embedded Systems Security interdit toujours le lancement d'une application si le lancement des applications considérées comme douteuses par KSN est interdit et si cette application est considérée comme douteuse par les services de KSN. Si une règle d'autorisation a été définie pour cette 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'ordinateur 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 préalable des règles.

► *Pour configurer les paramètres d'utilisation des services KSN dans la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Dans le volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Définissez dans le groupe **Utilisation du KSN** les paramètres d'utilisation des services KSN :

   - Le cas échéant, cochez la case **Interdire le lancement des programmes n'étant pas des programmes de confiance dans le KSN**.

     La case active ou désactive le contrôle du lancement des applications selon leur réputation dans le KSN.

     Si la case est cochée, Kaspersky Embedded Systems Security interdit le lancement des applications étant considérées comme douteuses dans le KSN. Dans ce cas, les règles d'autorisation du contrôle du lancement des applications couvrant des applications considérées comme douteuses dans le KSN ne se déclenchent pas. 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 considérées comme douteuses dans le KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

     Cette case est décochée par défaut.

   - Le cas échéant, cochez la case **Autoriser le lancement des programmes étant des programmes de confiance dans le KSN**.

     La case active ou désactive le contrôle du lancement des applications selon leur réputation dans le KSN.

     Si la case est cochée, Kaspersky Embedded Systems Security autorise le lancement des applications considérées comme douteuses dans le KSN. De plus, 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, mais qu'elle est interdite par les règle du Contrôle du lancement des applications, le lancement de cette application sera interdit.

Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte la réputation des applications considérées comme douteuses dans KSN et autorise ou interdit leur lancement conformément aux règles couvrant ces applications.

Cette case est décochée par défaut.

- Si la case **Autoriser le lancement des programmes étant des programmes de confiance dans 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 **Sélectionnez Utilisateurs ou Groupes** s'ouvre.

  b. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

  c. Cliquez sur le bouton **OK**.

5. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Composition de la liste des distributions des paquets de confiance

Vous pouvez simplifier la procédure d'installation ou de mise à jour du logiciel avec l'aide de la fonction du contrôle de distribution de logiciels. Le contrôle de distribution de logiciels permet d'autoriser automatiquement le lancement d'applications si celui-ci implique une application de confiance ou une distribution des paquets de confiance. Après le lancement de la distribution des paquets de confiance, Kaspersky Embedded Systems Security calcule automatiquement le hash de chacun des fichiers joints et n'applique plus par la suite le principe de blocage par défaut de ces fichiers. Kaspersky Embedded Systems Security autorise le décompactage de la distribution des paquets de confiance et le lancement de tous les fichiers joints si le lancement de ceux-ci n'est pas

interdit par les règles de la tâche Contrôle du lancement des applications ou s'ils ne sont pas considérés comme douteux dans KSN.

La modification ou le déplacement d'un fichier joint peut entraîner l'interdiction du lancement de ce fichier.

► *Pour ajouter une distribution des paquets de confiance, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sous l'onglet sélectionné, cochez la case **Autoriser automatiquement la diffusion à l'aide des applications et des paquets d'installation indiqués**.

   La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide des applications et des paquets d'installation repris dans la liste.

   Si la case est cochée, l'application autorise automatiquement le lancement des fichiers exécutés à l'aide des distributions des paquets de confiance. La liste des applications et des distributions qui peuvent être lancées est modifiable.

   Si la case est décochée, l'application ne tient pas compte des exclusions indiquées dans la liste.

   Cette case est décochée par défaut.

   Vous pouvez cocher la case **Autoriser automatiquement la diffusion à l'aide des applications et des paquets d'installation indiqués** si la case **Utiliser les règles pour les fichiers exécutables** est cochée dans les paramètres de la tâche Contrôle du lancement des applications.

5. Le cas échéant, décochez la case **Toujours autoriser la diffusion des applications à l'aide de Windows Installer**.

   La case active ou désactive la possibilité de créer automatiquement des exclusions pour tous les fichiers lancés à l'aide du sous-système Windows Installer.

   Si la case est cochée, l'application autorise toujours le lancement des fichiers installés à l'aide de Windows Installer.

   Si la case est décochée, l'utilisation de Windows Installer pour le lancement de l'application n'est pas un critère d'autorisation pour cette application.

   Cette case est cochée par défaut.

   La case ne peut être modifiée si la case **Autoriser automatiquement la diffusion à l'aide des applications et des paquets d'installation indiqués** n'est pas cochée.

   Il est conseillé de décocher la case **Toujours autoriser la diffusion des applications à l'aide de Windows Installer** uniquement dans les cas extrêmes. La désactivation de ce paramètre peut entraîner des problèmes lors de la mise à jour des fichiers du système d'exploitation ainsi que l'interdiction du lancement des fichiers enfants de la distribution des paquets de confiance.

6. 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)**.

   La case active ou désactive l'autorisation automatique de la diffusion du logiciel avec l'aide de la solution System Center Configuration Manager.

   Si la case est cochée, Kaspersky Embedded Systems Security autorise automatiquement le déploiement de Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de diffuser une application uniquement à l'aide du service de transfert intelligent en arrière-plan (Background Intelligent Transfer Service).

   Le système contrôle le lancement des objets qui portent les extensions suivantes :

- .exe
- .msi

Cette case est décochée par défaut.

> L'application contrôle le cycle de diffusion de l'application depuis la remise du paquet sur l'ordinateur jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la diffusion avait été réalisée avant l'installation du système sur l'ordinateur.

7. Pour modifier la liste des distributions des paquets de confiance, cliquez sur le bouton **Modifier la liste de paquets** et dans le menu qui s'ouvre, sélectionnez une des méthodes proposées :

- **Ajouter un manuellement.**

a. Cliquez sur le bouton **Parcourir** et sélectionnez le fichier de lancement de l'application ou le paquet d'installation.

Les données du fichier sélectionné sont ajoutées automatiquement au groupe **Critères de confiance**.

b. 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**

Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Cette option est conseillée si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

Cette option est sélectionnée par défaut.

- **Utiliser le hash SHA256**

Si cette option est sélectionnée, la valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la valeur de la somme de contrôle indiquée.

Il est conseillé d'appliquer cette option pour créer les règles les plus fiables : la somme de contrôle calculée selon l'algorithme SHA256 est le seul identifiant de ce fichier. L'utilisation de la valeur du hash obtenue en guise de critère de déclenchement de la règle réduit la zone d'application des règles à un fichier.

- **Ajouter plusieurs paquets d'installation 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 lorsque le système d'exploitation sollicite les fichiers indiqués.

- **Modifier l'élément 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 depuis un fichier texte**.

  Vous pouvez importer la liste des distributions des paquets de confiance depuis le fichier de configuration enregistré. Pour être reconnu par Kaspersky Embedded Systems Security, le fichier doit répondre aux paramètres suivants :

  - posséder une extension de fichier texte ;
  - contenir des informations présentées sur la forme d'une liste de lignes contenant chacune des données pour un fichier de confiance ;
  - contenir une liste correspondant à un des deux formats suivants :
    - <nom du fichier>:<hash SHA256> ;

- <hash SHA256>*<nom du fichier>.

Dans la fenêtre **Ouvrir**, désignez le fichier de configuration contenant la liste des distributions des paquets de confiance.

8. 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 le paquet d'installation**. Le lancement des fichiers intégrés sera autorisé.

   Pour interdire le lancement des fichiers intégrés, supprimez complètement l'application de l'ordinateur protégé ou créez une règle d'interdiction dans les paramètres de la tâche Contrôle du lancement des applications.

9. Cliquez sur **OK**.

Les paramètres de la tâche définis seront enregistrés.

A propos des règles du Contrôle du lancement des applications

Principes 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 d'applications et sont respectivement nommées règles *d'autorisation* et règles *d'interdiction*. Pour créer des listes de règles d'autorisation du contrôle du lancement des applications, vous pouvez utiliser la tâche de création de règles d'autorisation (cf. section « A propos de la tâche Génération des règles du Contrôle du lancement des applications » à la page 179) ou le mode **Statistiques uniquement** dans la tâche Contrôle du lancement des applications (cf. section « Composition de la liste des règles selon les événements de la tâche Contrôle du lancement des applications » à la page 177) ; Vous pouvez ajouter des règles d'autorisation manuellement (cf. section « Ajout d'une règle du Contrôle du lancement des applications » à la page 172) une à une.

- Utilisateur et / ou groupe d'utilisateurs.

  Les règles du Contrôle du lancement des applications contrôlent les lancements des applications initiés par l'utilisateur et / ou le groupe d'utilisateurs défini dans la règle.

- Zone d'application des règles.

  Les règles du Contrôle du lancement des applications peuvent s'appliquer aux lancements des *fichiers exécutables des applications* ou aux lancements des *scripts* et *paquets MSI*.

- Critères de déclenchement de la règle.

  Les règles du Contrôle du lancement des applications contrôlent le lancement des fichiers répondant à un critère défini dans les paramètres de la règle : présenter le *certificat numérique* indiqué, disposer du *hash SHA256* indiqué ou être situé à l'*emplacement* indiqué.

  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 :

  - **Utiliser l'en-tête**.

    La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que critère de déclenchement de la règle.

    Si la case est cochée, l'en-tête du certificat numérique indiqué sera utilisé en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications uniquement pour l'éditeur repris dans l'en-tête.

    Si la case est décochée, l'application n'utilise pas les en-têtes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, la règle contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quel en-tête.

    L'en-tête du certificat numérique dont dispose le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Indiquer les critères de déclenchement de la règle à partir des propriétés du fichier**, situé

sous le groupe **Critère de déclenchement de la règle**.

Cette case est décochée par défaut.

- **Utiliser l'empreinte**.

  La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de déclenchement de la règle.

  Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de déclenchement de la règle. La règle créée contrôlera le lancement des applications signées par le certificat numérique doté de l'empreinte indiquée.

  Si la case est décochée, l'application n'utilise pas les empreintes de certificat numérique en tant que critère de déclenchement de la règle. Si le critère **Certificat numérique** est sélectionné, l'application contrôlera le lancement des applications signées à l'aide du certificat numérique portant n'importe quelle empreinte.

  L'empreinte du certificat numérique dont dispose le fichier ne peut être indiquée que depuis les propriétés du fichier à l'aide du bouton **Indiquer les critères de déclenchement de la règle à partir des propriétés du fichier**, situé sous le groupe **Critère de déclenchement de la règle**.

  Cette case est décochée par défaut.

Le recours à 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 la règle : certificat numérique, hash SHA256 ou chemin d'accès au fichier. Des exclusions des règles du Contrôle du lancement des applications peuvent se justifier pour préciser des règles d'autorisation : par exemple, si vous souhaitez permettre aux utilisateurs de lancer les applications au chemin C:\Windows, mais que vous souhaitez interdire l'exécution du fichier Regedit.exe.

Si les fichiers système tombent sous le coup de l'application de la tâche Contrôle du lancement des applications, assurez-vous lors de la création des règles du Contrôle du lancement des applications que le lancement de ces applications est autorisé par les règles créées. 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.

Suppression des règles du Contrôle du lancement des applications

► *Pour supprimer des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du volet résultats de l'entrée **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. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.

5. Cliquez sur le bouton **Supprimer la sélection**.

6. Cliquez sur le bouton **Enregistrer**.

Les règles du Contrôle du lancement des applications sélectionnées seront supprimées.

Exportation des règles du Contrôle du lancement des applications

► *Pour exporter des règles du Contrôle du lancement des applications dans un fichier de configuration, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Dans la partie inférieure du volet résultats de l'entrée **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. Cliquez sur le lien **Exporter vers un fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.

5. 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.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la règle seront exportés dans le fichier indiqué.

Vérification du lancement des applications

Avant d'appliquer les règles du Contrôle du lancement des applications définies, vous pouvez les tester sur n'importe quelle application afin d'identifier les règles qui contrôlent le lancement de l'application sélectionnée.

Par défaut, Kaspersky Embedded Systems Security bloque les applications dont le lancement n'est contrôlé par aucune application. Pour éviter le blocage du lancement d'applications importantes, il faut créer des règles d'autorisation pour celles-ci.

Si le lancement de l'application est contrôlé par plusieurs règles de différents types, les règles d'interdiction ont la priorité : le lancement de l'application est bloqué si elle est couverte par au moins une règle d'interdiction.

► *Pour tester des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du volet résultats de l'entrée **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. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Afficher les règles pour le fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.
5. 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 des règles reprend toutes les règles trouvées qui seront déclenchées au lancement du fichier indiqué.

Présentation de la formation de la liste des règles du Contrôle du lancement des applications

Vous pouvez importer une liste de règles du Contrôle du lancement des applications depuis des fichiers XML créés automatiquement lors de l'exécution de la tâche Contrôle du lancement des applications ou de la tâche Génération des règles du Contrôle du lancement des applications. Les listes contenues dans ces fichiers XML peuvent servir uniquement à la création de règles d'autorisation du Contrôle du lancement des applications.

Les règles d'interdiction du Contrôle du lancement des applications sont créées manuellement. Le lancement des applications pour lesquelles aucune règle n'a été trouvée est également interdit.

Utilisation de la tâche Génération des règles du Contrôle du lancement des applications

Le fichier XML créé à la fin de la tâche Génération des règles du Contrôle du lancement des applications contient les règles d'autorisation pour le lancement des applications désignées lors de la configuration des paramètres de la tâche lors de son lancement. Pour les applications dont le lancement n'est pas autorisé dans les paramètres de la tâche, aucune règle ne sera créée et leur exécution sera bloquée par défaut.

Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles de la tâche Contrôle du lancement des applications.

Utilisation du rapport de la tâche Contrôle du lancement des applications en mode Statistiques uniquement

Le fichier XML obtenu à la fin de la tâche Contrôle du lancement des applications en mode **Statistiques uniquement** 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 tous les lancements d'application sur l'ordinateur à protéger dans le journal d'exécution de la tâche. Vous pouvez créer des règles d'autorisation en fonction des événements de la tâche et les exporter dans un fichier XML. Avant de lancer la tâche en mode **Statistiques uniquement**, vous devez configurer la période d'exécution de la tâche de telle sorte que tous les scénarios possibles du fonctionnement de l'ordinateur à protéger aient pu se dérouler pendant l'intervalle de temps et que l'ordinateur ait redémarré au moins une fois.

Les fichiers XML qui contiennent la liste des règles d'autorisation, sont créés sur la base de l'analyse des tâches lancées sur l'ordinateur à protéger. Le lancement de la tâche de génération automatique des règles d'autorisation et du Contrôle du lancement des applications en mode **Statistiques uniquement** pour composer les listes doit être réaliser sur la machine modèle de l'organisation afin de tenir compte de toutes les applications utilisées sur le réseau.

Avant de composer la liste des règles d'autorisation pour les applications lancées sur la machine modèle de l'organisation, assurez-vous que celle-ci n'est pas infectés par des applications malveillantes.

Vous pouvez utiliser la liste de règles obtenues suite à l'analyse du lancement des applications sur la machine modèle, lors de la configuration de la stratégie de contrôle du serveur depuis Kaspersky Security Center et de l'application des règles d'autorisation créées pour l'ensemble du réseau.

Dans cette section

Ajout d'une règle du Contrôle du lancement des applications

► *Pour ajouter une règle du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.
3. Dans la partie inférieure du volet résultats de l'entrée **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. Cliquez sur **Ajouter**.
5. Dans le menu contextuel du bouton, choisissez l'option **Ajouter une règle**.

   La fenêtre contextuelle **Paramètres des règles** s'ouvre.

6. 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 la règle :

- **Autorisé**, si vous souhaitez que la règle autorise le lancement des applications conformément aux critères définis dans les paramètres de la règle.
- **Interdit**, 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 des applications.
- **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et paquets MSI.

    d. Dans le champ **Utilisateur et / 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 :

        i. Cliquez sur le bouton **Sélectionner**.

        ii. La fenêtre standard de Microsoft Windows **Sélectionnez Utilisateur ou Groupes** s'ouvre.

        iii. Indiquez la liste des utilisateurs et/ou groupes d'utilisateurs.

        iv. 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 le groupe **Critère de déclenchement de la règle**, depuis un fichier :

        i. Cliquez sur le bouton **Définir le critère de déclenchement du fichier depuis les propriétés du fichier**.

        La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

        ii. Sélectionnez le fichier et cliquez sur le bouton **OK**.

Les valeurs des critères du fichier s'afficheront dans les champs du groupe **Critère 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 **Critère de déclenchement de la règle**, sélectionnez une des options suivantes :

- **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'en-tête**, 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 indiquée.
    - Cochez la case **Utiliser l'empreinte**, si vous souhaitez que la règle contrôle 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.

g. Réalisez les opérations suivantes si vous souhaitez ajouter des exclusions pour une règle :

i. Dans le groupe **Exclusions de la règle**, cliquez sur le bouton **Ajouter**.

La fenêtre **Exclusion de la règle** s'ouvre.

ii. Dans le champ **Nom**, saisissez le nom de l'exclusion de la règle.

iii. Indiquez les paramètres d'exclusions des fichiers du lancement 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**.

  Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide de fichiers disposant de la signature d'un certificat numérique.

  Ce critère est sélectionné par défaut.

  - **Utiliser l'en-tête**.

  La case active ou désactive l'utilisation de l'en-tête du certificat numérique en tant que critère de rattachement des fichiers aux exclusions de la règle.

  Si la case est cochée, l'en-tête du certificat numérique indiqué sera utilisé en tant que critère de rattachement des fichiers aux exclusions de la règle. L'application ne rattache aux exclusions de la règle que les fichiers disposant d'un certificat numérique portant cet en-tête.

  Si la case est décochée, l'en-tête du certificat numérique indiqué ne sera pas utilisé en tant que critère de rattachement des fichiers aux exclusions de la règle. Si le critère **Certificat numérique** est sélectionné, l'application rattache aux exclusions de la règle les fichiers disposant de la signature d'un certificat numérique portant n'importe quel en-tête.

  L'en-tête du certificat numérique dont dispose le fichier ne peut être défini que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des propriétés d'un fichier**.

  Cette case est décochée par défaut.

  - **Utiliser l'empreinte**.

  La case active ou désactive l'utilisation de l'empreinte du certificat numérique en tant que critère de rattachement des fichiers aux exclusions de la règle.

  Si la case est cochée, l'empreinte du certificat numérique indiquée sera utilisée en tant que critère de rattachement des fichiers aux exclusions de la règle. L'application ne rattache aux exclusions de la règle que les fichiers disposant d'un certificat numérique portant cette empreinte.

  Si la case est décochée, l'empreinte du certificat numérique indiquée ne sera pas utilisée en tant que critère de rattachement des fichiers aux exclusions de la règle. Si le critère **Certificat numérique** est sélectionné,

l'application rattache aux exclusions de la règle les fichiers disposant de la signature d'un certificat numérique portant n'importe quelle empreinte.

L'empreinte du certificat numérique dont dispose le fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des propriétés d'un fichier**.

Cette case est décochée par défaut.

- **Hash SHA256**.

  Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide d'un fichier présentant la somme de contrôle indiquée.

  La somme de contrôle du fichier ne peut être définie que depuis les propriétés du fichier à l'aide du bouton **Définir l'exclusion sur la base des propriétés d'un fichier**.

- **Chemin du fichier**.

  Si ce critère est sélectionné, l'application rattache aux exclusions les applications exécutées à l'aide de fichiers situés à l'emplacement indiqué.

i. Cliquez sur le bouton **OK**.

ii. Répétez les points (i) à (iv) pour ajouter des exclusions supplémentaires.

7. Dans la fenêtre **Paramètres des règles**, cliquez sur **OK**.

La règle créée sera affichée dans la liste de la fenêtre **Règles du contrôle du lancement des applications**.

Composition de la liste des règles selon les événements de la tâche Contrôle du lancement des applications

► *Pour créer le fichier de configuration contenant la liste des règles du Contrôle du lancement des applications formée sur la base des événements de l'exécution de la tâche Contrôle du lancement des applications, procédez comme suit :*

1. Lancez la tâche Contrôle du lancement des applications en mode **Statistiques uniquement** (cf. section « **Sélection du mode de fonctionnement la tâche Contrôle du lancement des applications »** à la page 153) pour consigner dans le journal d'exécution de la tâche tous les déclenchements de règles pour les lancements d'applications sur l'ordinateur protégé.

2. A la fin de l'exécution de la tâche en mode **Statistiques uniquement**, ouvrez le journal d'exécution de la tâche via le bouton **Ouvrir le journal d'exécution** dans le groupe **Administration** du volet résultats de l'entrée **Contrôle du lancement des applications**.

3. Dans la fenêtre **Journal d'exécution**, appuyez sur le bouton **Créer des règles selon les événements**.

Kaspersky Embedded Systems Security créera le fichier de configuration au format XML avec la liste des règles formées selon le fonctionnement de la tâche Contrôle du lancement des applications en mode **Statistiques uniquement**. Vous pouvez appliquer cette liste dans la tâche Contrôle du lancement des applications (cf. section « Importation des règles du Contrôle du lancement des applications depuis un fichier XML » à la page 178).

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 autorisent le lancement des applications indispensables au fonctionnement de l'ordinateur (par exemple, fichiers du système d'exploitation).

Tous les événements du travail de la tâche sont fixés dans le journal au cours de l'exécution de la tâche dans chacun de deux modes. Vous pouvez créer le fichier de configuration contenant la liste des règles selon les événements de la tâche en mode **Appliquer les règles du Contrôle du lancement des applications**. 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 avant le lancement de la tâche en mode d'application des règles du Contrôle du lancement des applications.

Importation des règles du Contrôle du lancement des applications depuis un fichier XML

► *Pour importer des règles du Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle du lancement des applications**.

3. Dans le volet résultats de l'entrée **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. Cliquez sur **Ajouter**.

5. Dans le menu contextuel du bouton, choisissez l'option **Importer des règles depuis un fichier**.

6. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez l'une des options du menu contextuel du bouton **Importer des règles depuis le fichier** :

   - **Ajouter les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles dont les paramètres sont identiques se superposent.

   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.

   - **Fusionner les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

7. Dans la fenêtre Microsoft Windows **Ouvrir**, sélectionnez le fichier XML qui contient les paramètres des règles du Contrôle du lancement des applications.

8. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du contrôle du lancement des applications**.

Présentation de la tâche Génération des règles du Contrôle du lancement des applications

La tâche Génération des règles du Contrôle du lancement des applications permet de générer automatiquement une liste de règles d'autorisation pour le Contrôle du lancement des applications sur la base des types de fichiers indiqués, issus des dossiers indiqués. Par exemple, si vous indiquez les fichiers exécutables du dossier C:\Program Files (x86) en tant que paramètres de la tâche, l'application créera automatiquement des règles autorisant le lancement de ces fichiers. L'application autorisera par la suite le lancement des applications pour lesquelles des règles d'autorisation ont été générées automatiquement.

Les règles créées s'affichent après que vous avez cliqué sur le lien **Règles du Contrôle du lancement des applications** dans l'entrée **Contrôle du lancement des applications**.

Configuration des paramètres de la tâche Génération des règles du Contrôle du lancement des applications

La tâche Génération des règles du Contrôle du lancement des applications possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 21. Paramètres par défaut de la tâche Génération des règles du Contrôle du lancement des applications

Paramètre	Valeur par défaut	Description
Préfixe des noms des règles d'autorisation	Correspond au nom de l'ordinateur 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 indiquant l'emplacement des dossiers et les types de fichiers dont le lancement est autorisé par les règles générées automatiquement. Vous pouvez également ne pas tenir compte des applications déjà en cours d'exécution lors de la création des règles d'autorisation.

Paramètre	Valeur par défaut	Description
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 de la tâche Contrôle du lancement des applications ; les nouvelles règles sont fusionnées avec les règles existantes. Les doublons sont supprimés.	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.
Paramètres du lancement de la tâche en tant que	La tâche est lancée sous les autorisations du compte système.	Vous pouvez autoriser le lancement de la tâche de génération automatique des règles d'autorisation 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.

► *Pour configurer les paramètres de la tâche Génération des règles pour le Contrôle du lancement des applications, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Génération automatique de règles**.

2. Sélectionnez la sous-entrée **Génération des règles du Contrôle du lancement des applications**.

3. Dans le volet résultats de l'entrée **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre. Configurez les paramètres suivants :

   - Sous l'onglet **Général** :

     - Indiquez le préfixe des noms des règles.

       Première partie du nom de la règle. La deuxième partie du nom de la règle est constituée à partir du nom de l'objet dont le lancement est interdit.

       Par défaut, le nom de l'ordinateur sur lequel est installé Kaspersky Embedded Systems Security est utilisé comme préfixe. Vous pouvez modifier le préfixe des noms des règles d'autorisation.

     - Configurez la zone d'application des règles d'autorisation (cf. section « Restriction de la zone d'application de la tâche » à la page 183).

   - Sous l'onglet **Actions**, définissez les actions que Kaspersky Embedded Systems Security doit réaliser :

     - Lors de la génération de règles (cf. section « Actions lors de la génération automatique de règles du Contrôle du lancement des applications » à la page 185).
     - Une fois la tâche terminée (cf. section « Actions à réaliser à la fin de la génération automatique des règles du Contrôle du lancement des applications » à la page 188).

- Sous les onglets **Planification** et **Avancé** :
  - Paramètres de lancement de la tâche selon la planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).
- Sous l'onglet **Exécuter en tant que** :
  - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81).

4. Cliquez sur **OK**.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution de la tâche.

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. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Génération automatique de règles**.
2. Sélectionnez la sous-entrée **Génération des règles du Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.

4. Configurez les paramètres de la tâche suivants :

   - **Créer des règles d'autorisation sur la base des applications en cours d'exécution**.

     La case active ou désactive la génération automatique des règles d'autorisation pour le contrôle du lancement des applications pour les applications déjà exécutées. Cette option est recommandée si une sélection représentative d'applications est en cours d'exécution sur l'ordinateur et que vous souhaitez utiliser celle-ci pour générer les règles d'autorisation.

     Si la case est cochée, les règles d'autorisation pour le contrôle du lancement des applications sont créées conformément aux applications exécutées.

     Si la case est décochée, les applications en cours d'exécution ne sont pas prises en compte pour la génération des règles d'autorisation.

     Cette case est cochée par défaut.

     La case ne peut être décochée si aucun dossier n'est sélectionné dans le tableau **Créer des règles d'autorisation pour les applications des dossiers**.

   - **Créer des règles d'autorisation pour les applications des dossiers**.

     Le tableau permet de sélectionner ou d'indiquer la zone d'analyse de la tâche et les types de fichiers exécutables qui seront pris en compte lors de la génération des règles du Contrôle du lancement des applications. La tâche génèrera des règles d'autorisation pour les fichiers des types sélectionnés et situés dans les dossiers indiqués.

5. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Actions lors de la génération automatique des règles du Contrôle du lancement des applications

► *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. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Génération automatique de règles**.
2. Sélectionnez la sous-entrée **Génération des règles du Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Ouvrez l'onglet **Actions**.
5. Configurez les paramètres suivants dans le groupe **Lors de la génération des règles d'autorisation** :

   - **Utiliser un certificat numérique**.

     Si cette option est sélectionnée, la présence d'un certificat numérique est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications à l'aide de fichiers disposant d'un certificat numérique. Cette option est conseillée si vous souhaitez autoriser le lancement de n'importe quelle application considérée comme étant de confiance dans le système d'exploitation.

     Cette option est sélectionnée par défaut.

- **Utiliser l'en-tête et l'empreinte du certificat numérique**.

  La case active ou désactive l'utilisation de l'en-tête et de l'empreinte du certificat numérique du fichier en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'activation de cette case permet de définir des conditions plus strictes d'analyse du certificat numérique.

  Si la case est cochée, les valeurs de l'en-tête et de l'empreinte du certificat numérique des fichiers pour lesquels sont créées les règles sont indiquées en tant que critère de déclenchement des règles d'autorisation du contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées à l'aide des fichiers disposant de l'en-tête et de l'empreinte de certificat numérique indiqués dans la règle.

  L'utilisation de cette case limite de manière plus stricte le déclenchement des règles d'autorisation du lancement des applications en fonction du certificat numérique car l'empreinte est l'identifiant unique du certificat numérique et elle ne peut être forgée.

  Si la case est désélectionnée, le critère de déclenchement des règles d'autorisation du contrôle du lancement des applications sera la valeur de n'importe quel certificat numérique considéré comme de confiance par le système d'exploitation.

  La case est accessible si vous avez choisi l'option **Utiliser un certificat numérique**.

  Cette case est cochée par défaut.

- **En cas d'absence de certificat, utiliser**.

  Liste déroulante permettant de sélectionner le critère de déclenchement des règles d'autorisation pour le contrôle du lancement des applications dans le cas où le fichier sur la base duquel est créée la règle ne dispose pas d'un certificat numérique.

- **Hash SHA256**. La valeur de la somme de contrôle du fichier sur la base duquel est créée 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 sur la base duquel est créée 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 par les fichiers qui se trouvent dans les dossiers indiqués sous l'onglet **Créer des règles d'autorisation pour les applications des dossiers** dans le tableau Créer des règles d'autorisation pour les applications des dossiers.

- **Utiliser le hash SHA256**.

  Si cette option est sélectionnée, la valeur de la somme de contrôle du fichier sur la base duquel est créée la règle est indiquée en tant que critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le contrôle du lancement des applications. L'application autorisera désormais le lancement des applications exécutées par les fichiers présentant la valeur de la somme de contrôle indiquée.

  Il est conseillé d'appliquer cette option pour créer les règles les plus fiables : la somme de contrôle calculée selon l'algorithme SHA256 est le seul identifiant de ce fichier. L'utilisation de la valeur du hash obtenue en guise de critère de déclenchement de la règle réduit la zone d'application des règles à un fichier.

- **Créer des règles pour un utilisateur et/ou un groupe d'utilisateurs**.

  Champ affichant l'utilisateur et/ou le groupe d'utilisateurs. L'application contrôlera les lancements des applications par l'utilisateur et/ou le groupe d'utilisateur défini.

  Par défaut, le groupe **Tous** est sélectionné.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Actions réalisées à la fin de la génération automatique des règles du Contrôle du lancement des applications

► *Pour configurer les actions que Kaspersky Embedded Systems Security doit réaliser à la fin de la génération automatique des règles, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Génération automatique de règles**.
2. Sélectionnez la sous-entrée **Génération des règles du Contrôle du lancement des applications**.
3. Dans le volet résultats de l'entrée **Génération des règles du Contrôle du lancement des applications**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Ouvrez l'onglet **Actions**.
5. Configurez les paramètres suivants dans le groupe **Une fois la tâche terminée** :

   - **Ajouter les règles d'autorisation à la liste des règles du Contrôle du lancement des applications**.

     La case active ou désactive l'ajout des règles d'autorisation créés à la liste des règles du Contrôle du lancement des applications. La liste des règles du Contrôle du lancement des applications est affichée via le lien **Règles du contrôle du lancement des applications** du volet résultats de l'entrée **Contrôle du lancement des applications**.

     Si la case est cochée, Kaspersky Embedded Systems Security ajoute les règles créées au cours de l'exécution de la tâche Génération des règles du Contrôle du lancement des applications à la liste de règles du Contrôle du lancement des applications conformément au principe d'ajout défini.

     Si la case est décochée, Kaspersky Embedded Systems Security n'ajoute pas les règles d'autorisation créées à la liste de règles du Contrôle du lancement des applications. Les règles créées sont exportées uniquement dans un fichier.

     Cette case est cochée par défaut.

     La case ne peut être décochée si la case **Exporter les règles d'autorisation vers un fichier** n'est pas cochée.

- **Principe d'ajout**.

  Liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles du Contrôle du lancement des applications.

  - **Ajouter aux règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques se superposent.
  - **Remplacer les règles existantes**. Les règles sont ajoutées à la place des règles existantes.
  - **Fusionner avec les règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

  Le mode **Fusionner avec les règles existantes** est défini par défaut.

- **Exporter les règles d'autorisation vers un fichier**.

  La case active ou désactive l'exportation des règles d'autorisation créées pour le contrôle du lancement des applications vers un fichier.

  Si la case est cochée, Kaspersky Embedded Systems Security exporte les règles créées dans le fichier indiqué dans le champ ci-dessous, une fois la tâche de génération automatique de règles d'autorisation terminée.

  Si la case est décochée, Kaspersky Embedded Systems Security n'exporte pas dans un fichier les règles créées à la fin de la tâche de génération automatique des règles d'autorisation. Il se contente de les ajouter à la liste des règles du Contrôle du lancement des applications.

  Cette case est décochée par défaut.

  La case ne peut être décochée si la case **Ajouter les règles d'autorisation à la liste des règles du Contrôle du lancement des applications** n'est pas cochée.

- **Ajouter des informations sur l'ordinateur dans le nom du fichier**.

  La case active ou désactive l'ajout des informations relatives à l'ordinateur à protéger dans le nom du fichier dans lequel sont exportées les règles du Contrôle du lancement des applications créées.

  Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur à protéger, la date et l'heure de création du fichier.

  Quand la case est décochée, l'application n'ajoute pas les informations relatives au serveur à protéger dans le nom du fichier d'exportation.

  La case est accessible si la case **Exporter les règles d'autorisation vers un fichier** est cochée.

  Cette case est cochée par défaut.

6. Cliquez sur **OK**.

Les paramètres définis seront enregistrés.

Contrôle des périphériques

Cette section contient les informations sur la tâche Contrôle des périphériques et les instructions de configuration de ses paramètres.

Dans cette section

Présentation de la tâche Contrôle des périphériques

Kaspersky Embedded Systems Security contrôle l'enregistrement et l'utilisation des *dispositifs de stockage de masse* et des lecteurs CD/DVD-ROM afin de protéger l'ordinateur contre les menaces sur la sécurité qui peuvent survenir pendant l'échange de fichiers avec le disque flash ou les périphériques externes d'un autre type connectés par USB. Un dispositif de stockage de masse est un périphérique externe destiné à l'enregistrement et la conservation des données.

Kaspersky Embedded Systems Security la contrôle la connexion des types de périphériques externe suivants :

- Disques flash USB ;
- Lecteurs CD/DVD-ROM ;
- Lecteurs de disquettes USB ;
- Périphériques mobiles MTP.USB.

La tâche Contrôle des périphériques surveille les tentatives de connexions de périphériques externes à l'ordinateur protégé et interdit leur utilisation en tant que dispositif de stockage de masse s'il n'existe pas de règles d'autorisation pour ces périphériques. 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 de deux états :

- *De confiance. P*ériphérique avec lequel l'échange de données est autorisé. Le chemin d'accès à ce périphérique tombe sous le coup au moins d'une règle d'autorisation.
- *Douteux.* Périphérique avec lequel l'échange de données est interdit. Le chemin d'accès à l'instance d'un tel 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 Génération des 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 le périphérique externe enregistré 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. Les informations relatives au chemin d'accès à l'instance du périphérique se trouvent dans les propriétés du périphérique externe dans le système Windows et sont définies automatiquement par Kaspersky Embedded Systems Security au moment de la création des règles d'autorisation.

La tâche Contrôle des périphériques peut être exécutée selon un des deux modes suivants :

- **Appliquer le blocage par défaut**. 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 *blocage par défaut* (Default Denys) 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 a été connecté à l'ordinateur protégé au moment du lancement de la tâche Contrôle des périphériques en mode **Appliquer le blocage par défaut**, ce dispositif ne sera pas bloqué par l'application. Il est recommandé de déconnecter indépendamment le périphérique douteux ou de redémarrer l'ordinateur, sans quoi le principe du blocage par défaut ne sera pas appliqué à un tel périphérique.

- **Statistiques uniquement**. Kaspersky Embedded Systems Security ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement dans le journal d'exécution de la tâche les informations relatives aux connexions ou aux enregistrements de périphériques externes sur l'ordinateur protégé ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques auxquelles les périphériques connectés satisfont. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

  Vous pouvez utiliser ce mode pour composer la liste des règles du contrôle des périphériques sur la base des informations fixées dans le journal d'exécution de la tâche (cf. section « Composition de la liste des règles sur la base des événements de la tâche Contrôle des périphériques » à la page 206).

Configuration des paramètres 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.

Tableau 22. Paramètres par défaut de la tâche Contrôle des périphériques

Paramètre	Valeur par défaut	Description
Mode de fonctionnement de la tâche	**Statistiques uniquement**	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 **Appliquer le blocage par défaut** pour la protection d'un ordinateur afin d'appliquer l'interdiction de fait des périphériques externes.
Autoriser l'utilisation de tous les périphériques externes si 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	Au lancement de l'application	La tâche Contrôle des périphériques est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez configurer le lancement de la tâche selon la planification.

► *Pour configurer les paramètres de la tâche Contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle des périphériques**.

3. Dans le volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

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

4. Sous l'onglet **Général**, configurez les paramètres de la tâche suivants :

   - Dans le groupe **Mode de fonctionnement**, indiquez le mode de fonctionnement de la tâche :

     - **Appliquer le blocage par défaut**.

       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 *blocage par défaut* (Default Denys) 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 a été connecté à l'ordinateur protégé au moment du lancement de la tâche Contrôle des périphériques en mode **Appliquer le blocage par défaut**, ce dispositif ne sera pas bloqué par l'application. Il est recommandé de déconnecter indépendamment le périphérique douteux ou de redémarrer l'ordinateur, sans quoi le principe du blocage par défaut ne sera pas appliqué à un tel périphérique.

     - **Statistiques uniquement**.

       Kaspersky Embedded Systems Security ne contrôle pas la connexion des disques flash et autres périphériques externes et consigne seulement dans le journal d'exécution de la tâche les informations relatives aux connexions ou aux enregistrements de périphériques externes sur l'ordinateur protégé

ainsi que les informations relatives aux règles d'autorisation du contrôle des périphériques auxquelles les périphériques connectés satisfont. L'utilisation de tous les périphériques externes est autorisée. Il s'agit du mode par défaut.

- Décochez ou cochez la case **Autoriser l'utilisation de tous les périphériques externes si la tâche Contrôle des périphériques n'est pas exécutée**.

  La case autorise ou interdit l'utilisation des dispositifs de stockage de masse 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 dispositif de stockage de masse sur l'ordinateur protégé.

  Si la case est décochée, Kaspersky Embedded Systems Security interdit l'utilisation des dispositifs de stockage de masse douteux sur l'ordinateur protégé si la tâche Contrôle des périphériques n'est pas exécutée ou si le service Kaspersky Security a été arrêté. Il est conseillé d'utiliser cette version 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.

5. Les onglets **Planification** et **Avancé** permettent de configurer, le cas échéant, les paramètres de lancement planifié de la tâche (cf. section « Configuration des paramètres de planification du lancement des tâches » à la page 76).

6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

7. Dans la partie inférieure du volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

8. Le cas échéant, modifiez la liste des règles de contrôle des périphériques.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution de la tâche.

Présentation des règles de contrôle des périphériques

Les tâches sont créées individuellement pour chaque périphérique connecté au moment donné ou connecté auparavant à l'ordinateur protégé, si les données relatives à ce périphérique ont été mémorisées dans le système.

Pour créer des règles d'autorisation du contrôle des périphériques, vous pouvez :

- utiliser la tâche de génération des règles d'autorisation (cf. section « Présentation de la tâche Génération des règles pour le Contrôle des périphériques » à la page 209) ;
- utiliser le mode **Statistiques uniquement** dans la tâche Contrôle des périphériques (cf. section « Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques » à la page 206) ;
- utiliser les données système relatives aux périphériques connectés (cf. section « Ajout d'une règle d'autorisation pour un ou plusieurs périphériques externes » à la page 205) ;
- élargir le domaine d'application des règles existantes (cf. section « Extension de la zone d'application des règles de contrôle des périphériques » à la page 201).

> Le nombre maximum de règles de contrôle des périphériques pris en charge par Kaspersky Embedded Systems Security est égal à 3 072.

Les règles de contrôle des périphériques contiennent les paramètres suivants :

- Type de règle ;
- Zone d'application des règles ;
- Données du périphérique d'origine ;
- Commentaires.

Type de règle

Les règles sont toujours des règles *Autorisé*. La tâche du contrôle des périphériques bloque par défaut la connexion 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 de contrôle des périphériques identifient les disques flash et autres périphériques externes connectés en fonction de la valeur du *chemin vers l'instance du périphérique (Device Instance Path).* 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 dispositif de stockage de masse ou de lecteur de CD/DVD (par exemple, IDE ou SCSI).

Kaspersky Embedded Systems Security contrôle la connexion des périphériques externes de lecture 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 dispositif de stockage de masse (Mass Storage) 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 du périphérique (VID) ;
- Type de contrôleur du périphérique (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 d'autorisation qui vient d'être créée contient un périphérique et Kaspersky Embedded Systems Security utilise les propriétés de celui-ci pour créer la règle d'autorisation. Vous pouvez modifier les valeurs indiquées à l'aide d'un masque dans les propriétés de la règle créée afin d'élargir la zone d'application des règles (cf. section « Extension de la zone d'application des règles de contrôle des périphériques » à la page 201).

Données du périphérique d'origine

Les données du périphérique sur la base desquelles Kaspersky Embedded Systems Security a créé la règle d'autorisation s'affichent dans les propriétés de chaque règle.

Les données du périphérique contiennent les informations suivantes :

- **Chemin d'accès à l'instance du périphérique**. Kaspersky Embedded Systems Security utilise cette valeur pour définir les critères de déclenchement de la règle et remplir les champs **Fabricant (VID)**, **Type de contrôleur (PID)**, **Numéro de série** dans le groupe **Zone d'application de la règle** de la fenêtre **Paramètres 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.

Commentaires

Vous pouvez ajouter des informations complémentaires pour chaque règle d'autorisation créée du contrôle des périphériques dans le champ **Commentaires**, par exemple, le nom du disque flash connecté ou le nom de son propriétaire. Le commentaire 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.

Suppression des règles de contrôle des périphériques

► *Pour supprimer des règles de contrôle de contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle des périphériques**.
3. Dans la partie inférieure du volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.
4. Dans la liste, sélectionnez la ou les règles que vous souhaitez supprimer.
5. Cliquez sur le bouton **Supprimer la sélection**.
6. Cliquez sur le bouton **Enregistrer**.

Les règles de contrôle des périphériques sélectionnées seront supprimées.

Exportation des règles de contrôle des périphériques

► *Pour exporter des règles de contrôle des périphériques dans un fichier de configuration, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle des périphériques**.
3. Dans la partie inférieure du volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

4. Cliquez sur le lien **Exporter vers un fichier**.

   La fenêtre standard de Microsoft Windows s'ouvre.

5. 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.

6. 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 créée du contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle des périphériques**.

3. Dans la partie inférieure du volet résultats de l'entrée Contrôle des périphériques, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

4. Dans la liste des règles définies, ouvrez la fenêtre **Paramètres des règles** d'un double clic sur la règle dont vous souhaitez configurer les paramètres.

5. Dans la fenêtre qui s'ouvre, décochez ou cochez la case **Appliquer la règle**.

   La case active ou désactive l'application d'une règle concrète de contrôle des périphériques.

   Si la case est cochée dans les paramètres de la règle, la règle sera appliquée. La connexion des périphériques externes couverts par la zone d'application de cette règle sera autorisée.

   Si la case est décochée dans les paramètres de la règle, cette règle ne sera pas appliquée. La connexion des périphériques externes couverts par la zone d'application de cette règle sera interdite.

   La case est cochée par défaut dans les paramètres de chaque règle créée.

6. Cliquez sur **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'exemplaire 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 dispositifs de stockage de masse.

► *Pour appliquer le masque du chemin d'accès à l'instance du périphérique dans les propriétés de la règle d'autorisation du contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
2. Sélectionnez la sous-entrée **Contrôle des périphériques**.
3. Dans la partie inférieure du volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.
4. Dans la fenêtre **Règles du Contrôle des périphériques** qui s'ouvre, choisissez la règle, sur la base des propriétés de laquelle vous voulez appliquer le masque du chemin d'accès à l'instance du périphérique.
5. Ouvrez la fenêtre **Paramètres des règles** d'un double clic de la souris sur la règle de contrôle des périphériques choisie.
6. Dans la fenêtre qui s'ouvre, exécutez une des actions suivantes :

   - Cochez la case **Utiliser un masque** en regard du champ **Type de contrôleur (PID)** si voulez que la règle modifiée autorise la connexion de tous les périphériques selon les données indiquées relatives au fabricant et au type du périphérique.
   - Cochez la case **Utiliser un masque** en regard du champ **Numéro de série** si voulez que la règle modifiée autorise la connexion de tous les périphériques selon les données indiquées relatives au fabricant et au numéro de série du périphérique.
   - Cochez les cases **Utiliser un masque** en regard des champ **Type de contrôleur (PID)** et **Numéro de série** si voulez que la règle modifiée autorise la connexion de tous les périphériques selon les données indiquées relatives au fabricant du périphérique.

   Si la case **Utiliser un masque** est cochée dans un champ au moins, les données des champs où la case n'est pas cochée sont remplacées par * et ne sont pas prises en compte lors du déclenchement de la règle.
7. Le cas échéant, ajoutez des informations dans le champ **Commentaires** pour expliquer la règle. Par exemple, précisez les périphériques auxquels la règle doit s'appliquer.
8. Cliquez sur **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.

Présentation de la formation de la liste des règles de 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 Génération des règles pour le Contrôle des périphériques.

Par défaut Kaspersky Embedded Systems Security interdit la connexion de n'importe quel disque flash et autre périphérique externe qui n'est pas soumis à l'action des règles d'autorisation de contrôle des périphériques indiquées.

Tableau 23. Objectifs et scénarios de création de listes de règles de contrôle des périphériques

Scénarios de création de la liste des règles	Tâche à exécuter
Tâche Génération des 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. • Il faut créer une liste des règles pour les périphériques de confiance dans le réseau d'ordinateurs protégés.
Créer des règles sur la base des données du système	Il faut ajouter des règles d'autorisation pour un ou plusieurs nouveaux périphériques connectés.
Mode **Statistiques uniquement** de la tâche Contrôle des périphériques	Il faut ajouter des règles d'autorisation pour un nombre important de nouveaux périphériques de confiance ou pour des périphériques mobiles MTP de confiance.

Utilisation de la tâche Génération des règles pour le Contrôle des périphériques

Le fichier XML formé à la fin de la tâche Génération des 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.

Au cours de l'exécution de la tâche, Kaspersky Embedded Systems Security analyse les données du système relatives à tous les périphériques externes connectés auparavant et actuellement et crée sur la base de celles-ci la liste des règles d'autorisation pour les périphériques détectés. A

l'issue de la tâche, l'application crée un fichier XML dans le dossier accessible via le chemin d'accès indiqué dans les paramètres de la tâche. Vous pouvez configurer l'importation automatique des règles générées dans la liste de règles de la tâche Contrôle des périphériques.

Il est conseillé d'utiliser ce scénario pour composer 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 utilisés sur l'ordinateur 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 auparavant ou actuellement à l'ordinateur protégé et affiche les périphériques trouvés dans la liste de la fenêtre **Créer les règles sur la base des données 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 dont les données ont été trouvées et ajouter directement les nouvelles règles à la liste des règles de contrôle des périphériques définies.

Il est conseillé d'utiliser ce scénario pour mettre à jour la liste des règles s'il faut autoriser l'utilisation d'un nombre limité de nouveaux dispositifs de stockage de masse.

> Kaspersky Embedded Systems Security n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles MTP de confiance à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

Utilisation du rapport de la tâche Contrôle des périphériques en mode Statistiques uniquement

Le fichier XML obtenu à la fin de la tâche Contrôle des périphériques en mode **Statistiques uniquement** 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 dans le journal d'exécution de la tâche toutes les connexions des disques flash et autres dispositifs de stockage de masse à l'ordinateur 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 uniquement**, il est conseillé de configurer la période d'exécution de la tâche de telle sorte que toutes les connexions possibles de périphériques externes à l'ordinateur protégé puissent être réalisées.

Il est conseillé d'utiliser ce scénario pour actualiser la liste existante des règles s'il faut autoriser l'utilisation d'un grand nombre de nouveaux périphériques externes et créer des règles d'autorisation pour des périphériques mobiles MTP.

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 ordinateurs du réseau protégé.

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 d'enrichissement de la liste des règles, l'application se fonde sur les données de Windows relatives à toutes les connexions de périphériques externes enregistrées dans le système et tient également compte des périphériques externes connectés en ce moment.

> Kaspersky Embedded Systems Security n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles MTP de confiance à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

► *Pour ajouter une règle d'autorisation pour un ou plusieurs périphériques externes utilisés en ce moment, procédez comme suit :*

1. Connectez le nouveau périphérique externe pour lequel vous souhaitez ajouter une règle d'autorisation pour l'ordinateur protégé.
2. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.
3. Sélectionnez la sous-entrée **Contrôle des périphériques**.

4. Dans le volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

5. Cliquez sur **Ajouter**.

6. Dans le menu contextuel du bouton, choisissez l'option **Créer les règles sur la base des données du système**.

7. Dans la fenêtre qui s'ouvre, sélectionnez dans la liste des périphériques détectés le ou les périphériques dont vous souhaitez autoriser l'utilisation sur l'ordinateur protégé.

8. 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.

Composition de la liste des règles selon les événements de la tâche Contrôle des périphériques

► *Pour créer le fichier de configuration contenant la liste des règles de contrôle des périphériques créées sur la base des événements de l'exécution de la tâche Contrôle des périphériques, procédez comme suit :*

1. Lancez la tâche Contrôle des périphériques en mode **Statistiques uniquement** (cf. section « **Configuration des paramètres de la tâche Contrôle des périphériques** » à la page 193) pour consigner dans le journal d'exécution de la tâche tous les événements créés suite à une connexion de disques flash ou d'autres périphériques externes à l'ordinateur protégé.

2. A la fin de l'exécution de la tâche en mode **Statistiques uniquement**, ouvrez le journal d'exécution de la tâche via le bouton **Ouvrir le journal d'exécution** dans le groupe **Administration** du volet résultats de l'entrée **Contrôle des périphériques**.

3. Dans la fenêtre **Journal d'exécution**, appuyez sur le bouton **Créer des règles selon les événements**.

Kaspersky Embedded Systems Security créera le fichier de configuration au format XML avec la liste des règles composées selon le fonctionnement de la tâche Contrôle des périphériques en mode **Statistiques uniquement**. Vous pouvez appliquer cette liste dans la tâche Contrôle des périphériques (cf. section « Importation des règles de contrôle des périphériques depuis un fichier XML » à la page 207).

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 du travail de la tâche sont fixés dans le journal au cours de l'exécution de la tâche dans chacun de deux modes. Vous pouvez créer le fichier de configuration contenant la liste des règles sur la base des événements de la tâche en mode **Appliquer le blocage par défaut**. 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 avant le lancement de la tâche en mode de contrôle actif des périphériques externes.

Importation des règles de contrôle des périphériques depuis un fichier XML

► *Pour importer des règles de contrôle de contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle de l'ordinateur**.

2. Sélectionnez la sous-entrée **Contrôle des périphériques**.

3. Dans le volet résultats de l'entrée **Contrôle des périphériques**, cliquez sur le lien **Règles du Contrôle des périphériques**.

   La fenêtre **Règles du Contrôle des périphériques** s'ouvre.

4. Cliquez sur **Ajouter**.

5. Dans le menu contextuel du bouton, choisissez l'option **Importer les règles depuis un fichier au format XML**.

6. Indiquez le mode d'ajout des règles à importer. Pour ce faire, sélectionnez l'une des options du menu contextuel du bouton **Importer les règles depuis un fichier au format XML** :

   - **Ajouter les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles dont les paramètres sont identiques se superposent.

   - **Remplacer les règles existantes**, si vous souhaitez que les règles à importer soient ajoutées à la place des règles déjà existantes.

   - **Fusionner les règles aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles déjà existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

   La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

7. Dans la fenêtre Microsoft Windows **Ouvrir**, sélectionnez le fichier XML qui contient les paramètres des règles de contrôle des périphériques.

8. Cliquez sur le bouton **Ouvrir**.

Les règles importées seront affichées dans la fenêtre **Règles du Contrôle des périphériques**.

Présentation de la tâche Génération des règles pour le Contrôle des périphériques

La tâche Génération des règles pour le Contrôle des périphériques permet de composer automatiquement la liste des règles d'autorisation de la connexion des disques flash et des autres dispositifs de stockage de masse sur la base des données du système relatives aux périphériques qui avaient été connectés auparavant à l'ordinateur protégé.

> Kaspersky Embedded Systems Security n'a pas accès aux données du système relatives aux périphériques mobiles connectés selon le protocole MTP. Vous ne pouvez pas créer de règles d'autorisation pour les périphériques mobiles MTP de confiance à l'aide des scénarios d'enrichissement de la liste des règles de contrôle des périphériques qui reposent sur l'application des données systèmes relatives à tous les périphériques.

À la fin de l'exécution de la tâche, Kaspersky Embedded Systems Security crée un fichier de configuration au format XML avec la liste des règles d'autorisation pour les dispositifs de stockage de masse détectés ou ajoute directement les règles formées à la tâche Contrôle des périphériques en fonction de la configuration de la tâche. L'application autorisera par la suite la connexion des périphériques pour lesquels des règles d'autorisation ont été générées automatiquement.

Les règles formées et ajoutées à la tâche s'affichent via le lien **Règles du Contrôle des périphériques** dans l'entrée **Contrôle des périphériques**.

Configuration des paramètres de la tâche Génération des règles pour le Contrôle des périphériques

La tâche Génération des règles pour le Contrôle des périphériques possède par défaut les paramètres décrits dans le tableau ci-dessous. Vous pouvez modifier les valeurs de ces paramètres.

Tableau 24. Paramètres par défaut de la tâche Génération des règles pour le Contrôle des périphériques

Paramètre	Valeur par défaut	Description
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 Génération des 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.

► *Pour configurer les paramètres de la tâche Génération des règles pour le Contrôle des périphériques, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Génération automatique de règles**.
2. Choisissez la sous-entrée **Génération des règles pour le Contrôle des périphériques**.
3. Dans le volet résultats de l'entrée **Génération des règles pour le Contrôle des périphériques**, cliquez sur le lien **Propriétés**.

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

4. Sous l'onglet **Général**, 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**.

        La case active ou désactive l'ajout des règles d'autorisation créés à la liste des règles de contrôle des périphériques. La liste des règles de contrôle des périphériques est affichée via le lien **Règles du Contrôle des périphériques** du volet résultats de l'entrée **Contrôle des périphériques**.

        Si la case est cochée, Kaspersky Embedded Systems Security ajoute les règles formées au cours de l'exécution de la tâche Génération de règles pour le contrôle des périphériques à la liste des règles de contrôle des périphériques selon le principe d'ajout indiqué.

        Si la case est décochée, Kaspersky Embedded Systems Security n'ajoute pas les règles d'autorisation créées à la liste de règles de contrôle des périphériques. Les règles créées sont exportées uniquement dans un fichier.

        Cette case est cochée par défaut.

        La case ne peut être décochée si la case **Exporter les règles d'autorisation vers un fichier** n'est pas cochée.

    - **Principe d'ajout**.

        Liste déroulante permettant de définir le mode d'ajout des règles d'autorisation créées à la liste des règles de contrôle des périphériques.

        - **Ajouter aux règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques se superposent.
        - **Remplacer les règles existantes**. Les règles sont ajoutées à la place des règles existantes.
        - **Fusionner avec les règles existantes**. Les règles viennent compléter la liste des règles existantes. Les règles possédant des paramètres redoublés ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres à une valeur différente.

        Le mode **Fusionner avec les règles existantes** est défini par défaut.

- **Exporter les règles d'autorisation vers un fichier**.

  La case active ou désactive l'exportation des règles d'autorisation créées pour le contrôle des périphériques vers un fichier.

  Si la case est cochée, Kaspersky Embedded Systems Security exporte les règles créées dans le fichier indiqué dans le champ ci-dessous, une fois la tâche de génération automatique de règles d'autorisation terminée.

  Si la case est décochée, Kaspersky Embedded Systems Security n'exporte pas dans un fichier les règles créées à la fin de la tâche de génération automatique des règles d'autorisation. Il se contente de les ajouter à la liste des règles de contrôle des périphériques.

  Cette case est décochée par défaut.

  La case ne peut être décochée si la case **Ajouter des règles d'autorisation à la liste des règles du Contrôle des périphériques** n'est pas cochée.

- **Ajouter des informations sur l'ordinateur dans le nom du fichier**.

  La case active ou désactive l'ajout des informations relatives à l'ordinateur à protéger dans le nom du fichier dans lequel sont exportées les règles de contrôle des périphériques créées.

  Si la case est cochée, l'application ajoute au nom du fichier d'exportation le nom du serveur à protéger, la date et l'heure de création du fichier.

  Quand la case est décochée, l'application n'ajoute pas les informations relatives au serveur à protéger dans le nom du fichier d'exportation.

  La case est accessible si la case **Exporter les règles d'autorisation vers un fichier** est cochée.

  Cette case est cochée par défaut.

5. Les onglets **Planification** et **Avancé** permettent de configurer les paramètres de lancement planifié de la tâche (cf. section « Configuration des paramètres de planification du lancement des tâches » à la page 76).
6. Cliquez sur **OK**.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution de la tâche.

Administration du pare-feu

Cette section contient des informations sur la tâche Administration du pare-feu et les instructions sur la configuration de cette tâche.

Dans cette section

Présentation de la tâche Administration du pare-feu

Kaspersky Embedded Systems Security offre une solution fiable et ergonomique pour la protection des connexions réseau grâce à la tâche Administration du pare-feu.

La tâche Administration du pare-feu ne réalise pas le filtrage en lui-même du trafic réseau, mais permet d'administrer le pare-feu Windows via l'interface graphique de Kaspersky Embedded Systems Security. Au cours de l'exécution de la tâche Administration du pare-feu, Kaspersky Embedded Systems Security assume complètement l'administration des paramètres et des règles du pare-feu du système d'exploitation et interdit tout tentative de configuration des paramètres du pare-feu par d'autres méthodes.

Au cours de l'installation de l'application, le composant Administration 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 Administration 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 Administration 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 Administration 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 Administration 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 à l'issue du sondage Kaspersky Embedded Systems Security détecte un écart entre les paramètres du pare-feu Windows et ceux de la tâche Administration du pare-feu, l'application impose les paramètres de la tâche au pare-feu du système d'exploitation.

Lors de l'interrogation du pare-feu Windows qui a lieu toutes les minutes, Kaspersky Embedded Systems Security contrôle les éléments suivants :

- l'état de fonctionnement du pare-feu Windows ;
- l'état de règles ajoutées après l'installation de Kaspersky Embedded Systems Security par d'autres applications ou outils (par exemple, ajout d'une nouvelle règle de l'application pour un port/une app à l'aide de wf.msc).

Suite à la communication des règles au pare-feu Windows, Kaspersky Embedded Systems Security crée le groupe de règles Kaspersky Security Group dans le composant logiciel enfichable **Pare-feu Windows**. Ce groupe reprend toutes les règles créées dans Kaspersky Embedded Systems Security à l'aide de la tâche Administration du pare-feu. Les règles qui figurent dans le groupe Kaspersky Security Group ne sont pas contrôlées par l'application lors du sondage toutes les minutes et elles ne sont pas synchronisées automatiquement avec la liste des règles définies dans les paramètres de la tâche Administration 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,*

relancez la tâche Administration 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 Administration du pare-feu est impossible si le pare-feu Windows est administré par une stratégie de groupe Kaspersky Security Center.

Présentation des règles du pare-feu

La tâche Administration 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 d'autorisation pour le trafic entrant définies dans le pare-feu et les copie dans les paramètres de la tâche Administration 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 app, 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 ;
- si les paramètre d'une règle existante sont modifiés dans les paramètres du pare-feu, Kaspersky Embedded Systems Security annule les modifications ;
- si une règle est créée dans les paramètres de la tâche Administration du pare-feu, Kaspersky Embedded Systems Security impose cette règle au pare-feu Windows ;
- si une règle existante est supprimée dans les paramètres de la tâche Administration du pare-feu, Kaspersky Embedded Systems Security impose la suppression de cette règle dans les paramètres du pare-feu Windows ;
- si les paramètres d'une règle existante sont modifiés dans les paramètres de la tâche Administration du pare-feu, Kaspersky Embedded Systems Security impose la mise à jour de cette règle dans les paramètres du pare-feu Windows.

Kaspersky Embedded Systems Security ne fonctionne pas avec les règles d'interdiction, ni avec les règles de contrôle du trafic sortant. Au lancement de la tâche Administration du pare-feu, Kaspersky Embedded Systems Security supprime toutes les règles de genre dans les paramètres du pare-feu Windows.

Vous pouvez créer, supprimer et modifier les règles de filtrage du trafic entrant.

Vous ne pouvez pas définir une nouvelle règle pour le contrôle du trafic sortant via les paramètres de la tâche Administration du pare-feu. Toutes les règles du pare-feu définies via Kaspersky Embedded Systems Security contrôlent uniquement le trafic entrant.

Vous pouvez utiliser les règles de pare-feu des types suivants :

- règles pour les apps ;
- règles pour les ports.

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.

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 e et la zone d'application de la règle.

Les règles pour les ports ont 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'ordinateur protégé.

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 Kaspersky Embedded Systems Security, développez l'entrée **Contrôle du serveur**.
2. Choisissez la sous-entrée **Administration du pare-feu**.
3. Dans le panneau des résultats de l'entrée **Administration 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 **Apps** 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 configurés de la tâche Administration du pare-feu sont enregistrés ; les nouveaux paramètres des règles sont transmis au pare-feu Windows.

Ajout manuel de règles du pare-feu

Vous pouvez ajouter et modifier uniquement les règles pour les apps et les ports. Vous ne pouvez pas ajouter de règles pour les groupes, ni modifier les règles existantes.

► *Pour ajouter une règle de filtrage du trafic entrant ou modifier les paramètres d'une règle existante, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Contrôle du serveur**.

2. Choisissez la sous-entrée **Administration du pare-feu**.

3. Dans le panneau des résultats de l'entrée **Administration du pare-feu**, cliquez sur le lien **Règles du pare-feu**.

4. La fenêtre **Règles du pare-feu** s'ouvre.

5. En fonction du type de règle que vous souhaitez ajouter, choisissez l'onglet **Apps** ou **Ports** et exécutez 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 **Configurer la règle pour l'app** s'ouvre.

6. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :

   - Si vous travaillez avec la règle pour une app, procédez comme suit :

     a. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.

     b. Saisissez dans le champ **Chemin d'accès à l'app** le chemin d'accès au fichier exécutable de l'app pour laquelle vous souhaitez autoriser la connexion en modifiant la règle. Vous pouvez définir le chemin d'accès manuellement ou via le bouton **Parcourir**.

     c. 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. Saisissez le nom de la règle à modifier dans le champ **Nom de la règle**.

     b. Saisissez dans le champ **Numéro de port** le numéro du port pour lequel l'application autorisera les connexions.

     c. Choisissez le type de protocole (TCP / UDP) pour lequel l'application autorisera les connexions.

     d. 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.

7. Dans la fenêtre **Configurer la règle pour l'app** ou **Configurer une règle pour un port**, cliquez sur le bouton **OK**.

8. Dans la fenêtre **Règles du pare-feu**, cliquez sur le bouton **Enregistrer**.

Les paramètres configurés de la tâche Administration du pare-feu sont enregistrés ; les nouveaux paramètres des règles sont transmis 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 Kaspersky Embedded Systems Security, développez l'entrée **Contrôle du serveur**.

2. Choisissez la sous-entrée **Administration du pare-feu**.

3. Dans le panneau des résultats de l'entrée **Administration 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 la règle que vous souhaitez supprimer, choisissez l'onglet **Apps** 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 configurés de la tâche seront enregistrés ; les nouveaux paramètres des règles seront communiqués au pare-feu Windows.

Diagnostic du système

Cette section contient des informations sur la tâche de contrôle des opérations sur les fichiers et les possibilités d'inspection du journal système du système d'exploitation.

Dans cette section

Moniteur d'intégrité des fichiers

Cette section fournit des informations sur la tâche Moniteur d'intégrité des fichiers et explique comment en configurer les paramètres.

Dans cette section

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 monitoring définies dans les paramètres de la tâche. Vous pouvez utiliser la tâche pour mettre en évidence des modifications des fichiers afin d'identifier une violation de la sécurité sur l'ordinateur protégé. Il est également possible de configurer le suivi des modifications des fichiers pendant la durée d'interruption du monitoring.

L'*interruption du monitoring* désigne une période au cours de laquelle la zone de monitoring est exclue temporairement de la zone d'action de la tâche, par exemple suite à la suspension de l'exécution de la tâche ou en l'absence physique d'un dispositif de stockage de masse sur l'ordinateur protégé. Kaspersky Embedded Systems Security signale la détection d'opérations sur les fichiers dans la zone de monitoring dès que le dispositif de stockage de masse est à nouveau connecté.

> Une suspension de l'exécution de la tâche dans la zone de monitoring définie suite à la réinstallation du composant Moniteur d'intégrité des fichiers ne constitue pas une interruption du monitoring. 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, les conditions suivantes doivent être remplies :

- un dispositif de stockage de masse, compatible avec les systèmes de fichiers ReFS et NTFS, doit être installé sur l'ordinateur protégé ;
- le journal USN Windows, dont l'interrogation permet au composant d'obtenir les données relatives aux opérations réalisées sur les fichiers, est activé.

  > 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 monitoring

Vous pouvez définir les exclusions pour la zone de monitoring (cf. section « Configuration des règles du monitoring » à la page 229).Les exclusions sont définies pour chaque règle distincte et fonctionnent uniquement pour la zone de monitoring indiquée. Vous pouvez définir un nombre illimité d'exclusions pour chaque règle.

> Les exclusions possèdent une priorité supérieure à celle de la zone de monitoring et ne sont pas contrôlées par la tâche, même si le dossier ou le fichier indiqué appartient à la zone de monitoring. Si une zone de monitoring de niveau inférieur au dossier défini dans les exclusions est définie dans les paramètres d'une des règles, cette zone de monitoring n'est pas prise en compte lors de l'exécution de la tâche.

Pour définir les exclusions, il convient d'utiliser les mêmes masques que ceux utilisés pour déterminer la zone de monitoring (cf. section « Configuration des règles de monitoring » à la page 229).

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 monitoring 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 événements pour les 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 monitoring.

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.

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 monitoring. 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 *Evénement critique* dans le journal d'exécution de la tâche.

L'*utilisateur de confiance* désigne un utilisateur ou un groupe d'utilisateurs autorisé à exécuter des opérations sur les fichiers dans la zone de monitoring 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 *Evénement 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 dans la durée d'interruption du monitoring. Dans ce cas, l'état de l'utilisateur est défini comme inconnu.

L'*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 dans la synchronisation des données du pilote 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.

Kaspersky Embedded Systems Security tient compte par défaut de tous les marqueurs d'opérations sur les fichiers accessibles. Vous pouvez sélectionner les marqueurs d'opérations sur les fichiers manuellement dans les paramètres des règles de la tâche (cf. tableau ci-dessous).

Tableau 25. 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 du fichier ou du dossier modifié	NTFS, ReFS

ID de l'opération exécutée sur le fichier	Marqueur d'opération sur les fichiers	Systèmes de fichiers pris en charge
FILE_CREATE	fichier ou dossier créés pour la première fois	NTFS, ReFS
FILE_DELETE	fichier ou dossier supprimé	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

Configuration des paramètres de la tâche Moniteur d'intégrité des fichiers

Vous pouvez modifier les paramètres de la tâche Moniteur d'intégrité des fichiers précisés par défaut (cf. tableau ci-dessous).

Tableau 26. Paramètres par défaut de la tâche Moniteur d'intégrité des fichiers

Paramètre	Valeur	Configuration
Zone de monitoring	Non définie	Vous pouvez 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 monitoring définie.
Liste des utilisateurs de confiance	Non définie	Vous pouvez désigner des utilisateurs ou des groupes d'utilisateurs dont les actions dans les dossiers indiqués sont considérées comme sans danger par le composant.
Contrôler les opérations sur les fichiers pendant la pause de la tâche	Appliquée	Vous pouvez activer ou désactiver la comptabilisation des opérations réalisées sur les fichiers dans les zones de monitoring indiquées pendant la durée d'interruption de la tâche.
Tenir compte des zones de monitoring exclues	Pas appliqué	Vous pouvez 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 monitoring définies en tant qu'exclusion.

Paramètre	Valeur	Configuration
Tenir compte des marqueurs d'opérations sur les fichiers	Tous les marqueurs d'opérations sur les fichiers disponibles sont pris en compte.	Vous pouvez définir un ensemble de marqueurs pour caractériser les opérations sur les fichiers. Si l'opération sur un fichier exécutée dans une zone de monitoring se caractérise par au moins un des marqueurs indiqués, Kaspersky Embedded Systems Security génère un événement de monitoring.
Calcul de la somme de contrôle	Pas appliqué	Vous pouvez configurer le calcul de la somme de contrôle d'un fichier après que des modifications ont été introduites dans celui-ci.
Planification du lancement de la tâche	Le prochain lancement n'est pas défini	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.

► *Pour configurer les paramètres de la tâche Moniteur d'intégrité des fichiers, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Diagnostic du système**.
2. Choisissez la sous-entrée **Moniteur d'intégrité des fichiers**.
3. Dans le volet résultats de l'entrée **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Propriétés**.

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

4. Dans la fenêtre qui s'ouvre, accédez à l'onglet **Général**, puis cochez ou décochez la case **Contrôler les opérations sur les fichiers pendant la pause de la tâche**.

   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 monitoring en cas d'interruption de la tâche Moniteur d'intégrité des fichiers.

   Si la case est décochée, les opérations sur les fichiers réalisées dans les zones de monitoring pendant l'interruption de la tâche ne sont pas enregistrées par l'application.

   Cette case est cochée par défaut.

5. Les onglets **Planification** et **Avancé** permettent de configurer le lancement planifié de la tâche (cf. section « Configuration des paramètres de planification du lancement des tâches » à la page 76).

6. Cliquez sur **OK**.

   Les paramètres définis seront enregistrés.

Configuration des règles de monitoring

Par défaut, la zone de monitoring n'est pas définie ; la tâche ne contrôle l'exécution des opérations sur les fichiers dans aucun répertoire.

► *Pour ajouter une zone de monitoring, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Diagnostic du système**.

2. Choisissez la sous-entrée **Moniteur d'intégrité des fichiers**.

3. Dans le volet résultats de l'entrée **Moniteur d'intégrité des fichiers**, cliquez sur le lien **Règles de monitoring**.

   La fenêtre **Règles de monitoring** 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 partie gauche de la fenêtre, cliquez sur le bouton **Parcourir**.

     La fenêtre standard de Microsoft Windows **Parcourir le dossier** s'ouvre.

     b. Dans la fenêtre qui s'ouvre, choisissez le dossier dans lequel vous souhaitez contrôler les opérations réalisées, 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 monitoring indiquée.

   - Si vous voulez définir la zone de monitoring 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 répertoire <\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 monitoring indiquée.

   Dans la partie droite de la fenêtre, l'onglet **Paramètres des règles** affiche les utilisateurs de confiance et les marqueur d'opérations sur les fichiers sélectionnés pour cette zone de monitoring.

5. Dans la liste des zones de monitoring ajoutées, sélectionnez celle pour laquelle vous souhaitez configurer d'autres paramètres.

6. Sélectionnez l'onglet **Utilisateurs**.

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 comme étant de confiance par Kaspersky Embedded Systems Security pour la zone de monitoring sélectionnée.

9. 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 génèrent pour ceux-ci des événements avec le niveau d'importance (cf. section « A propos des règles de monitoring des opérations sur les fichiers » à la page 223) *Événement critique*.

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 disponibles qui s'ouvre (cf. section « A propos des règles de monitoring des opérations sur les fichiers » à la page 223), cochez les cases en regard des opérations que vous souhaitez contrôler.

   Kaspersky Embedded Systems Security contrôle par défaut toutes les opérations sur les fichiers disponibles, l'option **Détecter les opérations sur les fichiers à l'aide de tous les marqueurs identifiables** est sélectionnée.

12. Si vous souhaitez que Kaspersky Embedded Systems Security calcule la somme de contrôle après les modifications, procédez comme suit :

    a. Dans le groupe **Somme de contrôle**, cochez la case **Calculer, si possible, la somme de contrôle du fichier modifié**.

        Si la case est cochée, Kaspersky Embedded Systems Security calcule la somme de contrôle du fichier modifié dans lequel une opération correspondant à au moins un marqueur d'opérations sur les fichiers a été détectée.

        Si l'opération sur le fichier est détectée à l'aide de plusieurs marqueurs, seule la somme de contrôle finale est calculée après la totalité des modifications ultérieures.

        Si la case est décochée, Kaspersky Embedded Systems Security ne calcule pas la somme de contrôle pour les fichiers modifiés.

        Kaspersky Embedded Systems Security ne calcule pas la somme de contrôle dans les cas suivants :

        - si le fichier est devenu inaccessible suite aux opérations réalisées (par exemple, modification des autorisations d'accès au fichier) ;
        - si l'opération réalisée sur le fichier concerne un fichier qui a été supprimé par la suite.

        Cette case est décochée par défaut.

    b. Sélectionnez une des options de la liste déroulante **Calculer la somme de contrôle selon l'algorithme** :

- **Hash MD5**
- **Hash SHA256**.

13. Le cas échéant, ajoutez des exclusions pour la zone de monitoring de la manière suivante :

    a. Sélectionnez l'onglet **Exclusions**.

    b. Cochez la case **Tenir compte des zones de monitoring exclues**.

        La case active ou désactive l'application des exclusions pour les dossiers dans lesquels il n'est pas nécessaire de contrôler les opérations sur les fichiers.

        Si la case est cochée, Kaspersky Embedded Systems Security ignore les zones de monitoring reprises dans la liste des exclusions lors de l'exécution de la tâche Moniteur d'intégrité des fichiers.

        Si la case est décochée, Kaspersky Embedded Systems Security enregistre les événements pour toutes les zones de monitoring définies.

        La case est décochée par défaut, la liste des exclusions est vide.

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

    La fenêtre standard de Microsoft Windows **Parcourir le dossier** s'ouvre.

    d. Dans la fenêtre qui s'ouvre, sélectionnez le dossier que vous souhaitez exclure de la zone de monitoring.

    e. Cliquez sur **Ajouter**.

    Le dossier indiqué est ajouté à la liste des zones exclues.

    > Vous pouvez également ajouter des exclusions pour la zone de monitoring manuellement en utilisant les masques identiques à ceux employés pour définir les zones de monitoring.

14. Cliquez sur le bouton **Enregistrer**.

Les règles de monitoring définie sont appliquées à la tâche Moniteur d'intégrité des fichiers.

Inspection des journaux

Cette section contient des informations sur la tâche Inspection des journaux et la configuration des paramètres de la tâche.

Dans cette section

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 informe l'administrateur en cas de détection de signes de comportement atypique dans le système pouvant indiquer des tentatives d'attaques informatiques.

Kaspersky Embedded Systems Security calcule les données des journaux des événements Windows et définit les violations conformément aux règles précisées par l'utilisateur ou aux paramètres de l'analyse heuristique, appliqués par la tâche d'inspection des journaux.

Analyseur heuristique

Vous pouvez utiliser la tâche Inspection des journaux pour contrôler l'état du système protégé sur la base des heuristiques prédéterminées. L'analyseur heuristique définit la présence d'une activité anormale sur l'ordinateur protégé qui peut être le signe d'une tentative attaque. Les modèles de définition d'une activité anormale sont inscrits dans les heuristiques accessibles dans les paramètres de l'analyseur heuristique.

La liste des heuristiques de la tâche Inspection des journaux répertorie sept heuristiques. Vous pouvez activer et désactiver l'application de n'importe quelle heuristique. Vous ne pouvez pas supprimer les heuristiques existantes ou en créer de nouvelles.

Pour chaque heuristique, vous pouvez configurer les critères de déclenchement suivants de l'analyse :

- Traitement de brute-force
- Traitement de la connexion au réseau

Dans les paramètres de la tâche, vous pouvez configurer également les exclusions. L'analyse heuristique ne se déclenche 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 du déclenchement de l'analyseur heuristique, l'application consigne l'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 de la tâche, 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 de la tâche Inspection des journaux contient quatre règles. Vous pouvez activer et désactiver l'application de 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 dans les paramètres de l'événement, l'identificateur de l'événement indiqué dans la règle est détecté. Vous pouvez ajouter et supprimer aussi des identificateurs pour chaque règle précisée.

- Source des événements.

  Pour chaque règle, vous pouvez préciser un sous-journal du journal des événements Windows. L'application exécutera la recherche des enregistrements avec les identificateurs d'événements indiqués seulement dans ce sous-journal. Vous pouvez choisir un des sous-journaux standard (App, Sécurité ou Système), ainsi qu'indiquer le sous-journal utilisateur.

  > L'application ne contrôle pas la présence réelle du sous-journal indiqué dans le journal des événements Windows.

Lors du déclenchement de la règle, Kaspersky Embedded Systems Security consigne l'événement avec le niveau d'importance *Critique* dans le journal d'exécution de la tâche Inspection des journaux.

Par défaut, la tâche Inspection des journaux ne prend pas en considération les règles utilisateur.

Configuration des règles d'inspection des journaux

Pour ajouter et configurer une nouvelle règle d'inspection des journaux définies par l'utilisateur, procédez comme suit :

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Diagnostic du système**.

2. Choisissez la sous-entrée **Inspection des journaux**.

3. Dans le volet résultats de l'entrée **Inspection des journaux**, cliquez sur le lien **Règles d'inspection des journaux**.

   La fenêtre **Règles d'inspection des journaux** s'ouvre.

4. Cochez ou décochez la case **Inspecter les journaux selon les règles définies par l'utilisateur**.

Si cette case est cochée, Kaspersky Embedded Systems Security applique les règles définies par utilisateur pour inspecter les journaux conformément aux paramètres configurés de chaque règle. Vous pouvez ajouter des règles d'inspection des journaux et les modifier.

Si la case est décochée, vous ne pouvez pas ajouter de règles définies par l'utilisateur ni en modifier. Kaspersky Embedded Systems Security applique les paramètres des règles par défaut.

Vous ne pouvez pas supprimer ou modifier les règles prédéfinies.

Cette case est décochée par défaut.

Vous pouvez contrôler l'application des règles prédéfinies dans la liste des règles. Cochez les cases en regard des règles que vous voulez appliquer à l'inspection des journaux.

1. Pour créer une règle définie par l'utilisateur, procédez comme suit :

   a. Saisissez le nom de la nouvelle règle.

   b. Cliquez sur **Ajouter**.

   La règle créée est ajoutée à la liste générale des règles.

2. Pour configurer n'importe quelle règle, procédez comme suit :

   a. Sélectionnez la règle dans la liste d'un clic gauche de la souris.

   Dans la partie droite de la fenêtre, les informations générales relatives à la règle s'affiche sous l'onglet **Commentaires**.

Les commentaires pour une nouvelle règle sont vides.

b. Sélectionnez l'onglet **Description**.

c. Dans le groupe **Général**, modifiez le nom de la règle le cas échéant.

d. Sélectionnez l'option **Source pour l'analyse des données**.

Sélectionnez le journal dont les événements sont utilisés pour l'inspection. Vous avez le choix parmi les types de journaux Windows suivants :

- Application
- Security
- System

3. Dans le groupe **Paramètres de déclenchement**, indiquez les identificateurs des enregistrements dont la détection va déclencher la règle :

a. Saisissez la valeur numérique de l'identifiant.

b. Cliquez sur **Ajouter**.

L'identifiant de la règle indiqué est ajouté à la liste. Vous pouvez ajouter un nombre illimité d'identifiants pour chaque règle.

c. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés des règles d'inspection des journaux sont appliqués.

Configuration de l'analyse heuristique

► *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 Kaspersky Embedded Systems Security, développez l'entrée **Diagnostic du système**.

2. Choisissez la sous-entrée **Inspection des journaux**.
3. Dans le volet résultats de l'entrée **Inspection des journaux**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Sélectionnez l'onglet **Analyse heuristique**.
5. Cochez ou décochez la case **Appliquer l'analyse heuristique à l'inspection des journaux**.

   Si cette case est cochée, Kaspersky Embedded Systems Security applique l'analyse heuristique pour détecter toute activité anormale sur l'ordinateur protégé.

   Si cette case n'est pas cochée, l'analyse heuristique est désactivée, Kaspersky Embedded Systems Security utilise les règles prédéfinies ou définies par l'utilisateur pour détecter les activités anormales.

Pour que la tâche fonctionne, il faut sélectionner au moins un mode d'inspection des journaux.

   Cette case est cochée par défaut.
1. Sélectionnez les éléments heuristiques que vous souhaitez appliquer à l'inspection des journaux dans la liste des éléments disponibles :
   - Détection d'une tentative possible d'effraction du mot de passe.
   - Détection d'indices de compromission des journaux Windows.
   - Détection d'une activité suspecte émanant d'un nouveau service installé.
   - Détection d'une authentification avec indication évident d'identifiants.
   - Détection d'indices d'attaque Kerberos forged PAC (MS14-068).
   - Détection de modifications suspectes du groupe privilégié Administrators.
2. Pour configurer les paramètres des éléments heuristiques choisis, accédez à l'onglet **Critères de déclenchement**.

3. Dans le groupe **Traitement de brute-force**, définissez le nombre de tentatives et l'intervalle d'exécution de celles-ci qui vont servir de critères de déclenchement de l'analyse heuristique.

4. Dans le groupe **Traitement de la 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.

5. Sélectionnez l'onglet **Exclusions**.

6. 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 **OK**.

    L'utilisateur indiqué est ajouté à la liste des utilisateurs de confiance.

7. Pour ajouter les adresses IP à considérer comme adresses de confiance, procédez comme suit :

    a. Saisissez l'adresse IP.

    b. Cliquez sur **Ajouter**.

8. L'adresse IP indiquée est ajoutée à la liste des adresses de confiance.

9. Sélectionnez l'onglet **Administration des tâches** pour configurer la planification du lancement de la tâche.

10. Cliquez sur **OK**.

    Les paramètres de la tâche Inspection des journaux sont enregistrés.

Analyse à la demande

Cette section contient des informations sur les tâches d'analyse à la demande et explique la configuration des paramètres des tâches d'analyse à la demande ainsi que la configuration des paramètres de la sécurité de l'ordinateur protégé.

Dans cette section

A propos des tâches d'analyse à la demande

Kaspersky Embedded Systems Security recherche une fois des virus et autres menaces informatique dans la zone indiquée. Kaspersky Embedded Systems Security analyse les fichiers, la mémoire vive de l'ordinateur et les objets de démarrage.

Kaspersky Embedded Systems Security prévoit quatre tâches système d'analyse à la demande :

- 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 d'amorçage et les principaux enregistrements d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des processus. A chaque exécution de la tâche, Kaspersky Embedded Systems Security crée une copie des secteurs d'amorçage sains et si lors de l'exécution suivante de la tâche il découvre une menace, il remplace les secteurs d'amorçage infectés par les copies de sauvegarde saines.
- La tâche Analyse des zones critiques 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 d'amorçage et entrées principales d'amorçage des disques durs et des disques amovibles, la mémoire système et la mémoire des 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 dont les valeurs correspondent au niveau **Recommandé** (cf. section « **Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande** » à la page 268). Vous pouvez modifier les paramètres la tâche Analyse des zones critiques.
- La tâche Analyse des objets en quarantaine est exécutée par défaut selon la programmation après chaque mise à jour des bases de données. Vous ne pouvez pas modifier les paramètres de la tâche Analyse des objets en quarantaine.
- La tâche Vérification de l'intégrité de l'application est exécutée à chaque démarrage de Kaspersky Embedded Systems Security. 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 sur l'exécution des tâches contiennent des informations sur le nombre de modules analysés ou endommagés. Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. La planification du lancement de la tâche peut être modifiée.

Vous pouvez créer des tâches d'analyse à la demande définies par l'utilisateur. Par exemple, vous pouvez créer une tâche d'analyse du dossier partagé sur l'ordinateur.

Kaspersky Embedded Systems Security peut exécuter simultanément plusieurs tâches d'analyse à la demande.

Statistiques des tâches d'analyse à la demande

Pendant que la tâche d'analyse à la demande est exécutée, vous pouvez consulter des informations détaillées sur le nombre d'objets traités par Kaspersky Embedded Systems Security depuis son lancement jusqu'à maintenant.

Ces informations seront accessibles même si vous arrêtez la tâche. Vous pouvez consulter les statistiques de la tâche dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches » à la page 345).

► *Pour consulter les statistiques de la tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.

Le volet résultats de l'entrée sélectionnée reprend les statistiques de la tâche dans le groupe **Statistiques**.

Vous pouvez consulter les informations suivantes sur les objets que Kaspersky Embedded Systems Security a traités depuis le lancement de la tâche jusqu'au moment présent (cf. tableau ci-dessous).

Tableau 27. 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 application malveillante dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres détectés	La quantité d'objets considérés comme infectés par Kaspersky Embedded Systems Security ou d'objets détectés qui sont des applications légitimes qui n'ont pas été exclues de la zone d'action des tâches de la protection en temps réel ou d'analyse.
Objets probablement infectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Embedded Systems Security.
Objets non désinfectés	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu désinfecter pour les raisons suivantes : • Le type d'objet détecté 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 un autre programme.
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.

Champ	Description
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 total 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** dans le groupe **Administration** du volet résultats.

A la fin de l'exécution de la tâche d'analyse à la demande, il est conseillé de traiter manuellement les événements du journal d'exécution de la tâche sous l'onglet **Evénements**.

Configuration des tâches 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 système et définies par l'utilisateur.

Tableau 28. Paramètres des tâches d'analyse à la demande

Paramètre	Valeur	Configuration
Zone d'analyse	S'applique aux tâches système et définies par l'utilisateur : • Analyse au démarrage du système d'exploitation : tout l'ordinateur, à l'exception des dossiers partagés et des objets de démarrage ; • Analyse rapide : tout l'ordinateur, à l'exception des dossiers partagés et de certains fichiers du système d'exploitation ; • Tâches d'analyse à la demande définies par l'utilisateur : tout l'ordinateur.	Vous pouvez modifier la zone d'analyse. Il est impossible de configurer la zone de protection pour les tâches système Analyse des objets en quarantaine et Vérification de l'intégrité de l'application.

Paramètre	Valeur	Configuration
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; correspondent au niveau de sécurité **Recommandé**.	Pour les entrées sélectionnées dans l'arborescence ou dans la liste des ressources de fichiers de l'ordinateur, 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 n'importe quel autre nœud.
Analyseur heuristique	Les tâches Analyse rapide et Analyse au démarrage du système d'exploitation, aussi que les tâches d'analyse définies par l'utilisateur, sont exécutées selon la valeur **Moyenne**. La tâche Analyse des objets en quarantaine est réalisée selon la valeur **Minutieuse**.	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 des objets en quarantaine. L'application de l'analyse heuristique n'est pas prévue dans la tâche Vérification de l'intégrité de l'application.
Zone de confiance	Appliquée	Seule liste d'exclusions que vous pouvez appliquer dans les tâches sélectionnées.

Paramètre	Valeur	Configuration
Utilisation du KSN	Appliquée	Vous pouvez améliorer l'efficacité de la protection de l'ordinateur en utilisant l'infrastructure de services cloud du Kaspersky Security Network.
Paramètres du lancement de la tâche en tant que	La tâche est lancée sous les autorisations du compte système.	Vous pouvez modifier les paramètres de lancement sous les autorisations d'un compte utilisateur pour tous les tâches d'analyse à la demande système ou définies par l'utilisateur, sauf pour les tâches Analyse des objets en quarantaine et Vérification de l'intégrité de l'application.
Exécution en mode arrière-plan (priorité basse)	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.

Paramètre	Valeur	Configuration
Planification du lancement de la tâche	S'applique aux tâches système : • Analyse au démarrage du système d'exploitation : **Au lancement de l'application** ; • Analyse des zones critiques : **Chaque semaine** ; • Analyse des objets en quarantaine : **A la mise à jour des bases de l'application** ; • Vérification de l'intégrité de l'application : **Au lancement de l'application**. Pas appliqué dans les tâches définies par l'utilisateur recréées.	Vous pouvez configurer les paramètres de lancement de la tâche selon la planification.
Enregistrement de l'exécution de l'analyse et de la mise à jour de l'état de la protection de l'ordinateur	L'état de la protection de l'ordinateur est actualisé chaque semaine après l'exécution de la tâche Analyse des zones critiques.	Vous pouvez configurer les paramètres d'enregistrement de l'exécution de l'analyse des zones critiques d'une des manières suivantes : • En modifiant les paramètres de la planification du lancement de la tâche Analyse des zones critiques ; • En modifiant la zone de protection de la tâche Analyse des zones critiques ; • En créant des tâches d'analyse à la demande définies par l'utilisateur.

► *Pour configurer une tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.

3. Sous l'onglet **Consultation et administration** dans le volet résultats de l'entrée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre. Configurez les paramètres de la tâche suivants :

   - Sous l'onglet **Général** :
     - Application de l'analyseur heuristique (à la page 251).
     - Exécution de la tâche en mode arrière-plan (cf. section « Exécution en mode arrière-plan de la tâche d'analyse à la demande » à la page 252).
     - Utilisation du KSN (à la page 253).
     - Application de la zone de confiance (cf. section « Activation et désactivation de l'application de la zone de confiance dans les tâches de Kaspersky Embedded Systems Security » à la page 65).
     - Enregistrement de l'exécution de l'analyse des zones critiques (à la page 255)
   - Sous les onglets **Planification** et **Avancé** :
     - Paramètres de lancement de la tâche selon la planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).
   - Sous l'onglet **Exécuter en tant que** :
     - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81).

4. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   Les modifications apportées aux paramètres seront enregistrées.

5. Le cas échéant, ouvrez l'onglet **Configuration de la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   Exécutez les actions suivantes :

- Dans l'arborescence des ressources fichier du serveur, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.

- Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section « Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande » à la page 268) ou configurez manuellement les paramètres de protection des objets (cf. section « Configuration manuelle des paramètres de sécurité » à la page 272).

6. Dans le menu contextuel du nom de la tâche sélectionnée, sélectionnez **Enregistrer la tâche**.

Kaspersky Embedded Systems Security appliquera immédiatement les nouvelles valeurs des paramètres dans la tâche en cours d'exécution. Les informations sur 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'exécution de la tâche.

Application de l'analyseur heuristique

► *Pour configurer l'analyse heuristique, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.
3. Dans le volet résultats, passez au lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Utiliser l'analyse heuristique**.
5. Si nécessaire, réglez le niveau de l'analyse à l'aide du curseur.

   Le curseur permet de régler le niveau de l'analyse heuristique. Le niveau de spécification de l'analyse 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 détail pour l'analyse :

   - **Superficielle**. L'analyse heuristique exécute moins d'actions contenues dans le fichier exécutable. 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 dans le fichier exécutable conforme aux recommandations des experts de Kaspersky Lab.

  Il s'agit du niveau par défaut.

- **Minutieuse**. L'analyseur 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 de faux positifs peut augmenter.

Le curseur est actif quand la case **Utiliser l'analyse heuristique** est cochée.

6. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Exécution en mode arrière-plan de la tâche d'analyse à la demande

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 de base **Faible** (**Low**) au processus dans lequel la tâche d'analyse à la demande sera exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur la vitesse d'exécution des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter quelques tâches en mode arrière-plan. Vous pouvez définir le nombre maximum de processus pour les tâches d'analyse à la demande en mode arrière-plan.

► *Pour modifier la priorité de la tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche dont vous souhaitez modifier la priorité.
3. Dans le volet résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Exécuter la tâche en arrière-plan**.

   La case modifie la priorité de la tâche.

   Quand la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et du système de fichiers du serveur par les autres tâches de Kaspersky Embedded Systems Security ou les autres applications. Par conséquente la vitesse d'exécution de la tâche diminuera quand la charge augmentera et augmentera dans le cas contraire.

   Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Embedded Systems Security et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

   Cette case est décochée par défaut.
5. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Utilisation du KSN

Il est indispensable d'accepter la Déclaration de Kaspersky Security Network afin de lancer la tâche Utilisation du KSN.

Si vous avez accepté la Déclaration de Kaspersky Security Network pendant l'installation de l'application, la tâche Utilisation du KSN est lancée automatiquement au démarrage de Kaspersky Embedded Systems Security. Vous pouvez lancer une tâche manuellement (cf. section « Lancement et arrêt d'une tâche Utilisation du KSN » à la page 132) ou planifier son exécution (cf. section « Configuration des paramètres d'une tâche Utilisation du KSN » à la page 134).

► *Pour configurer l'utilisation du KSN dans les tâches d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche que vous souhaitez configurer.
3. Dans le volet résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Cochez ou décochez la case **Utiliser KSN pour l'analyse**.

   La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

   Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

   Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

   Cette case est cochée par défaut.
5. Cliquez sur **OK**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Enregistrement de l'exécution de l'analyse des zones critiques

Par défaut, l'état de la protection de l'ordinateur apparaît dans le volet résultats de l'entrée **Kaspersky Embedded Systems Security** et il est actualisé chaque semaine après la fin de la tâche Analyse des zones critiques.

L'heure de l'actualisation de l'état de la protection de l'ordinateur 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. La case est cochée uniquement pour la tâche Analyse rapide et ne peut être modifiée.

> Vous pouvez réaffecter la tâche d'analyse à la demande à l'état de la protection de l'ordinateur uniquement au départ de Kaspersky Security Center.

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.

Dans cette section

Présentation de la zone d'analyse

Vous pouvez configurer la zone d'analyse pour les tâches Analyse au démarrage du système d'exploitation et Analyse rapide ainsi que pour les tâches d'analyse à la demande définies par l'utilisateur.

Par défaut, les tâches d'analyse à la demande analysent tous les objets du système de fichiers de l'ordinateur. Si les exigences en matière de sécurité ne nécessitent pas une analyse de tous les objets du système de fichiers, vous pouvez limiter la zone d'analyse.

Dans la Console de Kaspersky Embedded Systems Security, la zone d'analyse se présente sous la forme d'une arborescence ou d'une liste de ressources de fichiers de l'ordinateur que l'application peut analyser. Par défaut les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de la liste.

► *Pour insérer l'affichage des ressources fichiers de l'ordinateur sous la forme de l'arborescence,*

Dans la liste déroulante du coin supérieur gauche de la fenêtre **Configuration de la zone de protection**, choisissez l'option **Afficher sous forme d'arbre**.

Les entrées de la liste ou de l'arborescence des ressources de fichiers de l'ordinateur sont illustrées de la manière suivante :

☑ Nœud repris dans la zone d'analyse.

☐ Nœud exclu de la zone d'analyse.

☑ Au moins une des entrées intégrées à cette entrée est exclue de la zone d'analyse ou les paramètres de protection de ces entrées diffèrent des paramètres de protection de l'entrée de niveau supérieur.

L'icône ☑ s'affiche si toutes les sous-entrées ont été sélectionnées mais pas l'entrée principale. Le cas échéant, les modifications du contenu des fichiers et dossiers de l'entrée principale ne sont pas automatiquement prises en compte lors de la constitution de la zone d'analyse de la sous-entrée sélectionnée.

Le nom des nœuds virtuels de la zone d'analyse apparaît en lettres bleues.

Configuration des paramètres de l'affichage des ressources de fichiers de la zone d'analyse

► *Pour choisir le mode d'affichage des ressources de fichiers de l'ordinateur lors de la configuration des paramètres de la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.

3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

4. Dans un gauche angle supérieur de la fenêtre ouverte déployez la liste déroulante. Exécutez une des actions suivantes :

   - Choisissez le point **Afficher sous la forme de l'arborescence**, si vous voulez que les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de l'arborescence.

   - Choisissez le point **Afficher sous la forme de la liste**, si vous voulez que les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de la liste.

   > Par défaut les ressources fichiers de l'ordinateur protégé s'affichent sous la forme de la liste.

5. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone d'analyse** se ferme. Les paramètres de la tâche définis seront appliqués.

Zones d'analyse prédéfinies

L'arborescence ou la liste des ressources de fichiers de l'ordinateur est affichée dans le volet résultats de l'entrée de la tâche d'analyse à la demande sélectionnée via le lien **Configurer la zone d'analyse**.

L'arborescence des ressources fichiers représente les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security prévoit les zone d'analyse prédéfinies suivantes :

- **Poste de travail**. Kaspersky Embedded Systems Security analyse tout l'ordinateur.
- **Disques durs locaux**. Kaspersky Embedded Systems Security analyse les objets sur les disques durs de l'ordinateur. 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 objets sur les périphériques externes tels que les disques compacts ou 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.
- **Emplacements 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 répertoires de réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte système.
- **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 exécutés au démarrage du système**. Kaspersky Embedded Systems Security analyse les objets sur lesquels les clés de la base de registres et les fichiers de configuration, par exemple WIN.INI ou SYSTEM.INI, s'appuient ainsi que les modules logiciels des applications qui sont exécutées automatiquement au démarrage de l'ordinateur.

- **Dossiers partagés**. Vous pouvez ajouter les dossiers partagés de l'ordinateur à protéger à la zone d'analyse.
- **Disques virtuels**. Vous pouvez inclure dans la zone d'analyse les disques, les dossiers et les fichiers dynamiques ainsi que les disques qui sont contrôlés sur l'ordinateur, par exemple les disques partagés d'une grappe.

Les zone d'analyse prédéfinies s'affichent par défaut dans l'arborescence des ressources de fichiers de l'ordinateur et acceptent l'ajout à la liste des ressources de fichiers 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**.
- Tâche Analyse rapide :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles** ;
  - **Mémoire système** ;
  - **Objets exécutés au démarrage du système**.
- Tâche d'analyse à la demande définie par l'utilisateur :
  - **Disques durs locaux** (sauf dossier Windows) ;
  - **Disques amovibles** ;
  - **Mémoire système** ;
  - **Objets exécutés au démarrage du système** ;
  - **Dossiers partagés**.

Les pseudo-disques, créés à l'aide de la commande SUBST, ne figurent pas dans l'arborescence des ressources fichier du serveur dans la Console de Kaspersky Embedded Systems Security. Pour analyser les objets d'un pseudo-disque, il faut inclure dans la zone d'analyse le répertoire de l'ordinateur auquel ce pseudo-disque est lié.

Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier du serveur. 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).

Constitution de la zone d'analyse

Si vous administrez Kaspersky Embedded Systems Security sur l'ordinateur protégé à distance via la console de Kaspersky Embedded Systems Security 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 de l'ordinateur.

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 et Analyse des zones critiques, vous pourrez rétablir la zone d'analyse par défaut dans ces tâches en exécutant la restauration de Kaspersky Embedded Systems Security (**Démarrer** → **Programmes** → **Kaspersky Embedded Systems Security** → **Modification ou suppression**). Dans l'Assistant d'installation cochez la case **Rétablir les paramètres recommandés de fonctionnement de l'application**.

La procédure de constitution de la zone d'analyse dans les tâches d'analyse à la demande dépend du type d'affichage des ressources de fichiers de l'ordinateur protégé (cf. section « Configuration des paramètres de l'affichage des ressources de fichiers de la zone de protection » à la page 111). Vous pouvez configurer l'affichage des ressources fichiers sous la forme de la liste (est appliqué par défaut) ou sous la forme de l'arborescence.

► *Pour composer la zone d'analyse, au départ l'arborescence des ressources de fichiers, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.

3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

4. Dans la partie droite de la fenêtre ouverte déployez l'arborescence des ressources fichiers de l'ordinateur pour afficher tous les nœuds.

5. 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 à la zone d'analyse, décochez la case **Poste de travail** et procédez comme suit :

     - Si vous souhaitez inclure tous les disques d'un même type, cochez la case en regard du nom du type de disque requis (par exemple, pour inclure tous les disques amovibles sur le serveur, cochez la case **Disques amovibles**) ;

     - Si vous souhaitez inclure un disque particulier du type requis, déployez 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:**, ouvrez le nœud **Disques amovibles** et cochez la case en regard du disque **F:** ;

     - Si vous souhaitez inclure à la zone de protection un dossier ou un fichier sur le disque en particulier, cochez la case à côté de ce dossier ou de ce fichier.

6. Cliquez sur le bouton **Enregistrer**.

La fenêtre **Configuration de la zone de protection** sera fermée. Les paramètres de la tâche définis seront enregistrés.

► *Pour former la zone de protection, en travaillant avec la liste des ressources fichiers, exécutez les actions suivantes :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.

3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

4. Pour inclure certaines entrées 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 avec le bouton droit de la souris.

   b. Dans le menu contextuel, choisissez l'option **Ajouter 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 à la zone d'analyse :

   - **Zone prédéfinie**, si vous voulez inclure dans la zone d'analyse une des zones prédéfinies sur l'ordinateur protégé. Puis dans la liste déroulante choisissez la zone nécessaire.
   - **Disque, dossier ou objet réseau**, si vous voulez insérer dans la zone d'analyse un disque, un dossier ou un objet réseau distinct du type nécessaire. Puis choisissez la zone requise via le bouton **Parcourir**.
   - **Fichier**, si vous voulez insérer dans la zone d'analyse uniquement un fichier distinct sur le disque. Puis choisissez le fichier nécessaire via le bouton **Parcourir**.

   Vous ne pouvez pas ajouter un objet à la zone d'analyse s'il est déjà ajouté en tant qu'exclusion de la zone de protection.

5. 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 le type de l'objet que vous voulez ajouter à titre de l'exclusion de la zone de protection, de la même manière que l'ajout d'un objet à la zone d'analyse.

6. Pour modifier la zone d'analyse ou l'exclusion ajoutée, dans le menu contextuel de la zone que vous voulez modifier, choisissez l'option **Modifier la zone**.

7. Pour masquer l'affichage d'une zone d'analyse ou d'une exclusion ajoutée au préalable à la liste des ressources de fichiers, dans le menu contextuel de la zone que vous voulez masquer, choisissez l'option **Supprimer de la liste**.

    La zone d'analyse est exclue de la zone d'action de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichiers.

8. 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 inclure un objet de réseau dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dans la zone d'analyse de laquelle vous souhaitez ajouter un chemin de réseau.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le panneau des résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Dans le menu contextuel du nom de l'entrée **Emplacements réseau**, réalisez les opérations suivantes :
   - 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.
6. Saisissez le chemin d'accès au répertoire de réseau ou au fichier au format UNC (Universal Naming Convention) et appuyez sur la touche **ENTER**.
7. Cochez la case en regard du nom de l'objet réseau ajouté afin de l'inclure dans la zone d'analyse.
8. Le cas échéant, modifiez les paramètres de sécurité de l'objet réseau ajouté.
9. 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 dynamiques ou créer une zone d'analyse 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 des ressources de fichiers (cf. section « Configuration des paramètres de l'affichage des ressources de fichiers de la zone de protection » à la page 111).

► *Pour inclure un disque virtuel dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez constituer une zone d'analyse.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.
5. Dans l'arborescence des ressources de fichiers de l'ordinateur, ouvrez le menu contextuel de l'entrée **Disques virtuels** et sélectionnez le nom du disque virtuel créé dans la liste des noms disponibles.
6. Cochez la case à côté du disque ajouté afin de l'inclure dans la zone d'analyse.
7. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

► *Pour ajouter un dossier ou un fichier virtuel dans la zone d'analyse, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la tâche d'analyse à la demande pour laquelle vous souhaitez composer une zone d'analyse virtuelle.

3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

4. Dans la liste déroulante du coin supérieur gauche de la fenêtre, choisissez l'option **Afficher sous forme d'arbre**.

5. Dans l'arborescence des ressources de fichiers de l'ordinateur, ouvrez le menu contextuel de l'unité à laquelle 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 de protection.

   - **Ajouter un fichier virtuel**, si vous souhaitez ajouter un fichier virtuel à la zone de protection.

6. Dans le champ, saisissez le nom du dossier ou du fichier.

   Vous pouvez définir un masque de nom de fichier en utilisant les caractères * et ?.

7. Dans la ligne contenant le nom du dossier ou du fichier créé, cochez la case afin de l'inclure dans la zone d'analyse.

8. Cliquez sur le bouton **Enregistrer**.

Les modifications apportées aux paramètres de la tâche seront enregistrées.

Paramètres de sécurité de l'entrée sélectionnée dans la tâche d'analyse à la demande

Dans la tâche d'analyse 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 dans l'arborescence ou la liste des ressources de fichiers de l'ordinateur.

Les paramètres de sécurité configurés pour l'entrée principale sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

Vous pouvez configurer les paramètres 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 fichiers du serveur (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.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour l'entrée sélectionnée dans l'arborescence des ressources de fichiers de l'ordinateur, vous pouvez appliquer un des trois niveaux de sécurité prédéfinis suivant : **Performance maximale**, **Recommandé** et **Protection maximale**. Chacun de ces niveaux de sécurité prédéfinis possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Performance maximale

Il est conseillé d'appliquer le niveau de sécurité **Performance maximale** si votre réseau prévoit d'autres mesures de protection informatiques (par exemple, pare-feu) en plus de l'utilisation de Kaspersky Embedded Systems Security sur les serveurs et les postes de travail, si des mesures de sécurité complémentaires comme des pare-feu sont configurées ou si des stratégies de sécurité sont en vigueur pour les utilisateurs du réseau.

Recommandé

Le niveau de sécurité **Recommandé** offre l'équilibre idéal entre la qualité de la protection et l'impact sur les performances des serveurs protégés. Il est recommandé par les experts de Kaspersky Lab en tant que niveau suffisant pour la protection des serveurs de fichiers dans la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Il est conseillé d'utiliser le niveau de sécurité **Protection maximale** si vos exigences vis-à-vis de la sécurité du réseau de l'entreprise sont strictes.

Tableau 29. Niveaux de sécurité prédéfinis et valeurs des paramètres correspondants

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
Analyse des objets	En fonction du format	Tous les objets	Tous les objets
Optimisation	Activée	Désactivée	Désactivée
Actions à exécuter sur les objets infectés et autres détecté	Désinfecter, supprimer si la désinfection est impossible	Désinfecter, supprimer si la désinfection est impossible (**Exécuter l'action recommandée**)	Désinfecter, supprimer si la désinfection est impossible
Action à exécuter sur les objets probablement infectés	Placer en quarantaine	Placer en quarantaine (**Exécuter l'action recommandée**)	Placer en quarantaine

Paramètres	Niveau de sécurité		
	Performance maximale	Recommandé	Protection maximale
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* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * Tous les objets	• Archives* • Archives SFX* • Bases de données de messagerie électronique* • Message de texte plat* • Objets compactés* • Objets OLE intégrés* * Tous les objets

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** ou **Utiliser l'analyse heuristique**, le niveau de sécurité prédéfini que vous avez sélectionné ne change pas.

► *Pour sélectionner un des niveaux de sécurité prédéfinis, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Sélectionnez la sous-entrée qui correspond à la tâche pour laquelle vous souhaitez configurer les paramètres de sécurité.
3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.
4. Dans l'arborescence ou dans la liste des ressources de fichiers de l'ordinateur, sélectionnez l'entrée pour laquelle vous souhaitez sélectionner un niveau de sécurité prédéfini.
5. Assurez-vous que le nœud sélectionné se trouve dans la zone d'analyse.
6. Sous l'onglet **Niveau de sécurité** de la partie droite de la fenêtre, sélectionnez le niveau que vous souhaitez appliquer.

   La fenêtre reprend la liste des valeurs des paramètres de sécurité correspondant au niveau de sécurité que vous avez sélectionné.
7. Cliquez sur le bouton **Enregistrer**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, alors 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. Leurs valeurs correspondent aux valeurs du niveau de sécurité prédéfini **Recommandé** (cf. section « **Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande** » à la page 268).

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 différentes entrées dans l'arborescence ou la liste des ressources de fichiers de l'ordinateur.

Lors de l'utilisation de l'arborescence des ressources fichiers, les paramètres de sécurité configurés pour l'entrée principale sélectionnée sont appliqués automatiquement à toutes les sous-entrées. Les paramètres de sécurité de l'entrée mère ne sont pas appliqués aux sous-entrées configurées séparément.

► *Pour configurer les paramètres de sécurité manuellement, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.

2. Sélectionnez la sous-entrée qui correspond à la tâche pour laquelle vous souhaitez configurer les paramètres de sécurité.

3. Cliquez sur le lien **Configurer la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   La fenêtre **Configuration de la zone d'analyse** s'ouvre.

4. Dans la partie gauche de la fenêtre, sélectionnez l'entrée dont vous souhaitez configurer les paramètres de sécurité.

   Pour la zone d'analyse sélectionnée, vous pouvez appliquer un modèle prédéfini contenant un ensemble de paramètres de sécurité (cf. section « A propos des modèles de paramètres de sécurité » à la page 87).

5. Configurez les paramètres de sécurité requis pour le nœud sélectionné en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, configurez les paramètres suivants, si nécessaire :

     Dans le groupe **Couverture de l'analyse**, indiquez les objets que vous souhaitez inclure à la zone d'analyse :

     - **Tous les objets.**

       Kaspersky Embedded Systems Security analyse tous les objets.

     - **Objets analysés en fonction du format.**

       Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base du format du fichier.

       La liste de ces formats est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Embedded Systems Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus.**

       Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier.

       La liste de ces extensions est élaborée par les experts de Kaspersky Lab et fait partie des bases de Kaspersky Security.

     - **Objets analysés en fonction de la liste d'extensions indiquée.**

       Kaspersky Embedded Systems Security analyse les fichiers sur la base de l'extension. Vous pouvez définir manuellement la liste des extensions des fichiers à analyser en appuyant sur le bouton **Modifier** dans la fenêtre **Liste des extensions**.

     - **Secteurs d'amorçage des disques MBR.**

       Activation de la protection des secteurs d'amorçage et des enregistrements principaux d'amorçage.

       Quand la case est cochée, Kaspersky Embedded Systems Security analyse les secteurs et les enregistrements d'amorçage sur les disques durs et les disques amovibles du serveur.

       Cette case est cochée par défaut.

- **Analyser les flux NTFS alternatifs.**

  Analyse les flux complémentaires de fichiers et de dossiers dans les disques du système de fichiers NTFS.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les flux complémentaires des fichiers et des dossiers.

  Cette case est cochée par défaut.

Dans le groupe **Optimisation**, cochez ou décochez la case :

- **Analyser uniquement les nouveaux fichiers et les fichiers modifiés.**

  La case active ou désactive l'analyse et la protection des fichiers que Kaspersky Embedded Systems Security a identifié comme étant nouveaux ou ayant été modifiés depuis la dernière analyse.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse et protège uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse et protège tous les fichiers.

  La case est cochée par défaut pour le niveau de sécurité **Performance maximale**. Si le niveau de sécurité sélectionné est **Recommandé** ou **Protection maximale**, la case est décochée.

Dans le groupe **Analyse des objets composés**, indiquez les objets composés que vous souhaitez inclure à la zone d'analyse :

- **Toutes les / Uniquement les nouvelles archives.**

  Analyse des archives au format ZIP, CAB, RAR, ARJ et autres.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les archives.

  Si la case est décochée, Kaspersky Embedded Systems Security ignore les archives lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Toutes les / Les nouvelles archives SFX.**

  Analyse des archives qui contiennent un module logiciel de décompactage.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les archives SFX.

  Si la case est décochée, Kaspersky Embedded Systems Security ignore les archives SFX lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Le paramètre est actif si la case **Archives** n'est pas cochée.

- **Toutes les / Les nouvelles bases de données de messagerie.**

  Analyse des fichiers des bases de données de messagerie de Microsoft Office Outlook® et Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers des bases de données de messagerie.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers des bases de données de messagerie lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets compactés.**

  Analyse des fichiers exécutables compactés à l'aide d'un programme à double code comme UPX ou ASPack.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers exécutables compactés par des logiciels de compression.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers exécutables compactés par des logiciels de compression lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux messages de texte plat.**

  Analyse des fichiers des bases de données de messagerie, par exemple des messages au format Microsoft Outlook ou Microsoft Outlook Express.

  Quand la case est cochée, Kaspersky Embedded Systems Security analyse les fichiers aux formats de messagerie.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les fichiers aux formats de messagerie lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

- **Tous les / Les nouveaux objets OLE incorporés.**

  Analyse des objets intégrés à un fichier (par exemple, une macro Microsoft Word ou une pièce jointe dans un message électronique).

  Si la case est cochée, Kaspersky Embedded Systems Security analyse les objets intégrés au fichier.

  Quand la case est décochée, Kaspersky Embedded Systems Security ignore les objets intégrés au fichier lors de l'analyse.

  La valeur par défaut dépend du niveau de sécurité sélectionné.

  Vous pouvez choisir d'analyser tous les objets composés ou uniquement les nouveaux si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée. Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est décochée, Kaspersky Embedded Systems Security analyse tous les objets composés désignés.

- Sur l'onglet **Actions**, réalisez les actions suivantes, le cas échéant :

  - Sélectionnez l'action à exécuter sur les objets infectés et autres détectés.
  - Sélectionnez l'action à exécuter sur les objets probablement infectés.
  - Le cas échéant, configurez les actions en fonction du type d'objet à détecter.

- Choisissez les actions à exécuter sur les conteneurs non modifiables : cochez ou décochez la case **Forcer la suppression du fichier conteneur parent en cas de détection d'un objet infecté ou autre joint quand la modification du conteneur est impossible**.

  La case active ou désactive la suppression forcée du conteneur parent en cas de détection d'un objet intégré malveillant ou autre.

  Si la case est cochée et que **Supprimer** est l'action à exécuter sur les fichiers infectés et probablement infectés, Kaspersky Embedded Systems Security force la suppression de l'ensemble du conteneur parent en cas de détection d'un objet malveillant ou d'un autre type d'objet à détecter intégré. La suppression forcée du conteneur parent et de l'ensemble de son contenu a lieu si l'application ne parvient pas à supprimer uniquement l'objet détectable intégré (par exemple, si le conteneur parent ne peut pas être modifié).

  Si la case est décochée et que **Supprimer** est l'action à exécuter sur les fichiers infectés et probablement infectés, Kaspersky Embedded Systems Security n'exécute pas l'action indiquée pour le conteneur parent en cas de détection d'un objet malveillant ou d'un autre type d'objet à détecter intégré si ce conteneur parent n'est pas modifiable.

  La case est cochée par défaut pour le niveau de sécurité **Protection maximale**. La case est décochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- Sous l'onglet **Optimisation**, configurez les paramètres suivants, si nécessaire :

  Dans le groupe **Exclusions** :

  - **Exclure les fichiers.**

    Exclusion des objets de l'analyse sur la base d'un nom ou d'un masque de nom de fichier.

    Si la case est cochée, Kaspersky Embedded Systems Security ignore les objets indiqués pendant l'analyse.

    Si la case est décochée, Kaspersky Embedded Systems Security analyse tous les objets.

    Cette case est décochée par défaut.

- **Ne pas détecter**.

  Exclusion de l'analyse des objets à détecter sur la base du nom ou d'un masque de nom d'objet à détecter. La liste des noms des objets à détecter figure sur le site de l'Encyclopédie des virus (https://securelist.fr).

  Si la case est cochée, Kaspersky Embedded Systems Security ignore les objets à détecter indiqués pendant l'analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security détecte tous les objets indiqués par défaut dans l'application.

  Cette case est décochée par défaut.

Dans le groupe **Paramètres avancés** :

- **Arrêter si l'analyse dure plus de (s.).**

  Restriction de la durée d'analyse d'un objet. La valeur par défaut est de 60 secondes.

  Si la case est cochée, la durée maximale de l'analyse d'un objet est égale à la valeur indiquée.

  Si la case n'est pas cochée, aucune limite n'est imposée sur la durée de l'analyse.

  Cette case est cochée par défaut.

- **Ne pas analyser les objets composés de plus de (Mo).**

  Exclut de l'analyse les objets complexes dont la taille est supérieure à la valeur indiquée. La valeur par défaut est de 8 Mo.

  Si la case est cochée, Kaspersky Embedded Systems Security ne réalise pas la recherche de virus dans les objets complexes dont la taille est supérieure à la valeur indiquée.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les objets complexes sans tenir compte de la taille.

  La case est cochée par défaut pour les niveaux de sécurité **Recommandé** et **Performance maximale**.

- **Utiliser la technologie iChecker.**

  Analyse uniquement des nouveaux fichiers ou des fichiers modifiés depuis la dernière analyse.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse uniquement les fichiers considérés comme nouveaux ou modifiés depuis la dernière analyse.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les fichiers sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

- **Utiliser la technologie iSwift**.

  Analyse uniquement des nouveaux objets ou des fichiers objets depuis la dernière analyse dans le système de fichiers NTFS.

  Si la case est cochée, Kaspersky Embedded Systems Security analyse uniquement les objets considérés comme nouveaux ou modifiés depuis la dernière analyse du système de fichiers NTFS.

  Si la case est décochée, Kaspersky Embedded Systems Security analyse les objets du système de fichiers NTFS sans tenir compte de la date de création ou de modification.

  Cette case est cochée par défaut.

6. Cliquez sur le bouton **Enregistrer**.

Les paramètres de la tâche définis seront enregistrés.

Analyse des disques amovibles

Vous pouvez configurer l'analyse des disques amovibles connectés via USB à l'ordinateur protégé.

Kaspersky Embedded Systems Security analyse le disque amovible à l'aide de la tâche Analyse à la demande (cf. section « A propos des tâches d'analyse à la demande » à la page 241). 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 connectés via USB lors de l'enregistrement de ces derniers dans le système d'exploitation en guise de dispositif de stockage de masse (USB Mass Storage Device). 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 n'interdit pas l'accès au disque amovible pendant 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 de ce disque.

Vous pouvez modifier les valeurs des paramètres du composant Analyse des disques amovibles (cf. tableau ci-dessous).

Tableau 30. 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 des disques amovibles lors de leur connexion à l'ordinateur protégé.
Analyser si le volume des données sur le disque ne dépasse pas (Mo)	1024 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.
Lancer l'analyse selon 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**. Les algorithmes des actions à réaliser en cas de découverte d'objets infectés, probablement infectés ou autres ainsi que les autres paramètres d'analyse pour chaque niveau de sécurité correspondent aux niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande (cf. section « Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande » à la page 268).

► *Pour configurer les paramètres d'analyse des disques amovibles à la connexion, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Kaspersky Embedded Systems Security** et sélectionnez l'option **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.

2. Dans le groupe **Paramètres d'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 si le volume des données sur le disque ne dépasse pas (Mo)**) et définissez le seuil maximal dans le champ à droite.

   - Dans la liste déroulante **Lancer l'analyse selon le niveau de sécurité**, choisissez le niveau de sécurité selon lequel il faut lancer l'analyse des disques amovibles.

3. Cliquez sur **OK**.

   Les paramètres définis seront enregistrés et appliqués.

Création d'une tâche d'analyse à la demande

Vous pouvez créer des tâches définies par l'utilisateur dans le nœud **Analyse à la demande**. Les autres composants de Kaspersky Embedded Systems Security ne prévoient pas la création de tâches définies par l'utilisateur.

► *Pour créer une nouvelle tâche d'analyse à la demande, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Analyse à la demande**.

2. Choisissez l'option **Ajouter une tâche**.

   La fenêtre **Ajouter une tâche** s'ouvre.

3. Saisissez les informations suivantes relatives à la tâche :

   - **Nom** : nom de la tâche, 100 caractères maximum, peut contenir n'importe quel caractère sauf **% ? l \ | / : * < >**.

     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 complémentaire relative à la tâche, 2 000 caractères maximum. Ces informations figurent dans la fenêtre des propriétés de la tâche.

4. Le cas échéant, configurez les paramètres suivants de la tâche :

5. Sous l'onglet **Général** :

   - **Utiliser l'analyse heuristique**.

     La case active ou désactive l'utilisation de l'analyseur heuristique lors de l'analyse des objets.

     Quand la case est cochée, l'analyse heuristique est activée.

     Quand la case est décochée, l'analyse heuristique est désactivée.

     Cette case est cochée par défaut.

   - **Exécuter la tâche en arrière-plan**.

     La case modifie la priorité de la tâche.

     Quand la case est cochée, la priorité de la tâche dans le système d'exploitation diminue. Le système d'exploitation octroie les ressources nécessaires à l'exécution de la tâche en fonction de la charge exercée sur l'unité centrale et du système de fichiers du serveur par les autres tâches de Kaspersky Embedded Systems Security ou les autres applications. Par conséquente la vitesse d'exécution de la tâche diminuera quand la charge augmentera et augmentera dans le cas contraire.

     Si la case n'est pas cochée, la tâche est exécutée avec la même priorité que les autres tâches de Kaspersky Embedded Systems Security et les autres applications. Dans ce cas, la vitesse d'exécution de la tâche augmente.

     Cette case est décochée par défaut.

- **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 de fichiers des processus de confiance aux exclusions de l'analyse définies dans la configuration des paramètres de la tâche.

  Si la case est décochée, Kaspersky Embedded Systems Security ne prend pas en compte les opérations de fichiers des processus de confiance lors de la création de la zone de protection dans la tâche Protection des fichiers en temps réel.

  Cette case est cochée par défaut.

- **Considérer l'exécution de la tâche comme une analyse rapide**.

La case modifie la priorité de la tâche : active ou désactive l'enregistrement de l'événement *Analyse rapide réalisée* et l'actualisation de l'état de la protection de l'ordinateur. La case n'est pas accessible dans les propriétés des tâches locales de Kaspersky Embedded Systems Security système ou définies par l'utilisateur. Vous pouvez modifier la valeur de ce paramètre du côté de Kaspersky Security Center.

Quand la case est cochée, le Serveur d'administration consigne l'événement *Analyse rapide réalisée* et actualise l'état de la protection de l'ordinateur suite à l'exécution de la tâche. La priorité de la tâche d'analyse est élevée.

Si la case est décochée, la tâche d'analyse est exécutée selon une priorité faible.

La case est cochée par défaut pour la tâche Analyse rapide.

- **Utiliser KSN pour la protection**.

  La case active ou désactive l'utilisation des services cloud du Kaspersky Security Network (KSN) dans la tâche.

  Si la case est cochée, l'application utilise les données obtenues via les services du KSN afin d'augmenter sa vitesse de réaction face aux nouvelles menaces et de réduire la probabilité de faux-positifs.

  Si la case est décochée, la tâche de protection des fichiers en temps réel n'utilise pas les servies du KSN.

  Cette case est cochée par défaut.

- Sous les onglets **Planification** et **Avancé** :
  - Paramètres de lancement de la tâche selon la planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).
- Sous l'onglet **Exécuter en tant que** :
  - Paramètres du lancement de la tâche sous les autorisations d'un compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81).

6. Dans la fenêtre **Paramètres de la tâche**, cliquez sur **OK**.

   La tâche d'analyse à la demande définie par l'utilisateur a été créée. L'entrée portant le nom de la nouvelle tâche apparaîtra dans l'arborescence de la console. L'opération est enregistrée dans le journal d'audit système (cf. section « Journal d'audit système » à la page 338).

7. Le cas échéant, ouvrez l'onglet **Configuration de la zone d'analyse** dans le volet résultats de l'entrée sélectionnée.

   Exécutez les actions suivantes :

   - Dans l'arborescence des ressources fichier du serveur, sélectionnez les entrées que vous souhaitez inclure dans la zone d'analyse.
   - Sélectionnez l'un des niveaux de sécurité prédéfinis (cf. section « Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande » à la page 268) ou configurez manuellement les paramètres de protection des objets (cf. section « Configuration manuelle des paramètres de sécurité » à la page 272).

8. Dans le menu contextuel du nom de la tâche sélectionnée, sélectionnez **Enregistrer la tâche**.

La tâche d'analyse à la demande définie par l'utilisateur a été créée. Les paramètres configurés seront appliqués lors de la prochaine exécution de la tâche.

Suppression d'une tâche

Vous pouvez supprimer uniquement les tâches d'analyse à la demande définies par l'utilisateur dans la console de Kaspersky Embedded Systems Security. Vous ne pouvez pas supprimer les tâches système, ni les tâches de groupe.

► *Pour supprimer une tâche, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Ouvrez le menu contextuel du nom de la tâche définie par l'utilisateur que vous souhaitez supprimer.
3. Choisissez l'option **Supprimer la tâche**.

   La fenêtre de confirmation de la suppression s'ouvre.
4. Cliquez sur le bouton **Oui** pour confirmer la suppression.

La tâche sera supprimée et cette opération sera enregistrée dans le journal d'audit système.

Changement de nom d'une tâche

La console de Kaspersky Embedded Systems Security permet de renommer uniquement les tâches définies par l'utilisateur. Vous ne pouvez pas renommer les tâches système, ni les tâches de groupe.

► *Pour renommer une tâche, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, développez l'entrée **Analyse à la demande**.
2. Ouvrez le menu contextuel du nom de la tâche définie par l'utilisateur que vous souhaitez renommer.
3. Choisissez l'option **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Dans la fenêtre qui s'ouvre, saisissez le nouveau nom de la tâche dans le champ **Nom**.
5. Cliquez sur **OK**.

La tâche sera ainsi renommée. L'opération sera enregistrée dans le journal d'audit système.

Mise à jour des bases de données et des modules de Kaspersky Embedded Systems Security

Cette section présente les tâches de mises à jour des bases de données et des modules logiciels de Kaspersky Embedded Systems Security, la copie des mises à jour des bases 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 des bases de données et des modules de l'application.

Dans cette section

Présentation 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 serveurs de mise à jour de Kaspersky Lab, en définissant automatiquement les paramètres du serveur proxy dans le réseau et sans recourir à l'authentification lors de l'accès au serveur proxy.

Vous pouvez configurez toutes les tâches de mises à jour (cf. section « Configuration des tâches de mise à jour » à la page 297), à l'exception de 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 l'ordinateur protégé et les utilise directement dans la tâche Protection en temps réel en cours. Les tâches Analyse à la demande utiliseront les bases de l'application mises à jour à leur prochaine exécution.

Kaspersky Embedded Systems Security lance la tâche Mise à jour des bases de l'application toutes les heures par défaut.

Mise à jour des modules de l'application

Par défaut, Kaspersky Embedded Systems Security vérifier la présence des modules logiciels depuis la source des mises à jour sur l'ordinateur protégé. L'application des modules logiciels installés peut impliquer le redémarrage de l'ordinateur et / ou le relancement 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 16h00 (l'heure dépend des paramètres régionaux du serveur 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 copie pas.

Copie des mises à jour

Par défaut, lors de l'exécution de la tâche, Kaspersky Embedded Systems Security télécharge les fichiers des mises à jour des bases de données et des modules et les enregistre dans le répertoire de réseau ou local indiqué, sans les installer.

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.

Présentation de la mise à jour des modules de Kaspersky Embedded Systems Security

Kaspersky Lab peut diffuser des paquets de mise à jour des modules de Kaspersky Embedded Systems Security. Les mises à jour sont réparties entre les *mises à jour urgentes* (ou *critiques*) et 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 sont publiées sur les serveurs de mise à jour de Kaspersky Lab. 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 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Celles-ci peuvent être téléchargées depuis le site Web de Kaspersky Lab. Vous pouvez obtenir des informations sur la diffusion des mises à jour prévues de Kaspersky Embedded Systems Security à l'aide des tâches Mises à jour des modules de l'application.

Vous pouvez télécharger les mises à jour urgentes depuis Internet sur chaque ordinateur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez les mises à jour sans les installer avant de les diffuser sur les ordinateurs du réseau protégé. 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.

Présentation de la mise à jour des bases de données de Kaspersky Embedded Systems Security

Les bases de Kaspersky Embedded Systems Security sur l'ordinateur protégé sont très vite dépassées. Les experts en virus de Kaspersky Lab 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'ordinateur au minium, il est conseillé de réaliser une mise à jour régulière des bases de données.

Par défaut, si les bases 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 *Les bases de l'application sont dépassées* est déclenché. Si les bases restent deux semaines sans mises à jour, l'événement *Les bases de l'application sont fortement dépassées* est déclenché. Les informations relatives à l'actualité des bases sont affichées à l'entrée **Kaspersky Embedded Systems Security** de l'arborescence de la console (cf. « Consultation de l'état de la protection et des informations sur Kaspersky Embedded Systems Security » à la page 31) de l'arborescence de la console. Vous pouvez définir un nombre de jours différent avant le déclenchement de ces événements grâce aux paramètres généraux de Kaspersky Embedded

Systems Security et configurer les paramètres de notification de l'administrateur sur ces événements (cf. section « Configuration des notifications de l'administrateur et des utilisateurs » à la page 364).

Kaspersky Embedded Systems Security télécharge la mise à jour des bases de données et des modules de l'application depuis des serveurs FTP ou HTTP de mise à jour de Kaspersky Lab, depuis le serveur d'administration Kaspersky Security Center ou depuis d'autres sources de mises à jour.

Vous pouvez télécharger les mises à jour sur chaque ordinateur protégé ou choisir un ordinateur en guise d'intermédiaire où vous copierez la mise à jour avant de la diffuser sur les ordinateurs. Si vous utilisez Kaspersky Security Center pour l'administration centralisée de la protection des ordinateurs de l'entreprise, vous pouvez utiliser le serveur d'administration de Kaspersky Security Center en guise d'intermédiaire pour le chargement des mises à jour.

Vous pouvez lancer la tâche de mise à jour des bases de données manuellement ou selon une planification (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76). Kaspersky Embedded Systems Security lance la tâche Mise à jour des bases de l'application toutes les heures par défaut.

Si le chargement 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 installées. Si les bases de Kaspersky Embedded Systems Security sont endommagées, vous pouvez revenir à l'état antérieur à la mise à jour des bases de données installées (cf. section « Remise à l'état antérieur à la mise à jour des bases de données de Kaspersky Embedded Systems Security » à la page 306).

Schémas de mise à jour des bases de données et des modules des applications antivirus dans l'entreprise

Votre sélection de la source des mises à jour dans les tâches de mise à jour dépend du schéma de mise à jour des bases de données et des modules logiciels des applications antivirus que vous utilisez dans votre entreprise.

Vous pouvez actualiser les bases et les modules de Kaspersky Embedded Systems Security sur les ordinateurs protégés selon les schémas suivants :

- Télécharger les mises à jour directement depuis Internet sur chaque ordinateur protégé (schéma 1) ;
- Télécharger les mises à jour depuis Internet sur l'ordinateur intermédiaire et les diffuser sur les ordinateurs au départ de cet ordinateur.

  L'intermédiaire peut être n'importe quel ordinateur sur lequel une des applications suivantes est installée :

  - Kaspersky Embedded Systems Security (un des ordinateurs protégés) (schéma 2) ;
  - Serveur d'administration Kaspersky Security Center (schéma 3).

La mise à jour via un ordinateur intermédiaire permet non seulement de réduire le trafic Internet mais également d'offrir une sécurité supplémentaire aux ordinateurs du réseau.

Les différents schémas de mise à jour sont décrits ci-après.

Schéma 1. Mise à jour directement depuis Internet

► *Pour configurer la récupération des mises à jour de Kaspersky Embedded Systems Security directement depuis 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 ordinateur à protéger, désignez les serveurs de mise à jour de Kaspersky Lab en tant que sources des mises à jour.

En guise de source, vous pouvez indiquer d'autres serveurs HTTP ou FTP qui contiennent un répertoire avec les fichiers des mises à jour.

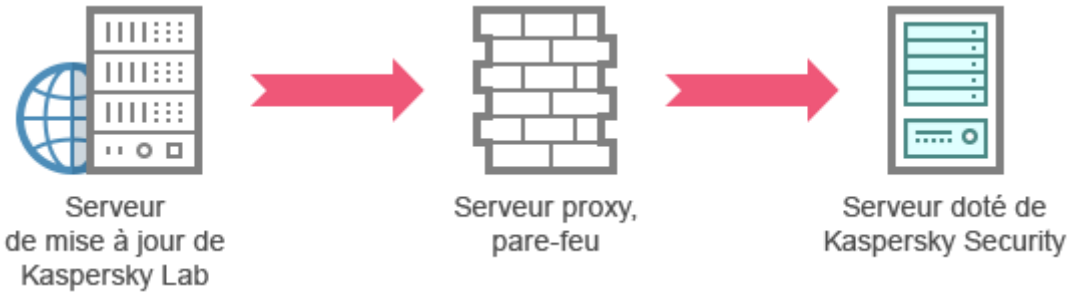

Illustration 1 : schéma de mise à jour des bases et des modules d'application

Schéma 2. Mise à jour via un des ordinateurs protégés

► *Pour configurer la récupération des mises à jour de Kaspersky Embedded Systems Security via un des ordinateurs à protéger, procédez comme suit :*

1. Copiez les mises à jour sur l'ordinateur protégé sélectionné. Pour ce faire, procédez comme suit :

   - Sur l'ordinateur sélectionné, configurez les paramètres de la tâche Copie des mises à jour :

     a. En guise de source des mises à jour, sélectionnez les ordinateurs de mise à jour de Kaspersky Lab.

     b. Désignez le dossier partagé en guise de dossier d'enregistrement des mises à jour.

2. Diffusez les mises à jour sur les autres ordinateurs protégés. Pour ce faire, procédez comme suit :

   - Sur chaque ordinateur protégé, configurez les paramètres de la tâche Mise à jour des bases de l'application ou 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'ordinateur intermédiaire dans lequel vous avez copié les mises à jour.

Kaspersky Embedded Systems Security récupèrera les mises à jour via un des ordinateurs à protéger.

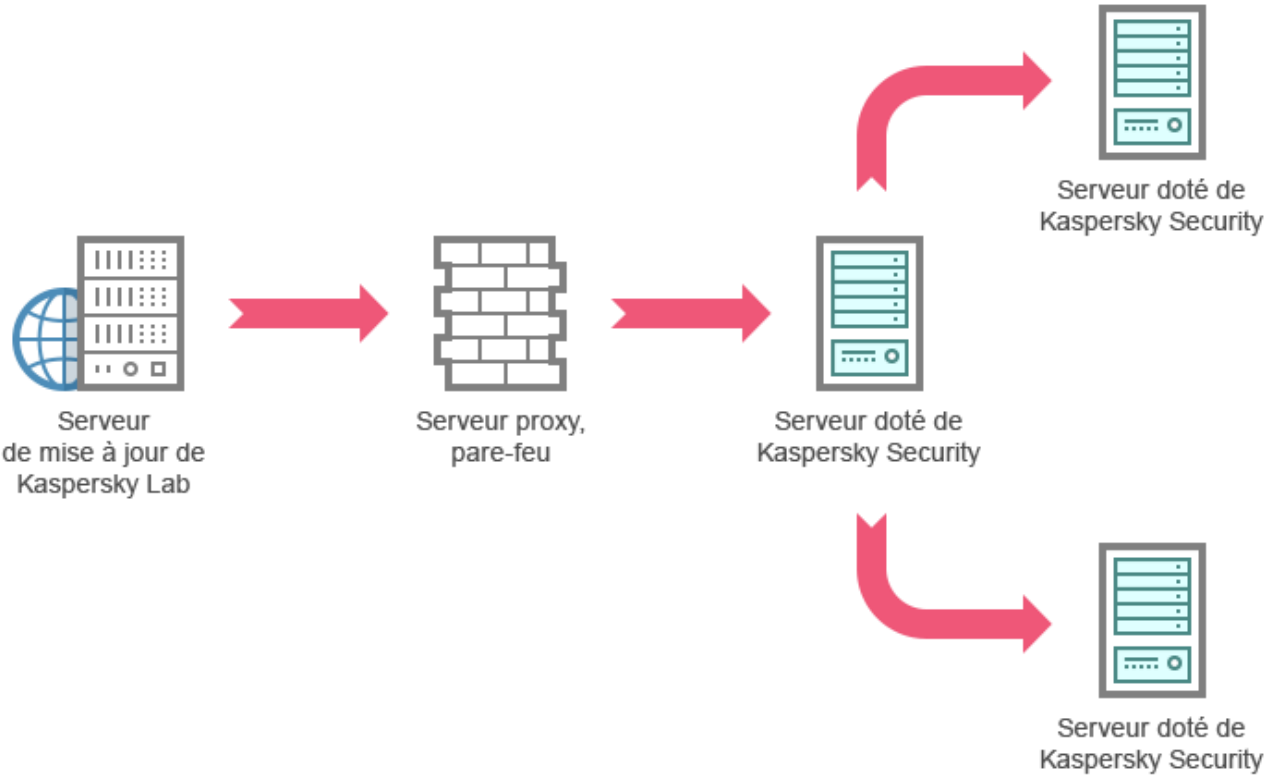

Figure 2: Mise à jour via un des serveurs protégés

Schéma 3. Réalisez la mise à jour via le serveur d'administration Kaspersky Security Center

Si vous utilisez l'application Kaspersky Security Center pour assurer l'administration centralisée de la protection de l'ordinateur, vous pouvez télécharger les mises à jour via le Serveur d'administration Kaspersky Security Center (cf. ill. ci-après).

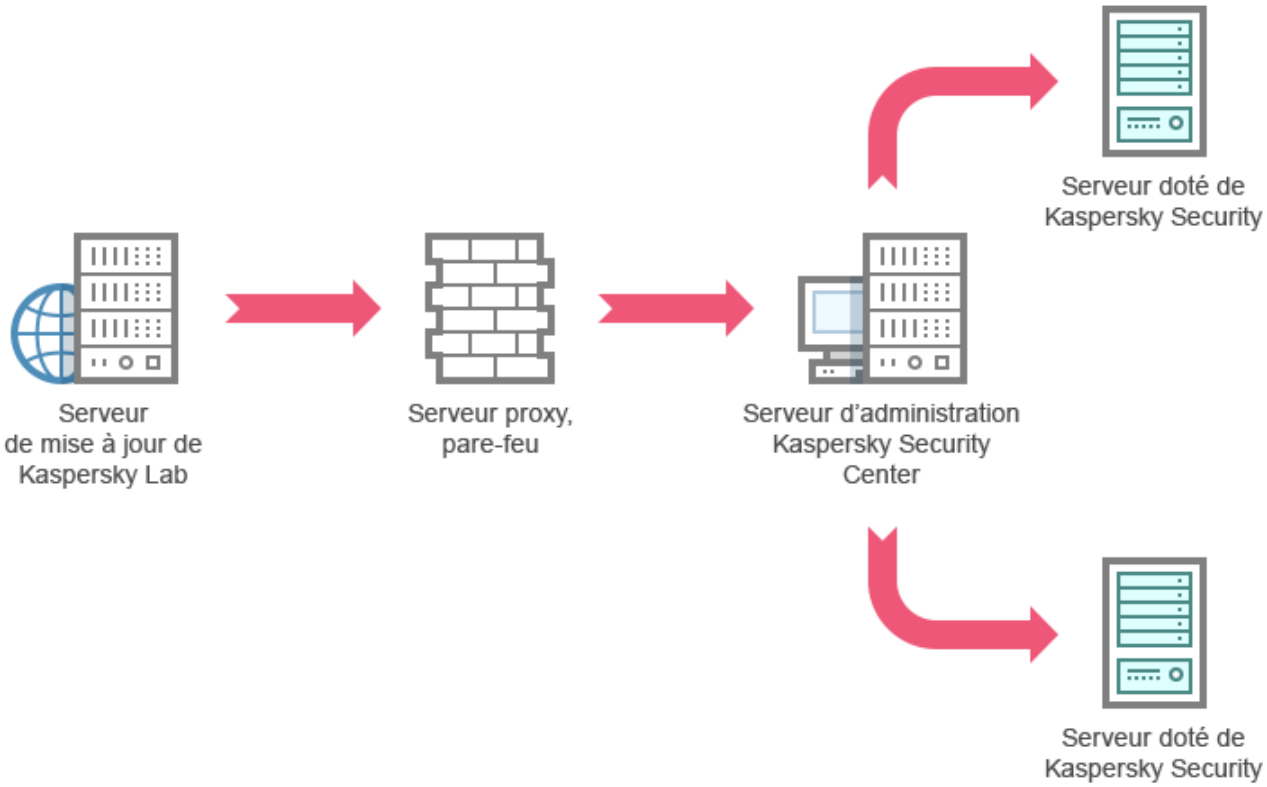

Figure 3 : mise à jour via le serveur d'administration Kaspersky Security Center

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 Lab 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'ordinateurs indiquée :
        a. En guise de source des mises à jour, sélectionnez les serveurs de mise à jour de Kaspersky Lab.

2. Diffusez les mises à jour sur les ordinateurs protégés. Pour ce faire, réalisez une des opérations suivantes :

   - Sur le serveur d'administration de Kaspersky Security Center, configurez une tâche de groupe de mise à jour pour la diffusion des mises à jour sur les serveurs protégés :

     a. Dans la programmation de la tâche, choisissez la fréquence **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 sélectionner la fréquence d'exécution **Après réception des mises à jour par le serveur d'administration** dans la console de Kaspersky Embedded Systems Security.

   - Configurez sur chaque ordinateur 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 récupèrera les mises à jour via le Serveur d'administration Kaspersky Security Center.

Si vous avez l'intention d'utiliser le serveur d'administration Kaspersky de Security Center pour la diffusion des mises à jour, installez au préalable sur chaque serveur protégé le module logiciel Agent d'administration qui fait partie du kit de distribution de l'application Kaspersky Security Center. Il assure l'interaction entre le serveur d'administration et Kaspersky Embedded Systems Security sur l'ordinateur protégé. Pour obtenir de plus amples informations sur l'agent

d'administration et sur sa configuration à l'aide de l'application Kaspersky Security Center, consultez le document *Manuel de l'administrateur 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.

Dans cette section

Configuration des paramètres d'utilisation des sources de mises 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 connexions 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 définir le type de source des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le volet résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
4. Dans le groupe **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**.

     Kaspersky Embedded Systems Security utilise le Serveur d'administration Kaspersky Security Center en tant que source de mise à jour.

     Cette option n'est disponible que si les applications de Kaspersky Lab de votre réseau sont gérées à partir du système d'administration à distance de Kaspersky Security Center et si l'Agent d'administration (composant de Kaspersky Security Center qui gère les connexions entre les ordinateurs et le serveur d'administration) est installé sur l'ordinateur sécurisé.
   - **Serveurs de mise à jour de Kaspersky Lab**.

     Kaspersky Embedded Systems Security utilise les sites Web de Kaspersky Lab comme source de mises à jour. Ces serveurs hébergent les mises à jour des bases de données et des modules de programme de tous les logiciels de Kaspersky Lab.

     Cette option est sélectionnée par défaut.
   - **Serveurs HTTP, FTP ou dossiers réseau personnalisés**.

     Kaspersky Embedded Systems Security utilise en guise de source de mises à jour les serveurs HTTP, FTP ou les dossiers des ordinateurs du réseau local désignés par l'administrateur.

     Vous pouvez composer la liste des sources qui contient la sélection la plus récente des mises à jour en cliquant sur le lien **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**.

        i. 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.

        ii. Cliquez sur **OK**.

    b. Dans le groupe **Source des mises à jour**, sous l'onglet **Général**, cochez ou décochez la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles**.

        La case active ou désactive la fonction d'utilisation des serveurs de mise à jour de Kaspersky Lab en guise de source des mises à jour si les sources que vous avez sélectionnées ne sont pas disponibles.

        Quand la case est cochée, la fonction est active.

        Cette case est cochée par défaut.

        Vous pouvez cocher la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles** quand l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** est sélectionnée.

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 :

    Exécutez les actions suivantes :

    - Décochez ou cochez la case **Utiliser le FTP en mode passif si possible**.

        La case active ou désactive la fonction qui permet de télécharger les mises à jour depuis des serveurs FTP en mode passif.

        Quand la case est cochée, la connexion est ouverte en mode passif.

        Quand la case est décochée, la connexion est ouverte en mode normal.

        Cette case est cochée par défaut.

    - Le cas échéant, définissez le délai d'attente (en secondes).

Dans le groupe **Paramètres de connexion avec les sources des mises à jour** :

- Cochez ou décochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux serveurs de mise à jour de Kaspersky Lab**.

  La case active ou désactive l'utilisation des paramètres du serveur proxy si la mise à jour s'opère depuis des serveurs de Kaspersky Lab ou si la case **Utiliser les serveurs de mise à jour de Kaspersky Lab si les serveurs ou le répertoire réseau ne sont pas accessibles** est cochée.

  Quand la case est cochée, les paramètres du serveur proxy sont utilisés.

  Quand la case est décochée, les paramètres du serveur proxy ne sont pas utilisés.

  Cette case est décochée par défaut.

- Cochez ou décochez la case **Utiliser les paramètres de proxy spécifiés pour se connecter aux autres serveurs**.

  La case active ou désactive l'utilisation des paramètres du serveur proxy si l'option **Serveurs HTTP, FTP ou dossiers réseau personnalisés** en tant que source des mises à jour.

  Quand la case est cochée, les paramètres du serveur proxy sont utilisés.

  Cette case est décochée par défaut.

7. Cliquez sur **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 Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.

2. Sélectionnez la sous-entrée qui correspond à la tâche de mise à jour que vous souhaitez configurer.
3. Dans le volet résultats de l'entrée sélectionnée, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
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 de mise à jour définie par l'utilisateur, saisissez dans la zone de saisie l'adresse du répertoire contenant les fichiers de mise à jour sur le serveur FTP ou HTTP ; saisissez le répertoire local ou de 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 des sources par Kaspersky Embedded Systems Security, 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 **OK**.

Les modifications introduites dans la liste des sources de mises à jour de l'application définies par l'utilisateur sont enregistrées.

Optimisation de l'utilisation du sous-système 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'ordinateur. Vous pouvez réduire la charge sur le sous-système disque de l'ordinateur 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.

► *Pour réduire la charge sur le sous-système disque de l'ordinateur lors de l'exécution de la tâche Mise à jour des bases de l'application, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée **mise à jour des bases de l'application**.
3. Dans le volet résultats de l'entrée **mise à jour des bases de l'application**, cliquez sur le lien **Propriétés**.
4. La fenêtre **Paramètres de la tâche**, sous l'onglet **Général**, s'ouvre.
5. Configurez les paramètres suivants dans le groupe **Optimisation de l'utilisation des I/O du disque** :
   - Cochez ou décochez la case **Réduire la charge sur les I/O du disque**.

     La case active ou désactive la fonction d'optimisation du sous-système disque grâce à un placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive.

     Quand la case est cochée, la fonction est active.

     Cette case est décochée par défaut.
   - Définissez le volume de mémoire vive en méga-octets dans le champ **Volume de mémoire vive utilisé pour l'optimisation**. 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.
6. Cliquez sur **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 Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée **Copie des mises à jour**.
3. Dans le volet résultats de l'entrée **Copie des mises à jour**, cliquez sur le lien **Propriétés**.

   La fenêtre **Paramètres de la tâche** s'ouvre.
4. Les onglets **Général** et **Configuration de connexion** permettent de configurer les paramètres d'utilisation des sources de mises à jour (cf. section « Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Embedded Systems Security » à la page 297).
5. Dans le groupe **Paramètres de copie des mises à jour** de l'onglet **Général**, procédez comme suit :
   - Définissez les conditions de copie des mises à jour de l'application :
     - **Copier les mises à jour de l'application**.

       Kaspersky Embedded Systems Security télécharge uniquement les mises à jour des bases de données de Kaspersky Embedded Systems Security.

       Cette option est sélectionnée par défaut.
     - **Copier les mises à jour critiques des modules de l'application**.

       Kaspersky Embedded Systems Security télécharge uniquement les mises à jour urgentes des modules de Kaspersky Embedded Systems Security.
     - **Copier les mises à jour des bases de l'application et les mises à jour critiques des modules de l'application**.

       Kaspersky Embedded Systems Security télécharge les mises à jour des bases de données et les mises à jour critiques des modules de Kaspersky Embedded Systems Security.
   - Indiquez le répertoire local ou de réseau dans lequel Kaspersky Embedded Systems Security copiera les mises à jour reçues.

6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76).

7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81).

8. Cliquez sur **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 Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.

2. Sélectionnez la sous-entrée **Mise à jour des modules de l'application**.

3. Dans le volet résultats de l'entrée **Mise à jour des modules de l'application**, cliquez sur le lien **Propriétés**.

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

4. Les onglets **Général** et **Configuration de connexion** permettent de configurer les paramètres d'utilisation des sources de mises à jour (cf. section « Configuration des paramètres d'utilisation des sources de mises à jour de Kaspersky Embedded Systems Security » à la page 297).

5. Dans le groupe **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 des mises à jour critiques des modules de l'application**.

     Kaspersky Embedded Systems Security signale la présence de mises à jour urgentes des modules de l'application sur la source sans les télécharger. La notification a lieu si la notification pour ce type d'événement a été configurée.

     Cette option est sélectionnée par défaut.

   - **Copier et installer les mises à jour critiques des modules de l'application**.

     Kaspersky Embedded Systems Security copie et installe les mises à jour critiques des modules de l'application.

   - **Autoriser le redémarrage de l'ordinateur**.

     Redémarrage du système d'exploitation après l'installation de mises à jour qui requièrent le redémarrage.

     Quand la case est cochée, Kaspersky Embedded Systems Security redémarre le système d'exploitation après l'installation des mises à jour qui requièrent le redémarrage.

     La case est active si l'option **Copier et installer les mises à jour critiques des modules de l'application** a été sélectionnée.

     Cette case est décochée par défaut.

   - **Recevoir des informations sur les mises à jour des modules de l'application prévues**.

     Réception des notifications sur toutes les mises à jour des modules de Kaspersky Embedded Systems Security prévues disponibles sur la source. Kaspersky Embedded Systems Security envoie les notifications si les notifications de ce type d'événement ont été configurées.

     Quand la case est cochée, Kaspersky Embedded Systems Security envoie les notifications relatives à toutes les mises à jour prévues des modules de l'application disponibles sur la source.

     Cette case est cochée par défaut.

6. Les onglets **Planification** et **Avancé** permettent de planifier le lancement de la tâche (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76). Par défaut, Kaspersky Embedded Systems Security lance la tâche Mise à jour des modules de l'application chaque semaine, le vendredi à 16h00 (l'heure dépend des paramètres régionaux du serveur protégé).
7. L'onglet **Exécuter en tant que** permet de configurer le lancement de la tâche sous les autorisations d'un autre compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81).
8. Cliquez sur **OK**.

Les paramètres configurés seront enregistrés et appliqués au prochain lancement de la tâche.

Kaspersky Lab ne publie pas les mises à jour prévues sur les serveurs de mises à jour pour la mise à jour automatique. Vous pouvez les télécharger depuis le site Web de Kaspersky Lab. Vous pouvez configurer une notification de l'administrateur pour l'événement *Une mise à jour prévue des modules de l'application est disponible*. Celle-ci reprendra l'adresse de la page du site d'où les mises à jour prévues peuvent être téléchargées.

Annulation de la mise à jour des bases de données de Kaspersky Embedded Systems Security

Avant d'appliquer 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 mises à jour 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 Retour à l'état antérieur à la mise à jour des bases.

► *Pour lancer la tâche Annulation de la mise à jour des bases de données,*

cliquez sur le lien **Démarrer** dans le volet résultats du volet **Annulation de la mise à jour des bases de l'application**.

Remise à l'état antérieur à la mise à jour des modules logiciels

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

Avant d'appliquer la mise à jour des modules logiciels, Kaspersky Embedded Systems Security crée une copie de sauvegarde des modules utilisés actuellement. Si la mise à jour des modules est interrompue ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des derniers modules actualisés installés.

Pour revenir à l'état antérieur des modules logiciels, utilisez le composant **Ajout/suppression de programme** du panneau de configuration de Microsoft Windows.

Statistiques sur les tâches de mise à jour

Tandis que la tâche de mise à jour est exécutée, vous pouvez consulter les informations en temps réel relatives aux données reçues depuis le lancement de la tâche jusqu'à maintenant.

Après l'arrêt ou la suspension de la tâche, vous pouvez consulter les informations dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches » à la page 345).

► *Pour consulter les statistiques de la tâche de mise à jour, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Mise à jour**.
2. Sélectionnez la sous-entrée qui correspond à la tâche dont vous souhaitez consulter les statistiques.

Le volet résultats de l'entrée sélectionnée reprend les statistiques de la tâche dans le groupe **Statistiques**.

Si vous consultez la tâche Mise à jour des bases de l'application ou la tâche Copie des mises à jour, le groupe **Statistiques** affiche le volume de données téléchargées par Kaspersky Embedded Systems Security en ce moment (**Données récupérées**).

Si vous consultez la tâche Mise à jour des modules de l'application, vous verrez les informations décrites dans le tableau ci-dessous.

Tableau 31. Informations sur la tâche Mise à jour des modules de l'application

Champ	Description
Données récupérées	Volume totale 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. Vous pouvez consulter le nom de la mise à jour pendant laquelle l'erreur s'est produite dans le journal d'exécution de la tâche (cf. section « Consultation des statistiques et informations relatives à la tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches » à la page 345).

L'isolement et les sauvegardes des objets

Cette section contient des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression. Elle fournit également des instructions sur l'isolement des fichiers probablement infectés.

Dans cette section

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 de la quarantaine.

Dans cette section

À propos de l'isolement 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 la *quarantaine*. Pour des raisons de sécurité, une fois en quarantaine, les objets sont chiffrés.

Consultation des objets en quarantaine

Vous pouvez consulter les objets en quarantaine dans le nœud **Quarantaine** de la console de Kaspersky Embedded Systems Security.

► *Pour consulter les objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.

2. Sélectionnez la sous-entrée **Quarantaine**.

Les informations relatives aux objets placés en quarantaine apparaissent dans le volet résultats de l'entrée sélectionnée.

► *Pour trouver l'objet requis dans la liste des objets en quarantaine,*

Triez les objets (cf. section « Tri des objets en quarantaine » à la page 311) ou filtrez-les (cf. section « Filtrage des objets en quarantaine » à la page 312).

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 souhaité, vous pouvez trier la liste selon le contenu des colonnes reprenant les informations sur les objets. Les résultats du tri sont préservés si vous fermez et ouvrez à nouveau l'entrée **Quarantaine**, ou si vous fermez la console Kaspersky Embedded Systems Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour trier les objets, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.

2. Sélectionnez la sous-entrée **Quarantaine**.

3. Dans le volet résultats de l'entrée **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 souhaité en quarantaine, vous pouvez filtrer les objets de la liste et 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 Kaspersky Embedded Systems Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour définir un ou plusieurs filtres, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Dans le menu contextuel du nom de l'entrée, sélectionnez l'option **Filtre**.

   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 pour la comparaison avec la valeur du filtre.

   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 a à d pour chaque filtre que vous souhaitez ajouter. Lors de la configuration de filtres, observez les règles 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**.
- 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.**

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 dans la liste des objets en quarantaine,* sélectionnez l'option **Supprimer le filtre** dans le menu contextuel de l'entrée **Quarantaine**.

Analyse des objets en quarantaine

Par défaut, Kaspersky Embedded Systems Security exécute la tâche système Analyse des objets en quarantaine après chaque mise à jour des bases de données. Les paramètres de la tâche sont présentés dans le tableau ci-après. Vous ne pouvez pas modifier les paramètres de la tâche Analyse des objets en quarantaine.

Vous pouvez planifier le lancement de la tâche (cf. section « Configuration des paramètres de la planification du lancement des tâches » à la page 76), la lancer manuellement et modifier les autorisations du compte (cf. section « Définition du compte utilisateur pour l'exécution de la tâche » à la page 81) sous lequel la tâche est lancée.

Suite à l'analyse des objets en quarantaine après la mise à jour des bases de données, Kaspersky Embedded Systems Security peut décider que certains d'entre eux sont sains : l'état de ces objets devient alors **Fausse alerte**. D'autres objets peuvent être considérés comme infectés par Kaspersky Embedded Systems Security, auquel cas il exécutera les actions définies dans les paramètres de la tâche d'analyse à la demande Analyse des objets en quarantaine : désinfecter, supprimer si la désinfection est impossible.

Tableau 32. Paramètres de la tâche Analyse des objets en quarantaine

Paramètre de la tâche Analyse des objets en quarantaine	Valeur
Zone d'analyse	Dossier de quarantaine
Paramètres de sécurité	Identiques pour toutes les zones d'analyse ; les valeurs possibles sont reprises au tableau suivant.

Tableau 33. Paramètres de sécurité de la tâche Analyse des objets en quarantaine

Paramètre de sécurité	Valeur
Analyse des objets	Tous les objets de la zone d'analyse
Optimisation	Désactivée
Action à exécuter sur les objets infectés et autres détectés	Désinfecter, supprimer si la désinfection est impossible
Action à exécuter sur les objets probablement infectés	Rapport uniquement
Exclure les objets	Non
Ne pas détecter	Non
Arrêter si l'analyse dure plus de (s.)	Non définie
Ne pas analyser les objets composés de plus de (Mo)	Non définie
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

Paramètre de sécurité	Valeur
Analyse des objets composés	• Archives* • Archives SFX* • Objets compactés* • Objets OLE intégrés* * L'analyse uniquement des nouveaux fichiers et des fichiers modifiés est désactivée.
Vérification de la signature Microsoft des fichiers	Non exécutée
Utiliser l'analyse heuristique	Appliqué au niveau d'analyse **Minutieuse**
Zone de confiance (cf. page 62)	Pas appliqué

Restauration d'un objet depuis la quarantaine

Kaspersky Embedded Systems Security place les objets probablement infectés sous une forme cryptée dans le répertoire de quarantaine afin de protéger l'ordinateur 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 est devenu **Fausse alerte** ou **Désinfecté** ;
- Vous estimez que l'objet ne présente aucun danger pour l'ordinateur 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 comme valeur du paramètre de sécurité **Exclure les objets** (selon le nom du fichier) ou **Ne pas détecter** dans ces tâches ou ajoutez-le à la zone de confiance (cf. section « Configuration de la zone de confiance » à page 62).

Lors de la restauration des objets, vous pouvez sélectionner l'endroit où sera placé l'objet : dans l'emplacement d'origine (défini par défaut), dans un dossier de restauration spécial sur l'ordinateur protégé, dans un répertoire désigné de l'ordinateur où est installée la console de Kaspersky Embedded Systems Security, ou sur un autre ordinateur du réseau.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur 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'ordinateur.

Vous pouvez restaurer l'objet en conservant une copie dans le répertoire de 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 fait 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 répertoire 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 Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Quarantaine**.
3. Dans le volet résultats de l'entrée **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**, puis ouvrez le menu contextuel d'un des objets sélectionnés et sélectionnez la commande **Restaurer**.

   La fenêtre **Restauration de l'objet** s'ouvre.

4. Dans la fenêtre **Restauration de l'objet**, indiquez pour chaque objet sélectionné le répertoire dans lequel vous souhaitez conserver la copie restaurée (le nom de l'objet figure dans le champ **Objet** de la partie supérieure de la fenêtre ; si vous avez sélectionné plusieurs objets, ce champ reprend le nom du premier objet de la liste de sélection).

   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 l'objet dans le répertoire que vous avez défini en tant que répertoire de restauration dans les paramètres de la quarantaine, sélectionnez **Restaurer dans le dossier par défaut** ;
   - Pour restaurer l'objet dans un autre répertoire de l'ordinateur où vous avez installé la console de Kaspersky Embedded Systems Security ou dans un répertoire de réseau, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis sélectionnez le répertoire souhaité ou saisissez le chemin d'accès à celui-ci.

5. Si vous souhaitez conserver une copie de l'objet dans le dossier de quarantaine après la restauration, désélectionnez la case **Supprimer les objets des stockages après leur restauration**.

6. 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 seront restaurés et enregistrés à l'emplacement que vous aurez désigné : 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 spécifié ou de la ressource réseau**, tous les objets seront enregistrés dans le dossier indiqué.

7. Cliquez sur **OK**.

   Kaspersky Embedded Systems Security commence par restaurer le premier des objets que vous avez sélectionnés.

8. 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. Choisissez l'une des actions suivantes pour Kaspersky Embedded Systems Security :

    - **Remplacer** afin d'enregistrer l'objet restauré au lieu du fichier existant ;
    - **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet 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 avez sélectionné plusieurs objets pour la restauration, alors pour appliquer l'action **Remplacer** ou **Renommer** à tous les objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).

    c. Cliquez sur **OK**.

    L'objet sera restauré ; les informations relatives à la restauration seront enregistrées 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**, alors la fenêtre **Restauration de l'objet** s'ouvrira 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, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel du nom de l'entrée **Quarantaine**.
2. Choisissez l'option **Ajouter**.
3. Dans la fenêtre **Ouvrir**, sélectionnez le fichier que vous souhaitez placer en quarantaine.
4. Cliquez sur **OK**.

    Kaspersky Embedded Systems Security place le fichier indiqué en quarantaine.

Suppression des objets de la quarantaine

Conformément aux paramètres de la tâche **Analyse des objets en quarantaine** (cf. page 313), Kaspersky Embedded Systems Security supprime automatiquement du répertoire de quarantaine les objets dont l'état est devenu *Infecté ou détecté* suite à l'analyse à l'aide des bases actualisées et que Kaspersky Embedded Systems Security n'a pu désinfecter. Kaspersky Embedded Systems Security ne supprime pas les autres objets.

Vous pouvez supprimer manuellement un ou plusieurs objets de la quarantaine.

► *Pour supprimer un ou plusieurs objets de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **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 Lab pour examen

Si le comportement d'un objet quelconque 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'un nouveau virus inconnu dont la description n'a pas encore été ajoutée à la base. Vous pouvez envoyer ce fichier à Kaspersky Lab pour examen. Les experts antivirus de Kaspersky Lab analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de désinfection aux bases. Il se peut que lors d'une analyse

ultérieure après la mise à jour des bases de données que Kaspersky Embedded Systems Security le considère comme un fichier infecté et parvienne à le désinfecter. 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 transfert, ils ne seront pas supprimés par le logiciel antivirus installé sur le serveur de messagerie.

Vous ne pouvez pas envoyer un objet de la quarantaine à Kaspersky Lab une fois que la licence n'est plus valide.

► *Pour envoyer un fichier à Kaspersky Lab pour examen, procédez comme suit :*

1. Si le fichier ne se trouve pas encore en quarantaine, placez-le à titre préventif (cf. page 318).

2. Dans le nœud **Quarantaine**, dans la liste des objets en quarantaine, ouvrez le menu contextuel du fichier que vous souhaitez envoyer à Kaspersky Lab 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 le poste où la console de Kaspersky Embedded Systems Security est installée, un nouveau message électronique sera créé. Lisez-le puis cliquez sur le bouton **Envoyer**.

   Le champ **Destinataire** du message contient l'adresse email de Kaspersky Lab 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 Lab 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. Il contient le fichier <uuid>.klq avec l'objet crypté (où uuid est l'identificateur unique de l'objet dans Kaspersky Embedded Systems Security), le fichier <uuid>.txt avec les informations obtenues par Kaspersky Embedded Systems Security sur l'objet et le fichier Sysinfo.txt qui contient les

informations relatives à Kaspersky Embedded Systems Security et au système d'exploitation de l'ordinateur :

- Nom et version du système d'exploitation ;
- Le nom et la version Kaspersky Embedded Systems Security ;
- Date de publication des dernières mises à jour des bases de données installées ;
- Numéro de la clé active.

Ces informations sont indispensables aux experts de Kaspersky Lab 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'ordinateur où se trouve la console de Kaspersky Embedded Systems Security, l'application propose d'enregistrer l'objet chiffré sélectionné dans un fichier. Ce fichier peut être envoyé seul à Kaspersky Lab.

► *Pour enregistrer l'objet crypté dans un fichier, procédez comme suit :*

1. Dans la fenêtre qui vous invite à enregistrer l'objet, cliquez sur le bouton **Oui**.
2. Sélectionnez le répertoire sur le disque de l'ordinateur 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 nouvelles valeurs des paramètres de la quarantaine sont appliquées directement après l'enregistrement.

► *Pour configurer les paramètres de la quarantaine, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Ouvrez le menu contextuel du nom de la sous-entrée **Quarantaine**.

3. Choisissez l'option **Propriétés**.

4. Dans fenêtre **Paramètres du stockage**, configurez les paramètres requis de la quarantaine en fonction de vos besoins :

   Dans le groupe **Paramètres de quarantaine** :

   - **Dossier de quarantaine**.

     Chemin d'accès au dossier de la quarantaine au format UNC (Universal Naming Convention).

     Le chemin par défaut est C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.0\Quarantine\.

   - **Taille maximale de la quarantaine**.

     La case active ou désactive la fonction qui surveille le volume total des objets placés en quarantaine. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Embedded Systems Security consigne l'événement *Dépassement de la taille maximum de la quarantaine* et une notification est générée conformément aux paramètres pour ce type d'événement.

     Quand la case est cochée, Kaspersky Embedded Systems Security surveille le volume total des objets placés dans la quarantaine.

     Si la case est décochée, Kaspersky Embedded Systems Security ne surveille pas le volume total des objets placés en quarantaine.

     Cette case est décochée par défaut.

   - **Seuil d'espace disponible**.

     La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est en dessous de ce seuil, Kaspersky Embedded Systems Security consigne l'événement *Seuil d'espace libre disponible dans la sauvegarde dépassé* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

     Si la case est cochée, Kaspersky Embedded Systems Security surveille le volume d'espace disponible dans la sauvegarde.

La case **Seuil d'espace disponible (Mo)** est active si la case **Taille maximale de sauvegarde (Mo)** a été cochée.

Cette case est cochée par défaut.

> 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 le groupe **Paramètres de restauration** :

- **Dossier dans lequel sont rétablis les objets**.

  Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

  On installe par défaut le chemin C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\1.1\Restored\.

5. Cliquez sur **OK**.

Les paramètres de la quarantaine définis 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 nom de l'entrée **Quarantaine** de l'arborescence de la console de Kaspersky Embedded Systems Security.*

La fenêtre **Statistiques** reprend les informations sur le nombre d'objets en quarantaine à l'heure actuelle (cf. tableau ci-dessous) :

Informations sur les objets en quarantaine dans la fenêtre Statistiques de quarantaine

Champ	Description
Objets probablement infectés	Nombre d'objets considérés comme probablement infectés par Kaspersky Embedded Systems Security.
Espace de quarantaine utilisé	Volume général de données dans le dossier de quarantaine.
Faux positifs	Nombre d'objets qui ont reçu l'état *Fausse alerte* car l'analyse de la quarantaine à l'aide des bases actualisées a indiqué ces objets comme étant sains.
Objets désinfectés	Nombre d'objets qui ont reçu l'état *Réparé* 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.

Dans cette section

A propos de la copie de sauvegarde des objets avant la désinfection ou la suppression

Kaspersky Embedded Systems Security enregistre une copie chiffrée des objets dont le statut est *Infecté ou détecté* et *Probablement infecté* dans la *Sauvegarde* avant de procéder à la désinfection ou à la suppression de ces objets.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Embedded Systems Security enregistre cet objet composé dans la sauvegarde. Par exemple, si Kaspersky Embedded Systems Security considère un des objets de la base de messagerie comme étant suspect, il place en sauvegarde l'ensemble de la base de messagerie.

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 de l'ordinateur peut être réduit.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur l'ordinateur protégé ou sur un autre ordinateur du réseau local de l'organisation. Vous pouvez restaurer le fichier du dossier de sauvegarde si, par exemple, le fichier original infecté ou probablement infecté contenait des informations cruciales et que lors de la désinfection, Kaspersky Embedded Systems Security n'a pas réussi à le préserver, ce qui a rendu les informations qu'il contenait inaccessibles.

La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Consultation des objets dans la sauvegarde

Vous pouvez consulter les objets du dossier de sauvegarde uniquement via la console de Kaspersky Embedded Systems Security dans 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 Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.

   Les informations relatives aux objets placés dans la sauvegarde apparaissent dans le volet résultats de l'entrée sélectionnée.

► *Pour trouver l'objet requis dans la liste des objets de la Sauvegarde, triez les objets ou filtrez-les.*

Dans cette section

Tri des fichiers de la Sauvegarde

Par défaut, les fichiers de la Sauvegarde sont classés par date d'enregistrement 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 tri sont préservés si vous quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Embedded Systems Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Dans la liste des fichiers de la Sauvegarde, sélectionnez l'en-tête de la colonne selon le contenu de 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 qu'il vous faut 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 quittez l'écran et ouvrez à nouveau le nœud **Sauvegarde**, ou si vous fermez la console de Kaspersky Embedded Systems Security en l'enregistrant dans un fichier msc et que vous ouvrez à nouveau ce fichier.

► *Pour trier les fichiers dans le dossier de sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Sauvegarde** et choisissez l'option **Filtre**.

   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 dont la valeur sera comparée à la valeur du filtre.

   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.

   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 souhaitez ajouter. Lors de la configuration de filtres, vous pouvez observer les règles 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**.
   - 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 de l'entrée **Sauvegarde**.

Restauration des fichiers depuis la sauvegarde

Kaspersky Embedded Systems Security place les fichiers sous une forme cryptée dans la Sauvegarde afin de protéger l'ordinateur 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, qui était infecté, contenait des informations importantes et que Kaspersky Embedded Systems Security n'a pas pu préserver son intégrité lors de la désinfection, ce qui a rendu les informations du fichier inaccessibles ;
- Vous estimez que le fichier ne présente aucun danger pour l'ordinateur 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 d'analyse à la demande. Pour ce faire désignez le fichier en tant que valeur du paramètre **Exclure les objets** ou du paramètre **Ne pas détecter** de ces tâches.

  La restauration de fichiers du dossier de sauvegarde peut entraîner l'infection de l'ordinateur.

Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement où le fichier restauré sera conservé : dans le répertoire d'origine (par défaut), dans un dossier spécial de restauration sur l'ordinateur protégé ou dans un autre dossier indiqué sur l'ordinateur où la console de Kaspersky Embedded Systems Security est installée ou sur un autre ordinateur du réseau.

Le dossier Restaurer dans le dossier est prévu pour accueillir les objets restaurés sur le serveur protégé. Vous pouvez définir une analyse spéciale pour celui-ci dans les paramètres de sécurité. Le chemin d'accès au dossier est défini dans les paramètres de la Sauvegarde (cf. section « Configuration des paramètres de la Sauvegarde » à la page 333).

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 des fichiers depuis la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Exécutez une des actions suivantes :
   - Pour restaurer un fichier, ouvrez le menu contextuel du fichier, dans la liste des fichiers de la Sauvegarde, que vous souhaitez restaurer et sélectionnez l'option **Restaurer**.
   - Pour restaurer plusieurs fichiers, sélectionnez les fichiers souhaités dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez l'option **Restaurer**.
4. Dans la fenêtre **Restauration de l'objet**, spécifiez le répertoire dans lequel le fichier restauré sera enregistré.

   Le nom du fichier apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous avez sélectionné plusieurs objets, dans ce champ est le nom du premier de la liste qui est affiché.

   Exécutez une des actions suivantes :

   - Pour enregistrer le fichier restauré sur l'ordinateur protégé, sélectionnez une des options suivantes :
     - **Restaurer dans le dossier d'origine**, si vous souhaitez restaurer le fichier dans le dossier d'origine.
     - **Restaurer dans le dossier par défaut**, si vous souhaitez restaurer le fichier dans le dossier que vous avez désigné en guise de dossier pour la restauration dans les paramètres de la Sauvegarde.
   - Pour enregistrer le fichier restauré dans un autre répertoire, sélectionnez **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, puis

sélectionnez le répertoire souhaité (sur l'ordinateur où est installée la console de Kaspersky Embedded Systems Security ou dans un répertoire de réseau) ou saisissez le chemin d'accès à celui-ci.

5. 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).

6. Si vous avez sélectionné plusieurs fichiers pour la restauration, alors pour appliquer les conditions de conservation définies aux autres fichiers sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

   Tous les fichiers sélectionnés seront restaurés et enregistrés dans le dossier que vous aurez désigné : si vous avez sélectionné l'option **Restaurer dans le dossier d'origine**, chacun des fichiers sera enregistré dans son dossier d'origine ; si vous avez sélectionné **Restaurer dans le dossier par défaut** ou **Restaurer dans le dossier de l'ordinateur spécifié ou de la ressource réseau**, tous les fichiers seront conservés dans le répertoire spécifié.

7. Cliquez sur **OK**.

   Kaspersky Embedded Systems Security commence par restaurer le premier des fichiers que vous avez sélectionnés.

   Si un fichier portant le même nom existe déjà dans le répertoire indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

8. Exécutez les actions suivantes :

   a. Sélectionnez une des conditions suivantes de conservation du fichier restauré :

   - **Remplacer** afin d'enregistrer le fichier restauré au lieu du fichier existant.
   - **Renommer** afin d'enregistrer le fichier restauré sous un autre nom. Saisissez le nouveau nom du fichier et son chemin d'accès complet dans le champ
   - **Renommer en ajoutant un suffixe** afin de renommer le fichier en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

   b. Si vous souhaitez appliquer l'action **Remplacer** ou **Renommer** en ajoutant un suffixe aux fichiers restants, cochez la case **Appliquer à tous les objets**.

Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets** ne sera pas accessible.

c. Cliquez sur **OK**.

Le fichier sera restauré. Les informations relatives à la restauration seront enregistrées dans le journal d'audit système.

Si vous n'avez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration de l'objet**, alors la fenêtre **Restauration de l'objet** s'ouvrira à nouveau. Vous pouvez y indiquer le répertoire dans lequel le prochain fichier de la sélection sera enregistré après la restauration (cf. étape 4 des présentes instructions).

Suppression des fichiers de la Sauvegarde

► *Pour supprimer un ou plusieurs fichiers de la Sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Sélectionnez la sous-entrée **Sauvegarde**.
3. Exécutez une des actions suivantes :
   - Pour supprimer un fichier, ouvrez le menu contextuel du fichier que vous souhaitez supprimer et sélectionnez la commande **Supprimer** ;
   - Pour supprimer plusieurs objets, sélectionnez les objets souhaités dans la liste à l'aide de la touche **Ctrl** ou **Maj**, puis ouvrez le menu contextuel d'un des fichiers sélectionnés et sélectionnez la commande **Supprimer**.
4. Dans la fenêtre **Confirmation**, 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, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Stockages**.
2. Ouvrez le menu contextuel du nom de la sous-entrée **Sauvegarde**.
3. Choisissez l'option **Propriétés**.
4. Dans fenêtre **Paramètres du stockage**, configurez les paramètres requis de la Sauvegarde en fonction de vos besoins :

   Dans le groupe **Paramètres de la Sauvegarde** :

   - **Dossier de sauvegarde**.

     Chemin d'accès à la sauvegarde au format UNC (Universal Naming Convention).

     Le chemin défini par défaut C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\1.1\Backup\.

   - **Taille maximale de sauvegarde (Mo)**.

     La case active ou désactive la fonction qui surveille le volume total des objets placés dans la sauvegarde. En cas de dépassement de cette valeur (fixée par défaut à 200 Mo), Kaspersky Embedded Systems Security consigne l'événement *Dépassement de la taille maximale de sauvegarde* et une notification est générée conformément aux paramètres pour ce type d'événement.

     Quand la case est cochée, Kaspersky Embedded Systems Security surveille le volume total des objets placés dans la sauvegarde.

     Cette case est décochée par défaut.

- **Seuil d'espace disponible (Mo)**.

  La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (50 Mo par défaut). Si l'espace libre est en dessous de ce seuil, Kaspersky Embedded Systems Security consigne l'événement *Seuil d'espace libre disponible dans la sauvegarde dépassé* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement.

  Si la case est cochée, Kaspersky Embedded Systems Security surveille le volume d'espace disponible dans la sauvegarde.

  La case **Seuil d'espace disponible (Mo)** est active si la case **Taille maximale de sauvegarde (Mo)** a été cochée.

  Cette case est cochée par défaut.

> 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 le groupe **Paramètres de restauration** :

- **Dossier dans lequel sont rétablis les objets**.

  Chemin d'accès au dossier dans lequel sont rétablis les objets au format UNC (Universal Naming Convention).

  On installe par défaut le chemin C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\1.1\Restored\.

5. Cliquez sur **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, 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).

Tableau 34. Informations sur l'état de la Sauvegarde

Champ	Description
Taille actuelle de la Sauvegarde	Volume de données dans la sauvegarde ; tient compte de la taille des fichiers chiffrés
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde

Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security

Cette section contient des informations sur l'utilisation des journaux de Kaspersky Embedded Systems Security : journal d'audit système, journaux d'exécution des tâches de Kaspersky Embedded Systems Security et journal des événements de Kaspersky Embedded Systems Security.

Dans cette section

Modes 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 d'une application, création ou suppression de tâches, exécution de tâches, modification des paramètres d'une tâche.

Kaspersky Embedded Systems Security utilise les méthodes suivantes pour enregistrer les événements :

- **Journaux d'exécution des tâches**. 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.
- **Journal des événements de sécurité**. Le journal des événements de la sécurité contient les informations relatives aux événements liées aux violations de la sécurité ou aux tentatives de violation de la sécurité sur l'ordinateur 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) et que vous souhaitez diagnostiquer le problème, vous pouvez créer un fichier de trace et un fichier dump de la mémoire des processus de Kaspersky Embedded Systems Security et envoyer ces fichiers avec ces informations au Support Technique de Kaspersky Lab pour analyse.

Kaspersky Embedded Systems Security consigne les informations dans les fichiers de trace et le fichier dump de mémoire en clair.

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 d'analyse à la demande. Les enregistrements de ces événements apparaissent dans le volet résultats après la sélection du nœud **Journal d'audit système** dans la console de Kaspersky Embedded Systems Security.

Par défaut, Kaspersky Embedded Systems Security conservera les entrées du journal d'audit système pendant une durée indéterminée. Vous pouvez instaurer une limite pour la durée de conservation des enregistrements dans le journal d'audit système.

Vous pouvez désigner le dossier dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers journal d'audit système, différent du dossier choisi par défaut.

Dans cette section

Tri des événements dans le journal d'audit système

Par défaut, les événements sont classés dans le 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 **Evénement**.

► *Pour trier les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journal d'audit système**.
3. Dans le volet résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les événements de la liste.

Le résultat du tri est conservé jusqu'à prochaine consultation du journal d'audit système.

Filtrage des événements dans le journal d'audit système

Si vous le souhaitez, vous pouvez afficher dans le journal d'audit système uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage que vous définissez (filtres).

► *Pour filtrer les événements dans le journal d'audit système, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.

3. Pour ajouter un filtre, procédez comme suit :

    a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez 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 à l'aide de l'opérateur logique « ET », sélectionnez l'option **Quand toutes les conditions sont remplies**.
    - Afin de réunir quelques filtres à l'aide de l'opérateur logique « OU », 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 alors uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusqu'à prochaine consultation du journal d'audit système.

► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.

2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **Supprimer le filtre**.

    La liste des événements du journal d'audit système reprend alors tous les événements.

Suppression des événements du journal d'audit système

Par défaut, Kaspersky Embedded Systems Security conservera les entrées du journal d'audit système pendant une durée indéterminée. Vous pouvez instaurer une limite pour la durée de conservation 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 Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Ouvrez le menu contextuel du nœud secondaire **Journal d'audit système** et choisissez l'option **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 à leur manipulation.

Dans cette section

A propos des journaux d'exécution des tâches

Les informations relatives à l'exécution des tâches de Kaspersky Embedded Systems Security apparaissent dans le volet résultats lorsque le nœud **Journaux d'exécution des tâches** a été sélectionné dans la console de Kaspersky Embedded Systems Security.

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 jusqu'à maintenant ainsi que les paramètres de la tâche.

Par défaut, Kaspersky Embedded Systems Security conservera 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 dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers journal d'exécution des tâches différent du dossier par défaut. Vous pouvez également sélectionner les événements qui seront consignés dans les journaux d'exécution des tâches de Kaspersky Embedded Systems Security.

Consultation de la liste des événements dans les journaux d'exécution des tâches

► *Pour consulter la liste des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

La liste des événements consignés dans les journaux d'exécution des tâches 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 événements dans les journaux d'exécution des tâches

Par défaut, les événements sont classés dans les journaux d'exécution des tâches par ordre chronologique inverse. Vous pouvez les trier selon le contenu de n'importe quelle colonne.

► *Pour trier les événements repris dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.
3. Dans le panneau de résultats, sélectionnez l'en-tête de la colonne selon le contenu de laquelle vous souhaitez trier les événements des journaux d'exécution des tâches de Kaspersky Embedded Systems Security.

Le résultat du tri est conservé jusqu'à la prochaine consultation des journaux d'exécution des tâches.

Filtrage des événements dans les 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 enregistrements relatifs aux événements qui répondent aux conditions de filtrage que vous définissez (filtres).

► *Pour filtrer les événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.

2. Ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Filtre**.

   La fenêtre **Paramètres du filtre** s'ouvre.

3. Pour ajouter un filtre, procédez comme suit :

   a. Dans la liste **Nom du champ**, sélectionnez la colonne selon laquelle vous souhaitez 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 à l'aide de l'opérateur logique « ET », sélectionnez l'option **Quand toutes les conditions sont remplies**.

   - Afin de réunir quelques filtres à l'aide de l'opérateur logique « OU », 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 événements des journaux d'exécution des tâches affiche alors uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusqu'à la prochaine consultation des journaux d'exécution des tâches.

► *Pour désactiver le filtre, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.

2. Ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Supprimer le filtre**.

La liste des événements des journaux d'exécution des tâches reprend alors tous les événements.

Consultation des statistiques et des informations relatives à une tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches

Les journaux d'exécution des tâches reprennent des informations détaillées sur tous les événements survenus dans ces tâches depuis leur lancement jusqu'au moment de la consultation 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 Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.

2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.

3. Dans le volet résultats, ouvrez la fenêtre **Journal d'exécution** à l'aide d'une des méthodes suivantes :

    - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.

    - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal 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 **Evénements** présente la liste des événements consignés pendant l'exécution de la tâche ;

    - L'onglet **Paramètres** reprend les paramètres de la tâche.

5. Le cas échéant, cliquez sur le bouton **Filtre** 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 **Journal d'exécution** sera fermée.

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 Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.
3. Dans le volet résultats, ouvrez la fenêtre **Journal d'exécution** à l'aide d'une des méthodes suivantes :
   - Double-clic de la souris sur l'événement survenu dans la tâche dont vous souhaitez consulter le journal.
   - Ouvrez le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez consulter le journal et choisissez l'option **Voir le journal**.
4. Dans la partie inférieure de la fenêtre **Journal d'exécution**, 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 événements des journaux d'exécution des tâches

Par défaut, Kaspersky Embedded Systems Security conservera 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 tous les événements des journaux d'exécution des tâches terminées à ce moment.

> Les événements des journaux des tâches en cours d'exécution et les journaux utilisés par d'autres utilisateurs ne seront pas supprimés.

► *Pour supprimer des événements dans les journaux d'exécution des tâches, procédez comme suit :*

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, développez l'entrée **Journaux**.
2. Choisissez le nœud secondaire **Journaux d'exécution des tâches**.
3. Exécutez une des actions suivantes :
   - Si vous souhaitez supprimer des événements de tous les journaux d'exécution des tâches terminées en ce moment, ouvrez le menu contextuel du nœud secondaire **Journaux d'exécution des tâches** et choisissez l'option **Effacer**.
   - Si vous souhaitez effacer le contenu du journal d'exécution d'une tâche distincte, ouvrez, dans le volet résultats, le menu contextuel de l'événement survenu dans la tâche dont vous souhaitez efface le journal d'exécution et choisissez l'option **Supprimer**.

- Si vous souhaitez effacer le contenu des journaux d'exécution de plusieurs tâches, procédez comme suit :

    a. Dans le volet résultats, enfoncez la touche **Ctrl** ou **Maj** et sélectionnez les événements survenus dans les tâches dont vous souhaitez supprimer les journaux d'exécution.

    b. Ouvrez le menu contextuel du menu de n'importe lequel des événements enregistrés 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 des tâches sélectionnés seront effacés. La suppression des événements des journaux d'exécution des tâches seront enregistrées dans le journal d'audit système.

Journal des événements de sécurité

Kaspersky Embedded Systems Security tient un journal des événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur l'ordinateur protégé. Ce journal enregistre les événements suivants :

- Les événements du composant 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, Analyse à la demande, Monitoring d'intégrité des fichiers, Contrôle du lancement des applications et Contrôle des périphériques).

Vous pouvez purger le journal des événements de sécurité de la même manière que pour le journal d'audit système (cf. section « Suppression des événements du journal d'audit système » à la page 341). Dans ce cas, Kaspersky Embedded Systems Security enregistre l'événement d'audit système sur la purge du journal des événements de sécurité.

Consultation du journal des événements de Kaspersky Embedded Systems Security dans la console Observateur d'événements

A l'aide du composant logiciel enfichable **Observateur d'événements** pour Microsoft Management Console, vous pouvez 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 Kaspersky Embedded Systems Security.

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 consignés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est **Evénements d'information** : les événements de tous les niveaux d'importance sont consignés ; le moins détaillé est le niveau **Evénements critiques** où seuls les événements critiques sont consignés. Par défaut, le niveau défini pour tous les composants à l'exception de **Mise à jour** est le niveau de détails **Evénements importants** (seuls les événements importants et critiques sont enregistrés) ; pour le composant **Mise à jour**, c'est le niveau **Evénements d'information** qui est sélectionné.

► *Pour consulter le journal des événements de Kaspersky Embedded Systems Security, procédez comme suit :*

1. Si vous configurez les paramètres localement, cliquez sur le bouton **Démarrer**, dans la barre de recherche, saisissez la commande `mmc`, puis appuyez sur la touche **ENTER**.

   La fenêtre de Microsoft Management Console s'ouvre.

2. Choisissez **Fichier** → **Ajouter ou supprimer des composants logiciels enfichables**.

   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** l'ordinateur 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 **OK**.

   Le nœud **Observateur d'événements** apparaît dans l'arborescence de la Console.

6. Dans l'arborescence de la Console, développez le nœud **Observateur d'événements**, puis sélectionnez le nœud secondaire **Journaux des apps et des services → Kaspersky Embedded Systems Security**.

Le journal des événements de Kaspersky Embedded Systems Security s'ouvre.

Configuration des paramètres des journaux dans la console de Kaspersky Embedded Systems Security

Vous pouvez configurer 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 journal d'exécution des tâches et du journal d'audit système ;
- Seuils de déclenchement des événements *Les bases de l'application sont dépassées*, *Les bases de l'application sont fortement dépassées* et *L'analyse des zones critiques de l'ordinateur n'a pas été réalisée depuis longtemps* ;
- Événements consignés par Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches, 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 paramètres des journaux de Kaspersky Embedded Systems Security, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel du nœud **Journaux et notifications** et choisissez l'option **Propriétés**.

   La fenêtre **Paramètres des journaux** s'ouvre.

2. Dans la fenêtre **Paramètres des journaux**, configurez les paramètres des journaux en fonction de vos exigences. Pour ce faire, procédez comme suit :

   - Sous l'onglet **Général**, sélectionnés, le cas échéant, les événements consignés par Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches, 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 dont vous souhaitez configurer le niveau de détails.

       S'agissant des composants Protection des fichiers en temps réel, Analyse à la demande et Mise à jour, il est prévu d'enregistrer les événements dans les journaux d'exécution des tâches et dans le journal des événements. Pour ces composants, le tableau de la liste des événements contient les colonnes **Journaux** et **Journal des événements**. S'agissant des composants Quarantaine et Sauvegarde, les événements sont consignés 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**.

     - 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 des tâches, 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.

- Sur l'onglet **Avancé**, configurez les paramètres de la conservation des journaux et les seuils de création des événements sur l'état de la protection de l'ordinateur :

  - Dans le groupe **Enregistrement des journaux** :

    - **Dossier des journaux**.

    Chemin d'accès au dossier contenant les journaux ; au format UNC (Universal Naming Convention).

    Le chemin défini par défaut C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\1.1\Reports\.

    - **Supprimer les journaux d'exécution des tâches et événements de plus de (jours)**.

    La case active ou désactive la fonction qui supprime les journaux contenant les résultats de l'exécution des tâches terminées et les événements publiés dans le journal d'exécution des tâches à l'issue de la période définie (par défaut, 30 jours).

    Quand la case est cochée, Kaspersky Embedded Systems Security supprime les journaux des résultats d'exécution des tâches terminées et les événements publiés dans les journaux d'exécution des tâches à l'issue de la période définie.

    Cette case est cochée par défaut.

    - **Supprimer les événements du journal d'audit de plus de (jours)**.

La case active ou désactive la fonction qui supprime les événements enregistrés dans le journal d'audit à l'issue de la période définie (par défaut, 60 jours).

Quand la case est cochée, Kaspersky Embedded Systems Security supprime les événements enregistrés dans le journal d'audit à l'issue de la période définie.

Cette case est cochée par défaut.

- Dans le groupe **Seuil de déclenchement des événements** :
  - Nombre de jours à l'issue desquels les événements *Les bases de l'application sont dépassées*, *Les bases de l'application sont fortement dépassées* et *L'analyse rapide de l'ordinateur n'a pas été réalisée depuis longtemps* seront déclenchés.

Tableau 35. Seuils de déclenchement des événements

Paramètre	Seuils de déclenchement des événements.
Description	Vous pouvez définir le seuil de déclenchement des événements des trois types suivants : • *Les bases de l'application sont dépassées* et *Les bases de l'application sont fortement dépassées*. Cet événement se déclenche lorsque les bases de Kaspersky Embedded Systems Security n'ont pas été actualisées durant une période (nombre de jours) définie depuis la création des dernières mises à jour des bases de données. Vous pouvez configurer la notification de l'administrateur lorsque ces événements surviennent. • *L'analyse rapide de l'ordinateur n'a pas été réalisée depuis longtemps*. Cet événement se déclenche si aucune des tâches accompagnées de la case **Considérer l'exécution de la tâche d'analyse des zones critiques** n'a été exécutée au cours du nombre de jours indiqué.
Valeurs possibles	Nombre de jours compris entre 1 et 365.
Valeur par défaut	Les bases de l'application sont dépassées – 7 jours ; Les bases de l'application sont fortement dépassées – 14 jours ; L'analyse des zones critiques n'a pas été réalisée depuis longtemps – 30 jours.

- Sous l'onglet **Intégration à SIEM**, configurez les paramètres de la publication des événements de l'audit et des événements des tâches exécutées (cf. section « Configuration des paramètres d'intégration à SIEM » à la page 358) sur le serveur syslog.

3. Cliquez sur **OK**.

Les modifications seront enregistrées.

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 volumes 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*.

Le serveur syslog est un serveur d'agrégation d'événements externe (SIEM), effectuant la collecte et l'analyse des événements reçus, ainsi que d'autres actions d'administration des journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : ce mode suppose que 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'ordinateur local même après avoir été envoyés à SIEM.

  Il est recommandé d'utiliser ce mode pour réduire au maximum la charge sur l'ordinateur protégé.

- Supprimer les copies locales des événements : ce mode suppose que tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans SIEM soient supprimés de l'ordinateur local.

  > L'application ne supprime jamais les versions locales du journal des violations de la sécurité.

Kaspersky Embedded Systems Security peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog pour transmettre les événements et les reconnaître au niveau du 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 SIEM utilisé.

Paramètres de restauration du logiciel

Vous pouvez réduire le risque d'erreur d'envoi des événements à 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 vous informe également d'une tentative manquée de connexion à SIEM et des erreurs d'envoi des événements à SIEM à l'aide des événements de l'audit système.

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 de fonctionnement (cf. tableau ci-dessous).

Tableau 36. 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 lors de l'écriture sur un serveur syslog externe	Pas appliqué	Vous pouvez configurer les paramètres de conservation des copies locales des journaux, après leur envoi à 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 SIEM.
Protocole de connexion	UDP	Vous pouvez configurer la connexion aux serveurs syslog principal et complémentaire via les protocoles UPD 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.

Paramètre	Valeur par défaut	Description
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 principal 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 Kaspersky Embedded Systems Security, ouvrez le menu contextuel de l'entrée **Journaux et notifications**.
2. Choisissez l'option **Paramètres**.

   La fenêtre **Paramètres des journaux** s'ouvre.
3. Sélectionnez l'onglet **Intégration à SIEM**.
4. Dans le groupe **Paramètres d'intégration**, cochez la case **Envoyer les événements à un serveur syslog externe via le protocole syslog**.

   La case active ou désactive l'utilisation de la fonction d'envoi des événements publiés au serveur syslog externe.

   Si la case est cochée, l'application exécute l'envoi des événements publiés sur SIEM conformément à la configuration des paramètres d'intégration à SIEM.

   Si la case est décochée, l'application n'exécute pas l'intégration à SIEM. Vous ne pouvez pas configurer les paramètres d'intégration à SIEM si la case est décochée.

   Cette case est décochée par défaut.

5. Si besoin, dans le groupe **Paramètres d'intégration**, cochez la case **Supprimer les copies locales des événements lors de l'écriture sur un serveur syslog externe**.

   La case active ou désactive la suppression des copies locales des journaux au moment de leur envoi à SIEM.

   Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le SIEM. Il est recommandé d'utiliser ce mode sur les ordinateurs de faible puissance.

   Si la case est décochée, l'application envoie uniquement les événements à SIEM. Les copies des journaux continuent d'être conservées localement.

   Cette case est décochée par défaut.

   L'état de la case **Supprimer les copies locales des événements lors de l'écriture sur un serveur syslog externe** n'influence pas les paramètres de conservation des événements du journal de la sécurité : l'application ne supprime jamais automatiquement les événements du journal de la sécurité.

6. Dans le groupe **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 à SIEM.

   Par défaut, l'application exécute la conversion au format de données structurées.

7. Dans le groupe **Paramètres du serveur syslog récepteur**, procédez comme suit :

   - Indiquez le protocole de connexion à SIEM.
   - Indiquez les paramètres de connexion au serveur syslog principal.

     Vous pouvez indiquer l'adresse IP uniquement au format IPv4.

   - Si besoin, cochez la case **Utiliser le serveur syslog complémentaire si le serveur syslog principal n'est pas disponible**, si voulez que l'application utilise d'autres paramètres de connexion, quand l'envoi des événements sur le serveur syslog principal n’est pas disponible. Indiquez les paramètres de connexion au serveur syslog miroir.

Les champs **Adresse IP** 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 indiquer l'adresse IP uniquement au format IPv4.

8. Cliquez sur **OK**.

Les paramètres d'intégration à SIEM configurés seront appliqués.

Licence

Les informations détaillées sur la licence de Kaspersky Embedded Systems Security figurent dans le *Manuel de l'administrateur Kaspersky Embedded Systems Security 2.0*, section Licence de l'application.

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 serveur, ainsi que les instructions relatives à la configuration des notifications.

Dans cette section

Moyens de notification de l'administrateur et des utilisateurs

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

L'application assure l'exécution des tâches suivantes :

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent l'ordinateur protégé et les utilisateurs de terminaux de l'ordinateur 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 Kaspersky Embedded Systems Security, vous pouvez activer les notifications de l'administrateur et 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 terminaux si l'ordinateur protégé est un ordinateur de terminaux.

    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'ordinateur protégé en fonction de l'événement.

    c. Envoi par email.

    Ce mode permet l'envoi de messages électroniques.

Vous pouvez créer un texte différent pour chaque type d'événement. Ce texte peut contenir des champs avec les informations sur l'événement. Un texte prédéfini du message 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 notifications sur les événements, procédez comme suit :*

1. Dans l'arborescence de la console de Kaspersky Embedded Systems Security, ouvrez le menu contextuel du nœud **Journaux** et choisissez la commande **Propriétés**.

    La fenêtre **Paramètres des journaux** 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 configurer les notifications des utilisateurs uniquement pour l'événement **Objet détecté**.

3. Si vous souhaitez modifier le texte de la notification, procédez comme suit :

    a. Cliquez sur le bouton **Texte du message**. Dans la fenêtre **Texte du message**, saisissez le texte qui sera affiché dans le message relatif à l'événement.

> Vous pouvez composer un texte du message de notification pour plusieurs types d'événements : après avoir choisi le mode de notification pour un type d'événement, sélectionnez, à l'aide de la touche **CTRL** ou **MAJ**, les autres types d'événements pour lesquels vous souhaitez créer ce même texte du message avant de clique sur le bouton **Texte du message**.

    b. 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 rubrique.

    c. Pour restaurer le texte du message prévu par défaut pour l'événement, cliquez sur **Par défaut**.

4. Si vous souhaitez configurer les modes de notification sélectionnés de l'administrateur sur un événement sélectionné, cliquez sur le bouton **Configuration** dans la fenêtre **Notifications** et dans la fenêtre **Paramètres avancés**, procédez à la configuration des modes sélectionnés. 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 **Sujet** et **De**. Le texte du champ **Sujet** 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 cochez la case **Authentification SMTP requise** 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 le service de messagerie, sous l'onglet **Service Windows Messenger**, composez la liste des ordinateurs des destinataires des messages : pour chaque ordinateur 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 de l'ordinateur protégé qui sera exécuté sur l'ordinateur lorsque l'événement se produira dans l'onglet **Fichier exécutable** ou saisissez le chemin d'accès à ce dernier. 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 répéter la notification plus de** sous l'onglet **Avancé** et indiquez la valeur souhaitée par unité de temps.

5. Cliquez sur **OK**.

Les paramètres de la notification définis seront enregistrés.

Tableau 37. Champs d'information sur les événements

Variable	Description
%EVENT_TYPE%	Type d'événement.
%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 de protection en temps réel et d'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 (https://securelist.fr). 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 (cf. section « Consultation des statistiques et des informations relatives à une tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches » à la page 345).
%VIRUS_TYPE%	Type de l'objet détecté selon la classification de Kaspersky Lab, 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 (cf. section « Consultation des statistiques et des informations relatives à une tâche de Kaspersky Embedded Systems Security dans les journaux d'exécution des tâches » à la page 345).
%USER_COMPUTER%	Dans la tâche Protection des fichiers en temps réel, il s'agit du nom de l'ordinateur dont l'utilisateur a sollicité un objet sur l'ordinateur.

Variable	Description
%USER_NAME%	Dans la tâche Protection des fichiers en temps réel, il s'agit du nom d'utilisateur qui a sollicité un objet sur l'ordinateur.
%FROM_COMPUTER%	Nom de l'ordinateur 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)

Glossaire

A

Analyse heuristique

Technologie d'identification des menaces impossibles à reconnaître à l'aide de la version actuelle des bases des applications de Kaspersky Lab. Elle permet de trouver les fichiers qui peuvent contenir des virus inconnus ou une nouvelle modification d'un virus connu.

Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état *infecté*.

Analyseur heuristique

Module de Kaspersky Embedded Systems Security qui exécute l'analyse heuristique.

Archive

Un ou plusieurs fichiers repris dans un fichier compressé. La compression et la décompression des données requièrent une application spéciale : un programme de décompression.

B

Bases antivirus

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases antivirus. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Ces bases antivirus sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

C

Clé active

Clé utilisée actuellement par l'application.

Clé additionnelle

Clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée actuellement.

D

Désinfection des objets

Mode de traitement des objets infectés qui entraîne la restauration complète ou partielle des données. Certains objets infectés ne peuvent être désinfectés.

F

Faux positif

Situation où un objet non infecté est considéré comme infecté par une application de Kaspersky Lab car son code évoque celui d'un virus.

Fichier infecté

Fichier contenant un code malveillant (pendant l'analyse du fichier, le code d'un programme connu présentant une menace a été détectée). Les experts de Kaspersky Lab vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

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 et d'activation de code malveillant est nettement élevé pour ces fichiers.

Fichier probablement infecté

Fichier contenant le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets probablement infectés sont identifiés à l'aide de l'analyse heuristique.

G

Groupe d'administration

Ensemble de périphériques regroupés selon leurs fonctions et les applications de Kaspersky Lab installées sur ceux-ci. Les périphériques sont regroupés pour en faciliter la gestion au sein d'un ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

M

Masque de fichier

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- ***** : remplace zéro ou plus de caractère de n'importe quel type.
- **?** : remplace n'importe quel caractère.

Il faut prendre en considération que le nom est toujours séparé de l'extension du fichier par un point.

Mise à jour

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

O

Objet OLE

Fichier associé ou intégré à un autre fichier. Les programmes de Kaspersky Lab permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Microsoft Office Excel® dans un document Microsoft Office Word, ce tableau sera analysé en tant qu'objet OLE.

Objets exécutés au démarrage du système

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur l'ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

Paramètres de la tâche

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

Paramètres de l'application

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la Sauvegarde.

Q

Quarantaine

Dossier dans lequel l'application de Kaspersky Lab place les objets probablement infectés qu'elle a détectés. Les objets en quarantaine sont chiffrés afin qu'ils ne puissent pas agir sur l'ordinateur.

R

Sauvegarde

Stockage spécial prévu pour conserver les copies de sauvegarde des fichiers créées avant leur désinfection ou leur suppression.

S

Serveur d'administration

Module de l'application Kaspersky Security Center qui remplit la fonction de centralisation des informations relatives aux applications de Kaspersky Lab installées sur le réseau de la société et qui permet de les administrer.

T

Tâche

Fonctions exécutées par l'application de Kaspersky Lab sous la forme de tâches, par exemple : Protection des fichiers en temps réel, Analyse complète du périphérique, Mise à jour des bases de données.

V

Vulnérabilité

Erreur dans un système d'exploitation ou dans un programme qui peut être utilisée par les éditeurs de 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.

AO Kaspersky Lab

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection informatique contre diverses menaces dont les virus et autres applications malveillantes, le courrier indésirable (spam), les attaques de réseau et les attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). D'après les données d'IDC, Kaspersky Lab est l'éditeur préféré de systèmes de protection informatique pour particuliers en Russie (« IDC Endpoint Tracker 2014 »).

Kaspersky Lab a été fondée en Russie en 1997. Kaspersky Lab est devenu un groupe international qui compte 38 bureaux dans 33 pays. L'entreprise emploie plus de 3000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers comprend des applications qui assurent la protection de l'information sur les ordinateurs de bureau et les ordinateurs portables, ainsi que sur les tablettes, les smartphones et autres périphériques nomades.

La société offre des solutions et des technologies de protection et de contrôle des postes de travail, des périphériques mobiles, des machines virtuelles, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. Elle propose également des produits spécialisés dans la protection contre les attaques DDoS, la protection des équipements gérés par l'automatisation industrielle et la prévention des escroqueries financières. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace et automatisée de toute organisation, quelle que soit sa taille, contre les menaces informatiques. Les applications de Kaspersky Lab sont certifiées par de grands organismes d'évaluation. Elles sont compatibles avec les logiciels de nombreux fournisseurs et sont optimisées pour une exécution sur de nombreuses plateformes.

Les experts antivirus de Kaspersky Lab travaillent 24 heures sur 24. Chaque jour, ils trouvent des centaines de milliers de nouvelles menaces informatiques, développent les outils d'identification et de désinfection de ces menaces et ajoutent les signatures de ces menaces aux bases utilisées par les applications de Kaspersky Lab.

Technologie. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est dès lors pas un hasard si le noyau logiciel de Kaspersky Anti-Virus a été adopté par de nombreux autres éditeurs de logiciels comme Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu ou ZyXEL. Beaucoup des innovations technologiques de l'entreprise sont brevetées.

Résultats. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a remporté des centaines de récompenses. Ainsi, Kaspersky Lab est devenue en 2014 une des deux sociétés détenant le plus de certificats Advanced+ à l'issue de tests réalisés par le laboratoire antivirus autrichien AV-Comparatives. Ces performances ont valu le certificat Top Rated à Kaspersky Lab. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 400 millions de personnes. Kaspersky Lab compte plus de 270 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	https://www.kaspersky.fr
Encyclopédie des virus :	https://securelist.fr
Laboratoire de virus :	https://virusdesk.kaspersky.com/fr (pour l'analyse de fichiers ou de sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.fr

Informations 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

Index

A

B

C

D

E

F

G

I

J

K

L

M

P

Q

R

S

T

Z