kaspersky

Kaspersky Embedded Systems Security 4.1 for Windows

© 2026 AO Kaspersky Lab

Contenu

Kaspersky Embedded Systems Security for Windows
- Nouveautés
- Problèmes résolus
- Distribution
- Configurations logicielles et matérielles
- Versions de Kaspersky Security Center prises en charge
- Exigences fonctionnelles et restrictions
  - Installation et suppression de l'application
  - Contrôle de l'intégrité du système
  - Pare-feu
  - Limitations des versions obsolètes de Windows
  - Intégration avec Kaspersky Security Center
  - Autres restrictions
- Compatibilité avec d'autres applications

Installation et suppression de l'application
- Planification de l'installation
  - Sélection des outils d'administration
  - Sélection du type d'installation
- Installation et suppression de l'application à l'aide de l'Assistant
  - Installation à l'aide de l'Assistant d'installation
    - Installation de Kaspersky Embedded Systems Security
    - Installation de la console de Kaspersky Embedded Systems Security
    - Configuration avancée après l'installation de la console de l'application sur un autre appareil
      - Autorisation de l'accès à distance anonyme aux applications COM
      - Autorisation des connexions réseau pour le processus d'administration à distance de Kaspersky Embedded Systems Security
    - Actions à réaliser après l'installation de Kaspersky Embedded Systems Security
      - Lancement et configuration de la tâche Mise à jour des bases et des modules d'application
      - Analyse rapide
  - Modification de la sélection de modules et réparation de Kaspersky Embedded Systems Security
  - Suppression à l'aide de l'Assistant d'installation
    - Désinstallation de Kaspersky Embedded Systems Security
    - Désinstallation de la console de Kaspersky Embedded Systems Security
- Installation et suppression de l'application via la ligne de commande
  - À propos de l'installation et de la désinstallation de Kaspersky Embedded Systems Security via la ligne de commande
  - Codes des modules logiciel de Kaspersky Embedded Systems Security pour le service Windows Installer
  - Paramètres d'installation et de récupération et options de ligne de commande de Windows Installer
  - Exemple de commandes pour l'installation de Kaspersky Embedded Systems Security
  - Actions à réaliser après l'installation de Kaspersky Embedded Systems Security
  - Ajout et suppression de modules. Exemples de commandes
  - Désinstallation de Kaspersky Embedded Systems Security. Exemples de commandes
  - Codes de retour

Installation et suppression de l'application via Kaspersky Security Center
Informations générales sur l'installation via Kaspersky Security Center
Privilèges pour l'installation ou la désinstallation de Kaspersky Embedded Systems Security
Installation de Kaspersky Embedded Systems Security via Kaspersky Security Center
Actions à réaliser après l'installation de Kaspersky Embedded Systems Security
Installation de la console de l'application via Kaspersky Security Center
Désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center
Modification de l'ensemble des modules d'application à l'aide de Kaspersky Security Center
Installation et suppression de l'application via les stratégies de groupe Active Directory
Installation de Kaspersky Embedded Systems Security via des stratégies de groupe d'Active Directory
Actions à réaliser après l'installation de Kaspersky Embedded Systems Security
Désinstallation de Kaspersky Embedded Systems Security via des stratégies de groupe d'Active Directory
Journaux d'installation et de désinstallation de Kaspersky Embedded Systems Security
Modifications introduites dans le système après l'installation de Kaspersky Embedded Systems Security
Processus de Kaspersky Embedded Systems Security
Vérification des fonctions de Kaspersky Embedded Systems Security. Utilisation du virus d'essai EICAR
À propos du virus d'essai EICAR
Vérification de la Protection des fichiers en temps réel et de l'Analyse à la demande
Mise à jour des anciennes versions de Kaspersky Embedded Systems Security vers la version 4.1
Mise à jour de Kaspersky Embedded Systems Security
Mise à jour des outils d'administration de Kaspersky Embedded Systems Security
Migration des stratégies et des tâches
Migration des paramètres de la version de l'application en cours de mise à jour
Correspondance des modules et des tâches dans les versions 3.4 et 4.1 de Kaspersky Embedded Systems Security
Interface de l'application
Utilisation du plug-in d'administration
Gestion de Kaspersky Embedded Systems Security à partir de Kaspersky Security Center
Administration des paramètres de l'application
Configuration des paramètres généraux de l'application dans Kaspersky Security Center
Configuration de l'interface et de l'analyse dans Kaspersky Security Center
Configuration des paramètres de sécurité dans Kaspersky Security Center
Configuration des paramètres de connexion dans Kaspersky Security Center
Configuration du mode d'exécution des tâches locales
Configuration des paramètres de la Sauvegarde dans Kaspersky Security Center
Création et configuration des stratégies
Création d'une stratégie
Configuration d'une stratégie
Indicateur du niveau de protection
Création et configuration de tâches via Kaspersky Security Center
À propos de la création de tâches dans Kaspersky Security Center
Création d'une tâche dans Kaspersky Security Center
Accès aux paramètres locaux de la tâche et aux paramètres généraux de l'application pour un ordinateur
Configuration des tâches de groupe dans Kaspersky Security Center
Tâche d'activation de l'application
Tâche Mise à jour
Vérification de l'intégrité de l'application
Planification des tâches

Rapports dans Kaspersky Security Center
État de la Protection en temps réel
Utilisation de la console de Kaspersky Embedded Systems Security
Ouverture de la Console de l'application
Interface de la console de Kaspersky Embedded Systems Security
Fenêtre de la console de Kaspersky Embedded Systems Security
Icône de la barre d'état système dans la zone de notification
Configuration des paramètres généraux via la Console de l'application
Administration des tâches de Kaspersky Embedded Systems Security
Catégories de tâche de Kaspersky Embedded Systems Security
Lancement, suspension, rétablissement et arrêt manuels des tâches
Planification des tâches
Utilisation des comptes utilisateur pour l'exécution des tâches
À propos de l'utilisation des comptes utilisateur pour l'exécution des tâches
Définition du compte utilisateur pour l'exécution de la tâche
Importation et exportation des paramètres
À propos de l'importation et de l'exportation des paramètres
Exportation des paramètres
Importation des paramètres
Consultation de l'état de la protection et des informations de Kaspersky Embedded Systems Security
Comment configurer les paramètres de la Sauvegarde dans la Console de l'application
Utilisation du Plug-in Web depuis Web Console et Cloud Console
Gestion de Kaspersky Embedded Systems Security à partir de Web Console ou de Cloud Console
Limitations du Plug-in Web
Administration des paramètres de l'application
Configuration des paramètres généraux de l'application dans le Plug-in Web
Configuration de l'interface et de l'analyse dans plug-in Web
Configuration des paramètres de sécurité et de fiabilité dans le plug-in Web
Configuration des paramètres de connexion dans le plug-in Web
Configuration du lancement planifié des tâches locales dans le plug-in web
Configuration des paramètres de la Sauvegarde dans le plug-in Web
Création et configuration des stratégies
Création et configuration de tâches via Kaspersky Security Center
À propos de la création de tâches dans le Plug-in Web
Création d'une tâche dans le Plug-in Web
Configuration des tâches de groupe dans le Plug-in Web
Configuration de la tâche Activation de l'application dans le plug-in Web
Configuration de la tâche Mise à jour dans le plug-in Web
Planification des tâches
Rapports dans Kaspersky Security Center
Licence de l'application
À propos du Contrat de licence
À propos de la licence
À propos du certificat de licence
À propos de la clé
À propos du fichier clé
À propos du code d'activation

Comparaison des fonctionnalités des applications en fonction du type de licence
Activation de l'application à l'aide d'un fichier clé
Activation de l'application à l'aide d'un code d'activation
Consultation des informations sur la licence active
Renouvelement de l'autorisation
Suppression de la clé
Lancement et arrêt de Kaspersky Embedded Systems Security
Démarrage et arrêt de l'application
Suspension et rétablissement de la protection et du contrôle de l'ordinateur
Interface de diagnostic compacte
À propos de l'interface de diagnostic compacte
Révision de l'état de Kaspersky Embedded Systems Security via l'interface de diagnostic compacte
Révision des statistiques des événements de sécurité
Révision de l'activité en cours de l'application
Configuration du traçage de l'application et de l'enregistrement des vidages de la mémoire
Auto-défense de Kaspersky Embedded Systems Security
Activation et désactivation du mécanisme de l'autodéfense
Prise en charge de la technologie AM-PPL
Protection des services du système d'exploitation
Configuration des autorisations utilisateurs pour administrer Kaspersky Embedded Systems Security
Configuration des autorisations d'accès des utilisateurs pour gérer le service Kaspersky Embedded Systems Security
Accès protégé par mot de passe aux fonctionnalités de Kaspersky Embedded Systems Security
Notifications du Bureau sécurisé
Exclusions de l'analyse pour l'application
Définition de l'exclusion de l'analyse
Sélection des types d'objets à détecter
Composition de la liste des applications de confiance
Création d'une zone de confiance locale
Exportation et importation de la zone de confiance
Utilisation du stockage système sécurisé des certificats
Exclusions d'analyse prédéfinies et applications de confiance
Protection des fichiers en temps réel
À propos de la zone de protection de la tâche et des paramètres de sécurité
Zones de protection prédéfinies
À propos des niveaux de sécurité prédéfinis
Extensions de fichiers analysés par défaut par le module Protection des fichiers en temps réel
Configuration du module Protection des fichiers en temps réel
Configuration de la zone de protection pour le module Protection des fichiers en temps réel
Configuration manuelle des paramètres de sécurité
Analyser les conteneurs.
Utilisation du KSN
Activation de l'utilisation de Kaspersky Security Network
Statistiques d'utilisation de Kaspersky Security Network
Limitations de Kaspersky Private Security Network
Paramètres du proxy KSN

Protection contre les Exploits
Mode de protection contre les exploits
Activation et désactivation de la Protection contre les Exploits
Activation et désactivation de la protection de la mémoire
Création de la liste des processus protégés
Réparation des actions malicieuses
Détection comportementale
Activation et désactivation de la protection par chiffrement des dossiers locaux
Protection des dossiers partagés contre le chiffrement externe
Activation et désactivation de la protection des dossiers partagés contre le chiffrement externe
Modification de la zone de protection
Ajout d'ordinateurs de confiance pour le chiffrement externe des données
Configuration de la période de blocage d'un ordinateur non fiable
Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe
Protection contre les menaces réseau
Activation et configuration de la Protection contre les menaces réseau
Création d'une exclusion du blocage
Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe
Analyseur AMSI
Activation et désactivation du Scanner AMSI
Paramètres du Scanner AMSI
Contrôle du lancement des applications
À propos des règles du Contrôle du lancement des applications
À propos du contrôle de la distribution des logiciels
À propos de la Génération des règles du Contrôle du lancement des applications
Activation et configuration du Contrôle du lancement des applications
Configuration du contrôle de la distribution des logiciels
Utilisation des règles du Contrôle du lancement des applications
Ajout des règles du Contrôle du lancement des applications
Ajout de conditions de déclenchement de la règle du Contrôle du lancement des applications
Ajout d'exclusions d'une zone de règles du Contrôle du lancement des applications
Autorisation du lancement de toutes les applications
Exportation des règles du Contrôle du lancement des applications
Création d'un fichier TXT avec une sélection d'événements d'applications bloqués par Kaspersky Security Center
Configuration d'une tâche de groupe Génération des règles du Contrôle du lancement des applications
Création des règles à l'aide d'une tâche de groupe Génération des règles du Contrôle du lancement des applications.
Contrôle des appareils
Règles d'accès aux appareils
Gestion de l'accès aux appareils par type
Contrôle des connexions Wi-Fi
Contrôle de l'impression
Contrôle des appareils d'entrée (HID)
Gestion de l'accès aux appareils mobiles
Surveillance de l'utilisation des disques amovibles
Gestion de l'accès aux appareils Bluetooth
Différenciation des privilèges d'accès des utilisateurs aux appareils
À propos du Générateur de règles pour le Contrôle des appareils

- Ajout d'appareils de confiance
- Exportation et importation de la liste des appareils de confiance

Pare-feu
- À propos des règles du pare-feu
- Configuration du pare-feu
  - Configuration des paramètres généraux du pare-feu
  - Création et configuration des règles du Pare-feu
  - Activation et désactivation des règles du pare-feu

Protection BadUSB

Contrôle de l'intégrité du système
- À propos des règles du Contrôle de l'intégrité du système
- Contrôle de l'intégrité du système en temps réel
- Vérification de l'intégrité du système sur demande
- Exportation et importation des règles du Contrôle de l'intégrité du système
- Affichage des rapports du Contrôle de l'intégrité du système

Inspection des journaux
- Ajout des règles personnalisées
- Configuration des règles prédéfinies

Analyse à la demande
- À propos des tâches d'analyse à la demande
- À propos de la zone d'analyse de la tâche et des paramètres de sécurité
- Zones d'analyse prédéfinies
- Analyse des fichiers dans le stockage en ligne
- À propos des niveaux de sécurité prédéfinis
- Analyse des disques amovibles
- Paramètres par défaut de la tâche d'analyse à la demande
- Gestion des tâches d'analyse à la demande
  - Création d'une tâche d'analyse à la demande
    - Exécution d'une tâche d'analyse à la demande en arrière-plan
    - Enregistrement de l'exécution d'une analyse rapide
  - Configuration de la zone d'analyse dans la tâche Analyse à la demande
  - Configuration des paramètres de la tâche d'analyse à la demande
  - Configuration de l'analyse des disques amovibles
  - Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande
  - Configuration manuelle des paramètres de sécurité
  - Statistiques des tâches d'analyse à la demande

Mise à jour des bases et des modules de Kaspersky Embedded Systems Security
- Mise à jour des bases et des modules de l'application
- À propos des tâches de mise à jour
- Schémas de mise à jour des bases de données et des modules de Kaspersky Embedded Systems Security
- Configuration des tâches de mise à jour
- Mise à jour SMU de l'application
- Copie sécurisée des bases de données de l'application
- Mise à jour sécurisée des bases de données de l'application
- Annulation des mises à jour des bases de l'application Kaspersky Embedded Systems Security
- Statistiques sur les tâches de mise à jour

Sauvegarde des objets
Sauvegarde des objets. Sauvegarde
Consultation des objets dans la sauvegarde
Restauration des fichiers depuis la Sauvegarde
Suppression des fichiers de la Sauvegarde
Envoi des objets probablement infectés à Kaspersky pour examen
Configuration des paramètres de la Sauvegarde
Statistiques de sauvegarde
Interdire l'accès aux ressources réseau. Sessions réseau bloquées
Liste des sessions réseau bloquées
Gestion de la liste des sessions réseau bloquées
Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security
Méthodes d'enregistrement des événements de Kaspersky Embedded Systems Security
Configuration des paramètres des journaux
Tri des événements dans le journal
Filtrage des événements dans le journal
Suppression des événements du journal
Exportation des informations depuis le journal
Journal d'audit système
Journaux des modules et des tâches
Consultation du journal des événements de Kaspersky Embedded Systems Security dans l'observateur d'événements
À propos de l'intégration à SIEM
Configuration des paramètres d'intégration à SIEM
Moyens de notification de l'administrateur et des utilisateurs
Configuration des notifications de l'administrateur et des utilisateurs
Configuration les notifications par email
Configuration de l'interaction avec le Serveur d'administration
Gestion du chiffrement du disque BitLocker
Lancement du chiffrement de disque BitLocker
Déchiffrement d'un disque dur protégé par BitLocker
Restauration de l'accès au disque protégé par BitLocker
Interruption de la protection BitLocker pour mettre à jour un logiciel
Intégration aux systèmes tiers
Compteurs de performance pour l'application Moniteur système
Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)
Nombre de requêtes soumises pour traitement
Nombre d'objets traités par seconde
Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)
Total de requêtes rejetées (Total number of requests denied)
Total de requêtes ignorées (Total number of requests skipped).
Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers
Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers
Compteurs et interruptions SNMP de Kaspersky Embedded Systems Security
Compteurs SNMP de Kaspersky Embedded Systems Security
Compteurs de performance
Compteur de sauvegarde

Compteurs généraux
Compteur de mise à jour
Compteurs de Protection des fichiers en temps réel
Compteurs du Scanner AMSI
Interruptions SNMP de Kaspersky Embedded Systems Security et leur option
Descriptions et valeurs possibles des options d'interruptions SNMP de Kaspersky Embedded Systems Security
Intégration de WMI
Managed Detection and Response
Configuration de l'intégration MDR
Gestion de Kaspersky Embedded Systems Security via la ligne de commande
APPCONTROL. Importation des règles du Contrôle du lancement des applications
APPCONTROL /CONFIG. Configuration du module Contrôle du lancement des applications
APPCONTROL /GENERATE. Générateur de règles pour le Contrôle du lancement des applications
CONFIG. Prise en charge de la technologie AM-PPL
DEVCONTROL. Importation des règles du Contrôle des appareils
DUMP. Enregistrement des vidages de la mémoire
EXITPOLICY. Désactivation de la stratégie sur l'appareil
EXPORT. Exportation des paramètres de l'application
FBRESET. Nettoyage de la base iSwift
FIM /BASELINE. Contrôle de l'intégrité du système par rapport à une référence
AIDE. Affichage de l'aide sur les commandes
IMPORT. Importation des paramètres de l'application
KSN. Utilisation de KSN/KPSN
LICENSE. Activation de l'application
MDR. Configuration de l'intégration de Managed Detection and Response
OMSINFO. Création d'un fichier JSON contenant des informations sur l'application
MOT DE PASSE. Accès protégé par mot de passe aux fonctionnalités de Kaspersky Embedded Systems Security
PATCHCOMPATIBILITYRESET. Suppression d'un correctif de la liste des correctifs incompatibles
REMOTEACCESS. Gestion des paramètres de connexion à distance de la Console de l'application
RESETMDRMACHINEID. Réinitialisation de l'identifiant de l'appareil
ROLLBACK. Annulation de la dernière mise à jour
RTP. Protection des fichiers en temps réel
ANALYSE. Analyse à la demande
SCANCRITICAL. Analyse des zones critiques
SERVERBINDINGDISABLE. Désactivation de la protection de la connexion au Serveur d'administration
START. Démarrage du service de l'application
STARTPOLICY. Activation de la stratégie
STOP. Arrêt du service de l'application
TASK. Gestion des tâches
TRAÇAGE. Traçage du fonctionnement de l'application
UPDATE. Mise à jour des bases de données et des modules de l'application
Contacter le Support Technique
Modes d'obtention de l'assistance technique
Assistance technique via Kaspersky CompanyAccount
Fourniture d'informations diagnostiques avancées aux experts du Support Technique
Traçage du fonctionnement de l'application
À propos de la composition et de la conservation des fichiers de traçage

Enregistrement des vidages de la mémoire
Protection des fichiers dump et de traçage
Obtention des données relatives au système d'exploitation (Kaspersky Get System Info)
Sources d'informations sur Kaspersky Embedded Systems Security
Annexes
Extensions de fichier pour analyse rapide
Comptes utilisateurs dans les règles des modules d'application
Informations légales
À propos des données
À propos des données dans le cadre du Contrat de licence utilisateur final
Collecte des données dans le cadre de l'utilisation de Kaspersky Security Network
Respect de la législation de l'Union européenne (RGPD)
Informations sur le code tiers
Notice sur les marques de commerce

Kaspersky Embedded Systems Security for Windows

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

L'application n'est pas conçue pour être utilisée dans des processus technologiques impliquant des systèmes de contrôle automatisés. Pour protéger les appareils dans de tels systèmes, il est recommandé d'utiliser l'application Kaspersky Industrial CyberSecurity for Nodes.

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

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

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

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

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

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

Modules et fonctions de Kaspersky Embedded Systems Security

L'application intègre les modules suivants :

- **Protection des fichiers en temps réel**. Kaspersky Embedded Systems Security analyse les objets à l'accès. Kaspersky Embedded Systems Security analyse les objets suivants :
  - Fichiers
  - Flux alternatifs des systèmes de fichiers (flux NTFS) ;
  - Enregistrements de démarrage principal et les secteurs d'amorçage des disques durs locaux ou amovibles.

- **Analyse à la demande**. Kaspersky Embedded Systems Security recherche une fois des virus et autres menaces informatique dans la zone indiquée. L'application analyse les fichiers, la mémoire vive et les objets de démarrage sur un appareil protégé.

- **Contrôle du lancement des applications**. Le module surveille les tentatives de lancement des applications par les utilisateurs et régule ce processus sur l'appareil protégé.

- **Contrôle des appareils**. Le module contrôle l'enregistrement et l'utilisation des appareils externes afin de protéger l'appareil contre les menaces sur la sécurité de l'information qui peuvent survenir pendant l'échange de fichiers avec des disques flash ou des appareils externes d'un autre type connectés par USB.

- **Pare-feu**. Selon son mode, le module : surveille le filtrage du trafic par le pare-feu Windows ; enregistre uniquement les événements relatifs à l'activité réseau de l'ordinateur protégé dans le journal du module ; ou filtre le trafic réseau en fonction des paramètres du Pare-feu.

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

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

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

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

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

- **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 modules distincts dans un fichier de configuration.

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

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

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

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

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

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

Nouveautés

Mise à jour 4.1

Nouvelles fonctionnalités et améliorations de Kaspersky Embedded Systems Security 4.1 for Windows :

- L'administration du chiffrement Windows BitLocker est désormais disponible. L'application permet d'utiliser Kaspersky Security Center pour chiffrer et déchiffrer les disques durs des appareils protégés et restaurer l'accès aux disques chiffrés.

- Vous pouvez désormais configurer les tâches planifiées pour qu'elles s'exécutent uniquement certains jours de la semaine, à un intervalle donné en semaines. La planification est disponible à partir de la version 16.1 de Kaspersky Security Center.

- Vous pouvez désormais suspendre les tâches d'analyse à la demande pendant une durée définie, par exemple pour effectuer une maintenance de routine.

- Les événements « *L'utilisation de l'appareil est interdite jusqu'au démarrage de Kaspersky Embedded Systems Security* » et « *La connexion de l'appareil est bloquée jusqu'au démarrage de Kaspersky Embedded Systems Security* » sont désormais disponibles. Désormais, si l'appareil est bloqué avant le lancement de l'application, l'événement correspondant est généré et envoyé au Serveur d'administration.

- Les systèmes d'exploitation suivants sont désormais pris en charge :

  - Windows 11 26H2

  - Windows 11 IoT 25H2

- Les performances du sous-système de disque dur sur l'appareil protégé ont été optimisées en réduisant le nombre d'opérations d'E/S.

- Lors du développement de cette version de Kaspersky Embedded Systems Security, nous avons intégré les modifications incluses dans les correctifs privés suivants : PF23074, PF23088, PF23089, PF23099, PF23102, PF23104, PF23105.

Mise à jour 4.0

Kaspersky Embedded Systems Security 4.0 offre les fonctionnalités et améliorations suivantes :

- Mise à jour notable de l'interface utilisateur de la Console d'application et des plug-ins d'administration de l'application à l'aide de Kaspersky Security Center.
- Prise en charge de Windows 11 24H2.
- Vous pouvez maintenant modifier le port que la Console d'application utilise pour se connecter à un ordinateur sur lequel l'application est installée.
- Dans la *Zone de confiance*, vous pouvez :
  - Configurer les processus de confiance de manière plus précise.
  - Utiliser le magasin de certificats de confiance.
- Nouveaux paramètres pour les privilèges d'administration de l'application par les utilisateurs et les groupes.
- Nouveau module *Anti-rootkit*. Par défaut, le module est activé si la *Protection des fichiers en temps réel* est activée. Vous pouvez désactiver le module lors de l'installation de l'application à l'aide de la tâche *Modifier les modules de l'application de Kaspersky Embedded Systems Security* ou dans les propriétés du paquet d'installation de l'application.
- Dans les paramètres de la *Protection contre les Exploits*, l'application peut désormais identifier automatiquement les processus protégés.
- Nouveau module *Réparation des actions malicieuses*.
- Le module Protection contre les menaces réseau peut surveiller le trafic réseau dans le but de détecter le balayage de ports et les requêtes réseau à haute intensité.
- L'application est désormais compatible avec le Pare-feu Windows. Il n'est plus nécessaire de supprimer le Pare-feu Windows pour installer l'application.
- Le module *Détection comportementale* surveille les dossiers partagés ainsi que les dossiers locaux.
- Le module *Contrôle du lancement des applications* a été retravaillé :
  - Modifications importantes dans la structure des paramètres du module.
  - Pour spécifier les conditions de déclenchement et les exclusions des règles du Contrôle du lancement des applications, vous pouvez désormais utiliser le type de disque, les catégories KL, les groupes KSN.
- Le module *Contrôle des appareils* a été retravaillé :
  - Par défaut, le module *Contrôle des appareils* est configuré pour autoriser la connexion de tous les appareils.
  - Le *Contrôle Wi-Fi* n'est plus un module distinct et fait maintenant partie du Contrôle des appareils.

- Ajout de la possibilité de contrôler les appareils connectés en fonction du bus de connexion.
- Ajout de la migration des paramètres d'accès aux disques amovibles lors de la mise à jour des versions antérieures de l'application vers la version 4.0.

- Le module *Gestion du pare-feu* a été retravaillé pour devenir le module *Pare-feu* qui, en plus d'assurer l'interface avec le pare-feu Windows, fonctionne désormais comme un pare-feu.
- Les fonctionnalités des modules *Contrôleur de l'intégrité des fichiers* et *Surveillance de l'accès au registre* ont été fusionnées dans le nouveau module *Contrôle de l'intégrité du système*. Cette amélioration vous permet de suivre efficacement les modifications apportées au système de fichiers et au registre Windows, ce qui renforce la protection contre les modifications non autorisées des données.
- L'application ne prend pas en charge la planification de modules individuels. Si les modules sont activés, ils tourneront tant que l'application est exécutée.
- Kaspersky Security Center Windows 15.1 est désormais pris en charge.
- Tâches de groupe ajoutées :
  - *Protection de la connexion au Serveur d'administration*
  - *Modification de l'ensemble de modules de Kaspersky Embedded Systems Security*
  - *Contrôle de l'intégrité du système par rapport à une référence* au lieu de *Surveillance de l'intégrité des fichiers*
  - *Mise à jour* au lieu de *Copie mises à jour*, *Mise à jour des bases de l'application* et *Mise à jour des modules de l'application*
  - *Annulation de la mise à jour* au lieu de *Annulation de la mise à jour des bases de l'application*
  - *Suppression de la clé*
- L'application vérifie la configuration des modules de contrôle avant d'enregistrer les paramètres. La vérification a été ajoutée pour les modules Contrôle du lancement des applications, Contrôle des appareils et Contrôle de l'intégrité du système. L'application affiche désormais un avertissement si les paramètres actuels du module de contrôle sont susceptibles d'augmenter la charge sur l'ordinateur ou de provoquer des défaillances du système. Par exemple, dans le cas du Contrôle du lancement des applications, si vous avez sélectionné le mode qui bloque toutes les applications sauf celles autorisées et que vous n'avez ajouté aucune règle d'autorisation, l'application affiche un avertissement, car une telle configuration peut entraîner des défaillances du système.
- Ajout de la possibilité de créer automatiquement des règles d'autorisation pour le contrôle du lancement des applications et d'exporter ces règles dans un fichier. Pour ce faire, exécutez la tâche *Générateur de règles pour le Contrôle du lancement des applications* et activez la création automatique de règles d'autorisation basées sur les applications en cours d'exécution, ainsi que l'exportation des règles d'autorisation. Vous pouvez utiliser le fichier obtenu pour dresser l'inventaire des logiciels installés sur l'appareil.
- Nouveau module, *Protection des attaques BadUSB*. Le module Protection BadUSB permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier. Lorsqu'un appareil USB identifié par le système d'exploitation comme un clavier est connecté à l'ordinateur, l'application invite l'utilisateur à taper sur ce clavier pour l'autoriser.
- L'*indicateur Niveau de sécurité* a été ajouté. L'indicateur Niveau de sécurité s'affiche en haut de la fenêtre des propriétés de la stratégie et indique le degré de conformité des paramètres de sécurité avec les recommandations de Kaspersky Lab. L'indicateur Niveau de sécurité vous permet de configurer rapidement la stratégie et d'activer les modules de protection requis.

Problèmes résolus

Le tableau ci-dessous répertorie tous les problèmes découverts dans les versions précédentes de Kaspersky Embedded Systems Security et corrigés dans la version actuelle.

Liste des problèmes corrigés dans la version 4.1

Identifiant	Description du problème
9986614	Dans Web Console et dans la Console d'administration de Kaspersky Security Center, il n'est pas possible d'importer une liste d'appareils de confiance à partir d'un fichier TXT contenant une sélection d'événements de Kaspersky Security Center liés aux appareils bloqués et exporté depuis Web Console.
10700703	Dans l'interface des modules Contrôle de l'intégrité du système, Zone de confiance, Contrôle du lancement des applications et Contrôle des appareils, la procédure de sélection des éléments de la liste en vue d'exécuter la commande **Exporter la sélection** n'est pas immédiatement évidente. La description figurant dans l'aide de l'application a été étoffée.
10720231	Le compteur des appareils de confiance ne s'affiche pas dans la section **Contrôle des appareils** de la stratégie dans la Console d'administration de Kaspersky Security Center.
10729552	Les événements liés aux opérations sur les fichiers stockés sur des disques amovibles ne sont pas générés, même si leur journalisation est activée.
10752491	Dans Web Console, il n'est pas possible d'importer une liste d'appareils de confiance à partir d'un fichier TXT contenant une sélection d'événements de Kaspersky Security Center liés aux appareils bloqués et exporté depuis la Console d'administration.

Distribution

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

- Lancer l'Assistant Installation de Kaspersky Embedded Systems Security.
- Lancer l'Assistant Installation de la console de Kaspersky Embedded Systems Security.
- Lancer Kaspersky Virus Removal Tool.
- En savoir plus sur cette version de Kaspersky Embedded Systems Security.
- Ouvrir l'aide de Kaspersky Embedded Systems Security 4.1.
- Ouvrir la page de Kaspersky Embedded Systems Security sur le site Internet de Kaspersky.
- Consulter le site Internet de Kaspersky.
- Visiter le site Web du Support technique.

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

Fichiers du kit de distribution de Kaspersky Embedded Systems Security

Fichier	Fonction
autorun.inf	Fichier de démarrage automatique de l'Assistant d'installation de Kaspersky Embedded Systems Security pour l'installation de l'application depuis un disque amovible.
setupui.exe	Fichier de lancement de l'écran d'accueil de l'application.
ess_win.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de l'application via Kaspersky Security Center.
\console\esstools.msi	Paquet d'installation Windows Installer, installe la Console de Kaspersky Embedded Systems Security sur les appareils protégés.
\console\setup_esstool.exe	Le fichier qui lance l'Assistant d'installation de la Console de Kaspersky Embedded Systems Security for Windows. Le fichier du paquet d'installation esstools.msi est lancé avec les paramètres d'installation définis par l'Assistant.
\console\license.txt	Fichier texte du Contrat de licence utilisateur final et de la politique de confidentialité de la Console d'administration de Kaspersky Embedded Systems Security.
\exec\bases.cab	Archive contenant les bases antivirus d'actualité au moment de l'édition de l'application.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Fichiers pour la suppression des applications incompatibles.
\exec\ess.cab	Fichiers pour l'interface graphique de l'application.
\exec\ess_win.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de l'application via Kaspersky Security Center.
\exec\ess_win.msi	Paquet d'installation Windows Installer : celui-ci installe Kaspersky Embedded Systems Security sur l'appareil protégé.
\exec\incompatible.txt	Kaspersky ne garantit pas la compatibilité de Kaspersky Embedded Systems Security avec les applications répertoriées dans le fichier.
\exec\installer.ini	Le fichier contenant les paramètres interne de la distribution.
\exec\klcfginst.msi	Programme d'installation du plug-in d'administration de Kaspersky Embedded Systems Security disponible via Kaspersky Security Center. Installez le plug-in d'administration sur chaque appareil protégé sur lequel la Console d'administration de Kaspersky Security Center est installée si vous prévoyez de l'utiliser pour l'administration de Kaspersky Embedded Systems Security.
\exec\ksn_en.txt	Fichier contenant la Déclaration de KSN.
\exec\license.txt	Fichier texte du Contrat de licence utilisateur final et de la politique de confidentialité de Kaspersky Embedded Systems Security.
\exec\package.kcat	Fichier contenant les signatures des fichiers du kit de distribution.
\exec\setup_ess.exe	Fichier qui lance l'assistant d'installation de Kaspersky Embedded Systems Security sur l'appareil protégé. Il lance le fichier du paquet d'installation ess_win.msi avec les paramètres d'installation définis par l'assistant.
\kvrt\KVRT.exe	Programme d'installation de Kaspersky Virus Removal Tool.
\product_long_term\cleaner_v2.cab \product_long_term\cleanerapi_v2.cab	Fichiers pour la suppression des applications incompatibles.
\product_long_term\ess.cab	Fichiers pour l'interface graphique de l'application.
\product_long_term\ess_win.kud	Fichier au format Kaspersky Unicode Definition avec la description du paquet d'installation pour l'installation à distance de l'application via Kaspersky Security Center.
\product_long_term\ess_win.msi	Paquet d'installation Windows Installer. Celui-ci installe Kaspersky Embedded Systems Security for Windows selon la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut** sur l'appareil protégé.
\product_long_term\incompatible.txt	Kaspersky ne garantit pas la compatibilité de Kaspersky Embedded Systems Security avec les applications répertoriées dans le fichier.
\product_long_term\installer.ini	Le fichier contenant les paramètres interne de la distribution.
\product_long_term\klcfginst.exe	Programme d'installation du plug-in d'administration de Kaspersky Embedded Systems Security disponible via Kaspersky Security Center. Installez le plug-in d'administration sur chaque appareil protégé sur lequel la Console d'administration de Kaspersky Security Center est installée si vous prévoyez de l'utiliser pour l'administration de Kaspersky Embedded Systems Security.
\product_long_term\ksn_en.txt	Fichier contenant la Déclaration de KSN en russe.

Fichier	Fonction
\product_long_term\license.txt	Fichier texte du Contrat de licence utilisateur final et de la politique de confidentialité de Kaspersky Embedded Systems Security.
\product_long_term\package.kcat	Fichier contenant les signatures des fichiers du kit de distribution.
\product_long_term\setup_ess.exe	Fichier qui lance l'assistant d'installation de Kaspersky Embedded Systems Security sur l'appareil protégé. Il lance le fichier du paquet d'installation ess_win.msi avec les paramètres d'installation définis par l'assistant.
\setup\images	Dossier contenant les fichiers de lancement de l'écran d'accueil de l'application.
\setup\setup.hta	Fichier de lancement de l'écran d'accueil de l'application.
\setup\SETUP_STRINGS.JS	Fichier avec les ressources de texte de l'application.

Les fichiers du kit de distribution peuvent être exécutés à partir du CD d'installation. Si vous avez préalablement copié les fichiers du paquet de distribution sur le disque local, assurez-vous que la structure des fichiers du kit de distribution a été conservée.

Configurations logicielles et matérielles

Configuration logicielle requise pour l'appareil protégé

Cet article répertorie les versions des logiciels sur lesquelles l'application a été testée et avec lesquelles son bon fonctionnement est garanti. L'application peut également fonctionner avec d'autres versions de logiciels, mais ces configurations n'ont pas fait l'objet d'un cycle de test complet et ne figurent pas dans la liste des versions dont la prise en charge est garantie.

Windows Installer 3.1 est requis pour l'installation et le fonctionnement corrects de l'application sur un appareil protégé exécutant Microsoft Windows XP.

Pour installer et utiliser Kaspersky Embedded Systems Security sur des appareils protégés avec des systèmes d'exploitation embarqués, le module Gestionnaire de filtre (Filter Manager) est requis.

Pour que Kaspersky Embedded Systems Security fonctionne correctement, la prise en charge du hachage SHA-2 dans Microsoft Windows est requise. Pour obtenir des informations détaillées, reportez-vous à la base de connaissances sur le site Internet du Support technique.

Vous pouvez installer Kaspersky Embedded Systems Security sur un appareil exécutant l'un des systèmes d'exploitation Microsoft Windows 32 bits ou 64 bits suivants :

Postes de travail :

- Windows XP Professionnel SP2 32 bits/64 bits
- Windows XP Professionnel SP2 32 bits

- Windows Vista SP2 32 32 bits/64 bits
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32 bits/64 bits
- Windows 8 Pro / Enterprise 32 bits/64 bits
- Windows 8.1 Pro / Enterprise 32 bits/64 bits
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 bits/64 bits
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 bits

Systèmes d'exploitation du serveur :

- Windows Serveur 2003 SP1 Standard/Entreprise 32 bits/64 bits
- Windows Serveur 2003 SP2 Standard/Entreprise 32 bits/64 bits
- Windows Serveur 2003 R2 SP2 Standard/Entreprise 64 bits

- Windows Serveur 2008 SP2 Standard/Entreprise 32 bits/64 bits
- Windows Server 2008 R2 SP2 Foundation/Standard/Enterprise 64 bits

Systèmes embarqués :

- Windows XP Embedded Service Pack 3 32 bits
- Windows Embedded POSReady 7 32 bits/64 bits
- Windows Embedded Standard 7 Service Pack 1 32 bits/64 bits
- Windows Embedded 8 Standard 32 bits/64 bits
- Windows Embedded 8.1 Industry Pro 32 bits/64 bits
- Windows 10 IoT Enterprise Version 1507 32 bits/64 bits
- Windows 10 IoT Enterprise Version 1607 32 bits/64 bits
- Windows 10 IoT Enterprise Version 1803 32 bits/64 bits
- Windows 10 IoT Enterprise Version 1809 32 bits/64 bits
- Windows 10 IoT Enterprise Version 1909 32 bits/64 bits
- Windows 10 IoT Enterprise Version 21H2 32 bits/64 bits
- Windows 10 IoT Enterprise Version 22H2 32 bits/64 bits
- Windows 11 IoT Enterprise Version 21H2 64 bits
- Windows 11 IoT Enterprise Version 22H2 64 bits
- Windows 11 IoT Enterprise Version 23H2 64 bits
- Windows 11 IoT Enterprise Version 24H2 64 bits
- Windows 11 IoT Enterprise Version 25H2 64 bits

Configuration matérielle requise pour l'appareil protégé

Configuration matérielle requise pour l'appareil protégé

Type de système d'exploitation	Nom du système d'exploitation	Exigences minimales	Exigences recommandées

Postes de travail	Windows XP x86 / x64	• Processeur : processeur monocœur Pentium III (x32), Pentium IV (x64) de 1.4 GHz
		• Mémoire vive :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 256 Mo
		  • Pour installer tous les modules de l'application : 512 Mo.
		• Espace disque libre :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 50 Mo
		  • Pour installer tous les modules de l'application : 2 Go.
			• Processeur : quadricœur 2,4 GHz
			• Mémoire vive : 2 Go
			• Espace disque libre :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.

	Windows 7 / 8 / 10 x86	• Processeur : processeur monocœur Pentium III (x32), Pentium IV (x64) de 1.4 GHz
		• Mémoire vive :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 256 Mo
		  • Pour installer tous les modules de l'application : 1 Go.
		• Espace disque libre :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 50 Mo
		  • Pour installer tous les modules de l'application : 2 Go.
			• Processeur : quadricœur 2,4 GHz
			• Mémoire vive : 2 Go
			• Espace disque libre :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.

	Windows 7 / 8 / 10 / 11 x64	• Processeur : processeur monocœur Pentium IV (x64) de 1.4 GHz
		• Mémoire vive :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 256 Mo
		  • Pour installer tous les modules de l'application : 1 Go.
		• Espace disque libre :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 50 Mo
		  • Pour installer tous les modules de l'application : 2 Go.
			• Processeur : quadricœur 2,4 GHz
			• Mémoire vive :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.
			• Espace disque libre :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.

Type de système d'exploitation	Nom du système d'exploitation	Exigences minimales	Exigences recommandées

Systèmes embarqués	Windows XP Embedded	• Processeur : processeur monocœur Pentium III (x32), Pentium IV (x64) de 1.4 GHz
		• Mémoire vive :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 256 Mo
		  • Pour installer tous les modules de l'application : 512 Mo.
		Espace disque libre :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 50 Mo
		  • Pour installer tous les modules de l'application : 2 Go.
			• Processeur : quadricœur 2,4 GHz
			• Mémoire vive : 2 Go
			• Espace disque libre :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.

	Windows 7 / 8 Embedded
	Windows 10 / 11 IoT
		• Processeur : processeur monocœur Pentium IV (x64) de 1.4 GHz
		• Mémoire vive : 256 Mo
		• Espace disque libre :
		  • Pour installer uniquement le module Contrôle du lancement des applications : 50 Mo
		  • Pour installer tous les modules de l'application : 2 Go.
			• Processeur : quadricœur 2,4 GHz
			• Mémoire vive : 2 Go
			• Espace disque libre :
			  • Pour installer uniquement le module Contrôle du lancement des applications : 2 Go
			  • Pour installer tous les modules de l'application : 4 Go.

Versions de Kaspersky Security Center prises en charge

Kaspersky Embedded Systems Security est compatible avec les versions suivantes de Kaspersky Security Center :

- Versions 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3 et 17.0 de Kaspersky Security Center Linux. L'administration de Kaspersky Embedded Systems Security est prise en charge via Kaspersky Security Center Web Console.
- Versions 14.2 et 15.1 de Kaspersky Security Center Windows. L'administration de Kaspersky Embedded Systems Security est prise en charge via la Console d'administration de Kaspersky Security Center et via Kaspersky Security Center Web Console.
- Versions 10.5 et 11 de Kaspersky Security Center Windows. L'administration de Kaspersky Embedded Systems Security installé sur des appareils exécutant le système d'exploitation Microsoft Windows XP SP2 est prise en charge via la Console d'administration de Kaspersky Security Center et via Kaspersky Security Center Web Console.

Pour gérer Kaspersky Embedded Systems Security via Kaspersky Security Center, l'Agent d'administration de Kaspersky Security Center est requis.

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

Exigences fonctionnelles et restrictions

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

Installation et suppression de l'application

- Pour que Kaspersky Embedded Systems Security fonctionne correctement, la prise en charge du hachage SHA-2 dans Microsoft Windows est requise.
- Lors de l'installation de l'application, un avertissement peut s'afficher à l'écran si le chemin d'accès au dossier d'installation saisi de Kaspersky Embedded Systems Security contient plus de 150 caractères. L'avertissement n'affecte pas le processus d'installation : vous pouvez installer et exécuter Kaspersky Embedded Systems Security.
- Si vous souhaitez installer le module prise en charge du protocole SNMP, assurez-vous de redémarrer le service SNMP si celui-ci est en cours d'exécution.
- Si vous souhaitez installer et exécuter Kaspersky Embedded Systems Security sur un appareil fonctionnant sous un système d'exploitation embarqué, assurez-vous d'installer le module Gestionnaire de filtre.
- Vous ne pouvez pas installer les Outils d'administration via les stratégies de groupe Microsoft Active Directory®.
- Si vous excluez le nœud Protection antivirus de la liste des modules d'application installés, ce nœud disparaît de la liste des modules disponibles une fois l'installation terminée. Pour installer les modules du nœud Endpoint Protection, lancez l'Assistant d'installation depuis le paquet d'installation, car celui-ci contient une liste complète des modules.
- Si la Console d'administration de Kaspersky Embedded Systems Security est installée, l'Assistant d'installation peut vous inviter à redémarrer l'ordinateur. Dans ce cas, le redémarrage n'est pas obligatoire. Il suffit de fermer la session de l'utilisateur qui a installé la Console d'Administration et de se connecter à nouveau au système.
- Lors de l'installation de l'application sur un appareil fonctionnant sous Windows XP ou Windows Vista, il peut être nécessaire d'installer le certificat DigiCert Assured ID Root CA pour activer la vérification de la signature du pilote. Le cas échéant, ce certificat sera installé automatiquement dans le stockage de certificats racine de confiance du système d'exploitation à partir du paquet d'installation de l'application.
- Lors de l'installation de l'application sur des appareils fonctionnant sous Windows XP ou Windows Vista, il faut vérifier si le certificat DigiCert High Assurance EV Root CA. est présent.

  Si ce certificat racine n'est pas installé, l'application peut ne pas fonctionner correctement. Nous vous recommandons d'installer le certificat dès que possible.
- L'installation de l'application se termine par une erreur si le chemin d'accès au dossier d'installation est identique au chemin d'accès d'au moins un des dossiers suivants : dossier des bases de données de l'application, dossier de la Sauvegarde, dossier pour la restauration des objets de la Quarantaine, dossier des fichiers temporaires.
- Si vous gérez Kaspersky Embedded Systems Security à l'aide de Kaspersky Security Center Cloud Console, la mise à jour de l'application localement n'est pas autorisée. Lors de la mise à jour de l'application localement, il n'est pas possible d'accepter l'accord relatif au traitement des données pour Kaspersky Security Center Cloud Console.

Contrôle de l'intégrité du système

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

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

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

L'application exclut les dossiers du niveau supérieur.

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

Pare-feu

- Vous devez indiquer plusieurs adresses. Sinon, l'utilisation avec IPv6 n'est pas disponible.
- Les règles prédéfinies du Pare-feu prennent en charge des scénarios d'interaction de base entre les appareils protégés et le Serveur d'administration. Pour exploiter totalement les fonctions de Kaspersky Security Center, il faut configurer les règles de port. Vous trouverez les informations relatives aux numéros de port, aux protocoles et à leurs fonctions dans la Base de connaissances de Kaspersky Security Center.
- Une fois l'application installée et les règles du pare-feu configurées, l'application surveille les modifications apportées aux règles et aux groupes de règles du pare-feu Windows lorsque le module Pare-feu est en cours d'exécution. Pour mettre à jour l'état et ajouter les règles de pare-feu Windows nécessaires, redémarrez le module Pare-feu.
- Lorsque vous démarrez le module Pare-feu, les règles de refus et les règles qui contrôlent le trafic sortant sont automatiquement supprimées des paramètres du pare-feu Windows.
- Les caractères `*` et `?` ne peuvent pas être utilisés dans le chemin d'accès à l'application ni dans le nom de la règle du pare-feu pour les applications.
- Si le mode *Observer l'état du pare-feu Windows* est sélectionné, les paramètres du Pare-feu Windows (**Paramètres → Mise à jour et sécurité → Sécurité Windows → Pare-feu et protection du réseau**) indiqueront que le Pare-feu de Kaspersky Embedded Systems Security est désactivé. Si vous cliquez sur le bouton d'activation du Pare-feu, son mode de fonctionnement devient *Bloquer*.
- Sur les ordinateurs fonctionnant sous Windows 7 et Windows Server 2008 R2, les règles de pare-feu configurées pour le service TermService sur la base du nom du service ne restreignent pas l'accès via RDP.
- Lorsque le pare-feu est exécuté en mode **Bloquer**, l'application empêche l'obtention d'une adresse IP depuis le serveur DHCP. Pour obtenir une adresse IP, il faut configurer le pare-feu de manière à autoriser le processus système svchost.exe.

Limitations des versions obsolètes de Windows

- La version Windows XP SP2 ne permet pas de bloquer les appareils distants et de configurer les paramètres de la liste des sessions réseau bloquées. Dans cette version de Windows, l'option **Bloquer l'accès aux ressources réseau partagées pour les sessions qui affichent une activité malveillante** est inactive.

- Installation de Kaspersky Embedded Systems Security :

  - Sur les ordinateurs fonctionnant sous Windows XP SP2 Professionnel (32 bits / 64 bits), Windows Server 2003 et Windows Server 2003 R2, il est nécessaire d'utiliser le kit de distribution de l'application ou de placer le fichier exécutable setup.exe provenant du paquet d'installation standard « Kaspersky Security Center 10.5 Network Agent for Windows XP » dans le dossier du paquet d'installation de l'application au sein de Kaspersky Security Center.

  - Sur les ordinateurs fonctionnant sous Windows XP SP3 Professionnel (32 bits) et Windows XP Embedded SP3 (32 bits), il est nécessaire d'utiliser le kit de distribution de l'application ou de placer le fichier exécutable setup.exe provenant du paquet d'installation de l'application créé dans la version 14 de Kaspersky Security Center ou du paquet d'installation standard « Kaspersky Security Center 14 Network Agent for Windows XP » dans le dossier du paquet d'installation de l'application au sein de Kaspersky Security Center.

  Comment extraire le fichier setup.exe du paquet d'installation standard de Kaspersky Security Center

  1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Avancé** → **Installation à distance** → **Paquets d'installation**.

  2. Dans l'espace de travail, cliquez sur **Actions supplémentaires** et sélectionnez **Consulter les versions actuelles des applications Kaspersky** dans la liste déroulante.

  3. Sélectionnez l'application nécessaire dans la liste. Par exemple, Kaspersky Security Center 10.5 Network Agent for Windows XP.

  4. Cliquez sur le bouton **Télécharger et créer le paquet d'installation**.

     Le paquet d'installation créé s'affichera dans la liste **Paquets d'installation**.

  5. Ouvrez les propriétés du paquet d'installation créé.

  6. Dans la section **Général**, copiez le chemin d'accès au dossier du paquet d'installation.

  7. Ouvrez le dossier du paquet d'installation.

  8. Copiez le fichier setup.exe.

- Pour gérer Kaspersky Embedded Systems Security via Kaspersky Security Center, procédez comme suit :

  - sur un ordinateur exécutant Windows XP SP2 Professionnel (32 bits/64 bits), Windows Server 2003 ou Windows Server 2003 R2, vous devez utiliser l'Agent d'administration de Kaspersky Security Center (klnagent) version 10.5.1781.

  - sur un ordinateur exécutant Windows XP SP3 Professionnel (32 bits) et Windows XP Embedded SP3 (32 bits), vous devez utiliser l'Agent d'administration de Kaspersky Security Center (klnagent) version 14.0.0.20023.

- Sur les ordinateurs Windows XP, il est impossible d'envoyer des données télémétriques à une diode de données via le protocole MQTT.

Intégration avec Kaspersky Security Center

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

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

- L'Agent d'administration 10.5 n'envoie pas d'informations sur les modules installés au Serveur d'administration de Kaspersky Security Center. Pour cette raison, dans la Console d'administration de Kaspersky Security Center et dans Kaspersky Security Center Web Console, les paramètres d'un appareil avec l'Agent d'administration 10.5 n'affichent pas les modules installés de Kaspersky Embedded Systems Security ni leurs paramètres.

- Si l'Agent d'administration de Kaspersky Security Center 10.5 est installé sur l'appareil, vous ne pouvez pas utiliser Kaspersky Security Center Web Console pour télécharger des fichiers dans la Sauvegarde.

- Si Kaspersky Embedded Systems Security est installé avec un mode de faible consommation de ressources activé pour l'Agent d'administration de Kaspersky Security Center (par défaut, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) et si l'Agent d'administration est ensuite installé, Kaspersky Embedded Systems Security ne crée pas d'exclusion pour l'Agent d'administration dans le Pare-feu Windows, ce dernier bloquant donc l'Agent d'administration.

- Si Kaspersky Embedded Systems Security est installé avec un mode de faible consommation de ressources activé pour l'Agent d'administration de Kaspersky Security Center (par défaut, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`), les modifications apportées aux listes de réseaux sont répercutées dans la Console d'administration de Kaspersky Security Center dans un délai d'environ 10 minutes.

- Lors de la recherche d'appareils administrés dans la Console d'administration de Kaspersky Security Center, l'onglet **Modules de l'application** peut afficher simultanément plusieurs variantes du nom d'un même module d'application, y compris les noms correspondant à d'anciennes versions de Kaspersky Embedded Systems Security. Les noms de certains modules peuvent également être en double.

  Pour la recherche par module, il suffit de sélectionner une des variantes présentées. Pour plus de détails sur la recherche d'appareils, consultez l'aide de Kaspersky Security Center.

Autres restrictions

Analyse à la demande et Protection des fichiers en temps réel

- L'analyse des appareils MTP connectés n'est pas disponible.
- L'analyse des archives n'est pas disponible sans l'analyse des archives SFX : si l'analyse des archives est activée dans les paramètres de protection de Kaspersky Embedded Systems Security, l'application analyse automatiquement les objets dans les archives et les archives SFX. L'analyse des archives SFX est disponible sans l'analyse des archives.
- Si les cases **Analyse approfondie du lancement de processus (le lancement de processus est bloqué pendant la durée de l'analyse)** et **Utilisation de KSN** sont cochées simultanément, tout processus lancé qui reçoit une adresse Internet comme argument sera bloqué, même si le mode "Informer" a été choisi. Pour éviter de bloquer le processus, veuillez choisir l'une des options suivantes :
  - Désactivez **Utilisation de KSN**.
  - Décochez la case **Analyse approfondie du lancement de processus (le lancement de processus est bloqué pendant la durée de l'analyse)**.

  Option recommandée : décochez la case **Analyse approfondie du lancement de processus (le lancement de processus est bloqué pendant la durée de l'analyse)**.

Licence

- Vous ne pouvez pas activer l'application avec une clé via l'Assistant d'installation si la clé a été créée à l'aide de la commande SUBST ou si le chemin d'accès au fichier clé est un chemin de réseau.
- Si vous prévoyez d'utiliser un serveur proxy de Kaspersky Security Center pour activer le produit sur un appareil client, désactivez l'optimisation VDI sur cet appareil lors de l'installation de l'Agent d'administration de Kaspersky Security Center.

Mise à jour

- Lors de l'installation et de la désinstallation des correctifs de Kaspersky Embedded Systems Security sur les appareils Windows XP, il peut être nécessaire de redémarrer l'appareil en raison des particularités de ce système d'exploitation.
- Par défaut, l'icône de l'application est masquée après l'installation des mises à jour critiques des modules Kaspersky Embedded Systems Security.

- KLRAMDISK n'est pas pris en charge sur les appareils protégés exécutant Windows XP ou Windows Server® 2003.

- Si l'installation du correctif de Kaspersky Embedded Systems Security échoue, le correctif est annulé, et vous êtes invité à redémarrer votre système d'exploitation.

Interface

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

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

- Dans la Console de l'application, dans la section **Serveurs de collecte de télémétrie**, l'heure à laquelle l'exécution des tâches est planifiée ne s'affiche pas. La colonne **Heure de lancement** est vide.

- Les fenêtres contextuelles pour les éléments de texte de l'interface dépassant 256 caractères ne s'affichent pas dans la Console d'administration de Kaspersky Security Center ni dans la Console de l'application.

- Dans la Console d'administration de Kaspersky Security Center, la fenêtre **Sélectionner un utilisateur ou un groupe d'utilisateurs** n'affiche que les 50 000 premiers utilisateurs de la liste des utilisateurs de Kaspersky Security Center. Consultez l'aide de Kaspersky Security Center pour plus de détails.

Sécurité

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

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

Protection contre les Exploits

- La Protection contre les Exploits n'est pas disponible si les bibliothèques apphelp.dll ne sont pas chargées dans la configuration d'environnement actuelle.
- Le module Protection contre les Exploits n'est pas compatible avec l'utilitaire EMET de Microsoft sur les appareils protégés exécutant le système d'exploitation Microsoft Windows 10. Kaspersky Embedded Systems Security bloque EMET si le module Protection contre les Exploits est installé sur un appareil protégé avec l'utilitaire EMET installé.
- Le module Protection contre les Exploits est incompatible avec le moteur de base de données SQL Server® 2012. Si vous installez Kaspersky Embedded Systems Security sur l'ordinateur doté de MS SQL Server 2012, vous devez ajouter la bibliothèque sqlos.dll du serveur de base de données à la liste des exclusions dans la tâche Protection contre les Exploits.

Detection and Response

- Si au cours du processus de réponse aux menaces, une erreur d'accès au dossier partagé se produit, cette erreur n'est pas répercutée dans l'historique des réponses aux menaces (Kaspersky Security Center Web Console → propriétés de l'hôte où l'application est installée → section **Detection and Response** – **Historique des réponses**).

Configuration de l'événement

Les paramètres de l'événement *Opération sur les fichiers non contrôlée dans la zone contrôlée* qui peuvent être configurés dans la section **Configuration de l'événement** de la stratégie Kaspersky Security Center sont également appliquées aux événements suivants :

- *Opération sur un fichier autorisée dans une zone contrôlée par un utilisateur de confiance*.
- *Opération sur les fichiers interdite dans la zone de contrôle*.
- *Statistiques uniquement : opération sur les fichiers interdite dans la zone de contrôle*.
- *Opération sur les fichiers non contrôlée dans la zone contrôlée*.

Interface de diagnostic compacte

Sur les ordinateurs Windows XP, l'Interface de diagnostic compacte requiert le fonctionnement du service Terminal.

Travailler en mode sans échec sous Windows

L'application ne peut pas fonctionner en mode Windows Safe Mode.

Compatibilité avec d'autres applications

Kaspersky Embedded Systems Security est incompatible avec les applications qui font partie de systèmes tiers de protection des terminaux (plateforme de protection des terminaux, PPE). Kaspersky Embedded Systems Security peut également être incompatible avec d'autres applications et certaines applications Kaspersky. Pour déterminer la compatibilité, Kaspersky Embedded Systems Security se base sur une liste de logiciels établie par Kaspersky. Cette liste est contenue dans le fichier incompatible.txt. Ce fichier est inclus dans le kit de distribution.

Si une application de la liste incompatible.txt est détectée, le programme d'installation interrompt l'installation de Kaspersky Embedded Systems Security. Vous devez supprimer l'application antivirus tierce. Il se peut que le programme d'installation supprime automatiquement certaines applications de la liste.

Si le pare-feu Windows est installé sur l'ordinateur, le programme d'installation le désactive pour procéder à l'installation de Kaspersky Embedded Systems Security.

Si, malgré les risques, vous devez installer Kaspersky Embedded Systems Security avec une application de la liste incompatible.txt, vous pouvez ignorer la vérification des applications antivirus tierces installées. Pour ce faire, lors de l'exécution de l'installateur, définissez les paramètres suivants : `SKIPPRODUCTCHECK=1` et `SKIPPRODUCTUNINSTALL=1`.

Exemple :

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

Installation et suppression de l'application

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

Planification de l'installation

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

Si vous installez Kaspersky Embedded Systems Security après la désinstallation de Kaspersky Industrial CyberSecurity for Nodes ou de Kaspersky Endpoint Security for Windows, vous devez redémarrer l'ordinateur.

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

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

Sélection des outils d'administration

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

Console de Kaspersky Embedded Systems Security

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

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

Utilitaire de la ligne de commande

Vous pouvez administrer Kaspersky Embedded Systems Security via la ligne de commande de l'appareil protégé.

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

Kaspersky Security Center

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

Il faudra installer les modules suivants :

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

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

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

Sélection du type d'installation

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

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

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

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

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

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

Lancement de l'Assistant d'installation

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

- Les modules de Kaspersky Embedded Systems Security sur l'appareil protégé, en cliquant sur le lien dans l'application de bienvenue, qui peut être lancée en ouvrant le fichier setupui.exe ou en utilisant directement le fichier \exec\setup_ess.exe du kit de distribution.
- Kaspersky Embedded Systems Security Console sur l'appareil protégé ou sur un autre appareil du LAN, en cliquant sur le lien dans l'application de bienvenue, qui peut être lancée en ouvrant le fichier \console\setup_esstools.exe ou en utilisant directement le fichier \console\setup.exe du kit de distribution.

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

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

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

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

Installation centralisée via Kaspersky Security Center

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

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

Installation centralisée via les stratégies de groupe Active Directory

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

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

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

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

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

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

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

Pour installer et utiliser Kaspersky Embedded Systems Security :

1. Installez Kaspersky Embedded Systems Security sur l'appareil protégé.
2. Installez la Console de l'application sur les appareils à partir desquels vous souhaitez administrer Kaspersky Embedded Systems Security.
3. Si la Console de l'application a été installée sur un appareil du réseau autre que l'appareil protégé, effectuez une configuration complémentaire afin que les utilisateurs de la Console de l'application puissent administrer Kaspersky Embedded Systems Security à distance.
4. Effectuez les actions requises après l'installation de Kaspersky Embedded Systems Security.

Installation de Kaspersky Embedded Systems Security

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

1. Assurez-vous qu'aucune autre application antivirus n'est installée sur l'appareil protégé. Vous devez supprimer Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition. Il n'est pas nécessaire de supprimer Kaspersky Security 10 for Windows Server pour installer Kaspersky Embedded Systems Security.
2. Assurez-vous que le compte utilisateur sous lequel l'Assistant d'installation est exécuté appartient au groupe des administrateurs sur l'appareil protégé.

Kaspersky Embedded Systems Security inclut les configurations prédéfinies suivantes :

Protéger l'ordinateur à l'aide de la technologie Interdire par défaut

Les modules permettant les mises à jour ne sont pas inclus dans la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut**.

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

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

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

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

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

Protéger l'ordinateur à l'aide des bases antivirus

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

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

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

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

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

1. Exécutez le fichier setupui.exe sur l'appareil protégé.
2. Dans la fenêtre qui s'ouvre, dans la section **Installation**, cliquez sur le lien **Protéger l'ordinateur avec la technologie d'interdiction par défaut** ou sur le lien **Protéger l'ordinateur avec des bases antivirus**.
3. Dans la fenêtre d'accueil de l'Assistant d'installation de Kaspersky Embedded Systems Security, appuyez sur le bouton **Suivant >**.

   La fenêtre **Contrat de licence utilisateur final** s'ouvre.
4. Révisez le Contrat de licence et la Politique de confidentialité.
5. Si vous acceptez les termes et conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **J'affirme que j'ai lu les termes et conditions de ces Contrats de licence utilisateur final dans leur intégralité, que je les ai compris et que je les accepte** et **Je comprends et j'accepte que mes données peuvent être traitées et transmises (y compris vers des pays tiers) dans le respect de la "Politique de confidentialité". Je confirme avoir lu et compris l'intégralité de la Politique de confidentialité**.

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

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

   Sélectionnez les modules que vous souhaitez installer.

   Le module Prise en charge du protocole SNMP de Kaspersky Embedded Systems Security apparaît dans la liste des modules à installer uniquement si le service SNMP Microsoft Windows est installé sur l'appareil protégé.
7. Pour annuler toutes les modifications, cliquez sur, cliquez sur le bouton **Réinitialiser** dans la fenêtre **Installation personnalisée**. Cliquez sur **Suivant >**.
8. Dans la fenêtre **Sélection du dossier d'installation de l'application**, réalisez une des opérations suivantes :

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

   Cliquez sur **Suivant >**.
9. Dans la fenêtre **Configurer**, vous pouvez exclure des objets et des dossiers de la zone de protection et configurer la Protection des fichiers en temps réel.
10. Dans la fenêtre **Importer les paramètres d'un fichier de configuration**, indiquez le chemin d'accès au fichier de configuration si vous souhaitez importer les paramètres de Kaspersky Embedded Systems Security à partir d'un fichier de configuration existant créé dans une version précédente de l'application.

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

    - Si vous souhaitez activer l'application, sélectionnez un fichier clé de Kaspersky Embedded Systems Security.
    - Si vous souhaitez activer l'application plus tard, cliquez sur le bouton **Suivant >**.
    - Si vous aviez déjà enregistré un fichier clé dans le dossier \exec du kit de distribution, le nom de ce fichier s'affiche dans le champ **Clé**.
    - Si vous souhaitez ajouter une licence à l'aide d'un fichier clé qui se trouve dans un autre dossier, spécifiez le fichier clé.

      L'Assistant d'installation ne permet pas d'activer l'application à l'aide d'un code d'activation. Si vous souhaitez activer l'application à l'aide d'un code d'activation, vous pouvez en définir un après l'installation de l'application.

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

      Cliquez sur **Suivant >** pour ajouter le fichier clé à l'application.

12. Si nécessaire, dans la section **Paramètres d'accès à distance**, modifiez les numéros de port TCP que la Console de l'application utilise pour la connexion à distance à l'ordinateur sur lequel l'application est installée.

    Le numéro de port par défaut pour la connexion avec les informations d'identification Windows est 13032, et le numéro de port par défaut pour la connexion avec les informations d'identification des utilisateurs créés manuellement est 13031. Plage de numéros de port possibles : 1–65535.

    Pour interdire la connexion avec les identifiants des comptes utilisateurs créés manuellement, décochez la case **Utilisation des identifiants d'utilisateurs créés manuellement**.

13. Dans la fenêtre **Préparation de l'installation de l'application**, vous pouvez désactiver l'option **Protéger le processus d'installation** si nécessaire. La protection de l'installation comprend la protection contre la substitution du paquet de distribution par des programmes malveillants, le blocage de l'accès au dossier de l'installation de Kaspersky Embedded Systems Security et le blocage de l'accès à la section du registre système contenant les clés de l'application. Il est conseillé de désactiver la protection du processus d'installation s'il est impossible autrement d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop).

14. Si nécessaire, ajoutez le chemin d'accès au fichier kavshell.exe à la variable système %PATH% pour une utilisation pratique de l'interface de la ligne de commande.

15. Cliquez sur **Installer**.

16. La fenêtre **Fin de l'installation** s'ouvre à la fin de l'installation.

17. Cliquez sur le bouton **Terminer**.

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

Installation de la console de Kaspersky Embedded Systems Security

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

Pour installer la Console de l'application :

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

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

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

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

   La fenêtre d'accueil de l'Assistant d'installation s'ouvre. Cliquez sur **Suivant >**.

4. Si vous acceptez les termes et conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **J'affirme que j'ai lu les termes et conditions de ces Contrats de licence utilisateur final dans leur intégralité, que je les ai compris et que je les accepte** et **Je comprends et j'accepte que mes données peuvent être traitées et transmises (y compris vers des pays tiers) dans le respect de la "Politique de confidentialité". Je confirme avoir lu et compris l'intégralité de la Politique de confidentialité**. Cliquez sur **Suivant >**.

5. Spécifiez le dossier dans lequel les fichiers en cours d'installation doivent être enregistrés dans la fenêtre **Sélection du dossier d'installation de l'application**.

6. Cliquez sur **Suivant >**.

7. Cliquez sur le bouton **Installer** dans la fenêtre **Préparation de l'installation de l'application**.

   L'Assistant lance l'installation des modules sélectionnés.

8. Cliquez sur **Terminer**.

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

Si vous avez installé la Console de l'application sur un appareil du réseau autre que l'appareil protégé, configurez les paramètres avancés.

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

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

- Utilisez un compte utilisateur autorisé à se connecter à distance dans les paramètres de l'application. Par défaut, tous les utilisateurs des groupes Administrateurs et Administrateurs ESS disposent de cette autorisation.

- Sur l'appareil distant, dans les paramètres du pare-feu Windows, ouvrez le port TCP 13032 pour la connexion par les comptes utilisateurs du système Windows et le port TCP 13031 pour la connexion par les comptes utilisateurs créés manuellement dans les paramètres de l'application. Autorisez également les connexions réseau pour le fichier exécutable du processus de gestion à distance Kaspersky Embedded Systems Security, avp.exe. Vous pouvez gérer ce paramètre à l'aide de l'option `ADDWFEXCLUSION=1` lors de l'installation de l'application à l'aide de la ligne de commande.

Si vous devez exécuter Kaspersky Embedded Systems Security à distance, procédez également comme suit :

Le compte utilisateur qui lancera l'application à distance doit faire partie du groupe Administrateurs.

- Sur l'appareil distant, dans les paramètres du pare-feu Windows, activez la règle **Partage de fichiers et d'imprimantes (SMB-In)** (port TCP 445). Nous vous recommandons également d'ouvrir le port TCP 135 pour faciliter la connexion à l'appareil.

- Pour les appareils distants fonctionnant sous Windows Vista ou une version ultérieure qui ne font pas partie d'un domaine ou qui sont gérés par un compte utilisateur local, **désactivez le contrôle à distance des comptes utilisateurs (UAC)**.

  1. Ouvrez l'éditeur du registre sur l'ordinateur.

  2. Dans l'éditeur du registre, ouvrez la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

  3. Ouvrez la valeur LocalAccountTokenFilterPolicy.

     Si la valeur LocalAccountTokenFilterPolicy est manquante sous cette clé, créez une valeur DWORD (32 bits) portant ce nom (cf. site de l'assistance technique de Microsoft).

  4. Définissez la valeur `1` et cliquez sur le bouton **OK**.

     La désactivation du contrôle de compte d'utilisateur à distance est sans incidence sur le contrôle de compte d'utilisateur local.

- Si l'appareil sur lequel la Console des applications est installée ou l'appareil protégé fonctionne sous Windows 8.1 ou une version antérieure de Windows, **activez la prise en charge de l'accès partagé aux fichiers SMB 1.0/CIFS sur les appareils fonctionnant sous Windows 10 ou une version ultérieure**.
  - Dans l'application « Fonctionnalités Windows » :
    1. Sélectionnez **Démarrer** → **Panneau de configuration** → **Programmes et fonctionnalités** → **Activer ou désactiver les fonctionnalités Windows**.
    2. Dans la fenêtre **Fonctionnalités Windows**, cochez la case **Prise en charge du partage de fichiers SMB 1.0/CIFS**.
    3. Cliquez sur le bouton **OK**.
  - Dans Windows PowerShell :
    1. Exécutez Windows PowerShell en tant qu'administrateur.
    2. Exécutez la commande :

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

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

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

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

Les nouvelles valeurs des paramètres de connexion seront appliquées.

Autorisation de l'accès à distance anonyme aux applications COM

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

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

1. Sur l'appareil distant sur lequel la console de Kaspersky Embedded Systems Security est installée, ouvrez la console du **Service des modules**. Pour ce faire, procédez comme suit :

   a. Choisissez **Démarrer** → **Exécuter**.

   b. Exécutez la commande:

   ```
   dcomcnfg
   ```

   c. La console **Services des modules** s'ouvre.

2. Dans la console du **Service des modules** de votre appareil protégé, développez le nœud **Ordinateurs**.

3. Ouvrez le menu contextuel du nœud **Poste de travail**.

4. Choisissez l'option **Propriétés**.

5. Sous l'onglet Sécurité COM de la fenêtre **Propriétés**, cliquez sur le bouton **Modifier les limites** du groupe de paramètres **Autorisations d'accès**.

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

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

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

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

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

1. Sur l'appareil distant, fermez la console de Kaspersky Embedded Systems Security.

2. Réalisez une des opérations suivantes :

   - Dans Microsoft Windows XP SP2 et suivants :

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

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

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

     d. Sélectionnez le protocole **TCP**.

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

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

- Dans Microsoft Windows 7 et suivants :

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

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

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

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

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

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

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

Kaspersky Embedded Systems Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si la case **Activer la Protection des fichiers en temps réel après l'installation de l'application (recommandé)** est cochée lors de l'installation de Kaspersky Embedded Systems Security, l'application analyse les objets du système de fichiers de l'appareil lorsqu'ils sont consultés. Si le module Surveillance des scripts a été installé dans le cadre d'une installation personnalisée, Kaspersky Embedded Systems Security analyse le code source de tous les scripts lorsqu'ils sont lancés. Chaque vendredi à 20h00, Kaspersky Embedded Systems Security exécute la tâche *Analyse des zones critiques*.

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

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

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

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

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

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

Lancement et configuration de la tâche Mise à jour des bases et des modules d'application

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

1. Sous *Mise à jour*, configurez la connexion à la source des mises à jour :
2. Lancer la tâche *Mise à jour*.

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

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

1. Dans la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Sélectionnez **Propriétés de l'application**.
3. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres du réseau**.
4. Dans la section **Paramètres du serveur proxy**, cliquez sur **Paramètres**, et dans la fenêtre qui s'ouvre, cochez la case **Utiliser les paramètres indiqués du serveur proxy**.
5. Saisissez l'adresse du serveur proxy dans le champ **Adresse** et saisissez le numéro de port du serveur proxy dans le champ **Port**.
6. Le cas échéant, décochez la case **Ne pas utiliser de serveur proxy pour les adresses locales**. Si la fonctionnalité est activée, les échanges avec les autres appareils du réseau auquel appartient l'appareil protégé disposant de Kaspersky Embedded Systems Security se font directement. Cette option est activée par défaut.
7. Dans la section **Paramètres d'authentification du serveur proxy**, sélectionnez la méthode d'authentification nécessaire dans la liste déroulante :
   - **Ne pas utiliser l'authentification**.
   - **Authentification NTLM**. Authentification NTLM avec le compte utilisateur actuel (par défaut).
   - **Authentification NTLM avec nom d'utilisateur et mot de passe**. Authentification NTLM avec des identifiants spécifiés manuellement.
   - **Authentification Kerberos**. Authentification Kerberos avec le compte utilisateur actuel.

     Pour garantir le bon fonctionnement de l'authentification Kerberos lorsque vous utilisez des enregistrements CNAME pour l'adresse du serveur proxy, vous devez enregistrer un Service Principal Name (SPN) pour chaque enregistrement CNAME.

   - **Authentification Kerberos avec nom d'utilisateur et mot de passe**. Authentification Kerberos avec des identifiants spécifiés manuellement.
   - **Nom d'utilisateur et mot de passe**. Authentification avec des identifiants spécifiés manuellement.

Si nécessaire, indiquez le nom d'utilisateur et le mot de passe.

Si l'authentification Kerberos est sélectionnée, Kaspersky Embedded Systems Security peut, en fonction de la configuration du serveur proxy, procéder à l'authentification selon le protocole Kerberos ou NTLM.

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

Pour lancer la tâche Mise à jour, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Mise à jour**.
2. Dans le menu contextuel du nœud enfant **Mise à jour des bases**, sélectionnez l'option **Lancement**.

La tâche *Mise à jour* est lancée.

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

Analyse rapide

Une fois que les bases de Kaspersky Embedded Systems Security ont été mises à jour, recherchez la présence éventuelle d'applications malveillantes sur l'appareil protégé à l'aide de la tâche *Analyse des zones critiques*.

Pour lancer la tâche Analyse des zones critiques, procédez comme suit :

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

La tâche est lancée et l'état **En cours** apparaît dans le panneau des résultats.

Pour consulter le journal d'exécution de la tâche,

dans le panneau des résultats du nœud **Analyse des zones critiques**, cliquez sur le lien **Ouvrir le journal des tâches**.

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

Vous pouvez ajouter ou supprimer des modules de Kaspersky Embedded Systems Security. Il faut arrêter la tâche Protection des fichiers en temps réel avant de supprimer le module Protection des fichiers en temps réel. Dans tous les autres cas, il n'est pas nécessaire d'arrêter la tâche Protection des fichiers en temps réel ou le Kaspersky Embedded Systems Security Service.

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

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

1. Dans le **Panneau de configuration** Windows, sélectionnez **Applications et fonctionnalités**. La fenêtre **Modifier ou supprimer** s'ouvre.

2. Cliquez avec le bouton droit de la souris sur **Kaspersky Embedded Systems Security** et sélectionnez **Modifier**.

   L'Assistant de configuration **Modification, restauration ou suppression de l'application** s'ouvre.

3. Sélectionnez **Modification**.

   La fenêtre **Installation personnalisée** s'ouvre. Sélectionnez **Fonctionnalité complète** et cliquez sur **Suivant >**.

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

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

     - **Le module sera installé sur un disque dur local**, si vous souhaitez installer un module ;

     - **Le module et ses sous-modules seront entièrement installés**, si vous souhaitez installer le groupe de modules ;

   - Pour supprimer un module déjà installé, cliquez sur le bouton en regard du nom du module sélectionné. Sélectionnez **Le module sera inaccessible** dans le menu contextuel.

   Cliquez sur **Suivant >**.

5. Dans la fenêtre **Préparation de l'installation de l'application**, confirmez la sélection des modules d'application en cliquant sur **Installer**.

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

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

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

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

1. Dans le **Panneau de configuration** Windows, sélectionnez **Applications et fonctionnalités**. La fenêtre **Modifier ou supprimer** s'ouvre.

2. Cliquez avec le bouton droit de la souris sur **Kaspersky Embedded Systems Security** et sélectionnez **Modifier**.

3. L'Assistant de configuration **Modification, restauration ou suppression de l'application** s'ouvre.

4. Choisissez l'option **Restauration**.

   La fenêtre **Restauration de Kaspersky Embedded Systems Security** s'ouvre. Cliquez sur **Suivant >**.

5. Attendez que l'opération de restauration se termine et, dans la fenêtre qui s'ouvre, cliquez sur **Terminer**.

Kaspersky Embedded Systems Security sera réparés conformément aux paramètres définis.

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

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

Désinstallation de Kaspersky Embedded Systems Security

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

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

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

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

La désinstallation, la réparation et l'installation de l'application ne sont pas disponibles via le panneau de configuration Windows.

Kaspersky Embedded Systems Security demande les informations d'identification du compte utilisateur lorsque celui-ci tente de supprimer ou de modifier l'ensemble des modules dans l'Assistant d'installation. Vous devez saisir les identifiants d'un utilisateur disposant des droits suffisants. Si un mot de passe Windows vide est défini pour le compte utilisateur qui effectue la suppression, désactivez la fonctionnalité **Demander un mot de passe pour confirmer les actions critiques** avant de commencer la suppression.

Pour désinstaller Kaspersky Embedded Systems Security :

1. Dans le **Panneau de configuration** Windows, sélectionnez **Applications et fonctionnalités**. La fenêtre **Modifier ou supprimer** s'ouvre.

2. Cliquez avec le bouton droit de la souris sur **Kaspersky Embedded Systems Security** et sélectionnez **Modifier**.

3. L'Assistant de configuration **Modification, restauration ou suppression de l'application** s'ouvre.

4. Sélectionnez **Suppression**.

   La fenêtre **Enregistrer les objets** s'ouvre.

5. Si nécessaire, dans la fenêtre **Enregistrer les objets**, réalisez une des opérations suivantes :

   Sous **Enregistrer les objets**, spécifiez les objets ou les paramètres que vous souhaitez conserver. Par défaut, les cases sont décochées.

   - Cochez la case **Informations sur l'activation**.
   - Cochez la case **Fichiers de la sauvegarde**.
   - Cochez la case **Paramètres de fonctionnement de l'application**.

   Sous **Exporter les objets**, spécifiez les objets que vous souhaitez exporter. Par défaut, les cases sont décochées.

   - Cochez la case **Exporter les objets de la quarantaine** pour que Kaspersky Embedded Systems Security exporte les objets qui ont été mis en quarantaine. Par défaut, la case est décochée.
   - Cochez la case **Exporter les objets de la sauvegarde** pour exporter les objets de la Sauvegarde de Kaspersky Embedded Systems Security. Par défaut, la case est décochée.
   - Cliquez sur le bouton **Enregistrer** et indiquez le dossier vers lequel vous souhaitez exporter les objets. Par défaut, les objets seront exportés vers %ProgramData%\Kaspersky Lab\KESS.4.1\QB.

     Cliquez sur **Suivant**.

6. Dans la fenêtre **Confirmation de la suppression de l'application**, confirmez la suppression en cliquant sur **Supprimer**.
7. Dans la fenêtre qui s'ouvre lorsque la désinstallation est terminée, cliquez sur le bouton **Terminer**.

Kaspersky Embedded Systems Security est désinstallé de l'appareil protégé.

Désinstallation de la console de Kaspersky Embedded Systems Security

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

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

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

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

1. Dans le **Panneau de configuration** Windows, sélectionnez **Applications et fonctionnalités**. La fenêtre **Modifier ou supprimer** s'ouvre.
2. Cliquez avec le bouton droit de la souris sur **Console de Kaspersky Embedded Systems Security** et sélectionnez **Modifier**.

   La fenêtre de l'Assistant **Modification, restauration ou suppression de l'application** s'ouvre.

3. Sélectionnez **Suppression**.

   La fenêtre **Confirmation de la suppression de l'application** s'ouvre. Cliquez sur **Désinstaller**.

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

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

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

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

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

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

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

Vous pouvez installer Kaspersky Embedded Systems Security Console sur l'appareil protégé ou sur un autre appareil du réseau afin d'utiliser l'application localement ou à distance. Pour ce faire, utilisez le paquet d'installation \client\esstools.msi.

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

Si vous exécutez le fichier \exec\ess_win.msi sur l'appareil protégé sans options de ligne de commande supplémentaires, Kaspersky Embedded Systems Security est installé avec les paramètres d'installation par défaut.

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

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

Le fichier \product_long_term\ess_win.msi est conçu pour installer la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut** de Kaspersky Embedded Systems Security, tandis que le fichier \exec\ess_win.msi est prévu pour installer la configuration **Protéger l'ordinateur avec les bases antivirus** de Kaspersky Embedded Systems Security.

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

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

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

Les modules permettant les mises à jour ne sont pas inclus dans la configuration **Protéger l'ordinateur avec la technologie d'interdiction par défaut**.

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

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

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

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

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

Le fichier \console\esstools.msi est conçu pour installer la Console de Kaspersky Embedded Systems Security.

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

Description des modules logiciels de Kaspersky Embedded Systems Security

Module	Code	Fonctions du module
Protection des fichiers en temps réel	`FileThreatProtection`	Ce module réalise les recherches de virus sur les fichiers sur l'appareil protégé lorsque ces fichiers sont sollicités.
Analyseur AMSI	`AMSI`	Ce module est prévu pour la prise en charge de l'interface Antimalware Scan Interface de Microsoft. L'interface AMSI (Antimalware Scan Interface) permet aux applications tierces compatibles avec AMSI d'envoyer des objets (par exemple, des scripts PowerShell) à Kaspersky Embedded Systems Security pour une analyse supplémentaire et de recevoir les résultats de l'analyse de ces objets.
Détection comportementale	`BehaviorDetection`	Ce module remplit la liste des hôtes bloqués avec les noms des appareils distants qui présentent une activité malveillante.
Protection contre les Exploits	`ExploitPrevention`	Ce module garantit l'administration des paramètres de la protection des processus dans la mémoire de l'appareil protégé.
Réparation des actions malicieuses	`RemediationEngine`	Ce module permet à Kaspersky Embedded Systems Security d'exécuter le retour à l'état antérieur aux actions des applications malveillantes dans le système d'exploitation.
Pare-feu	`Firewall`	Ce module permet de gérer le Pare-feu Windows via l'interface utilisateur graphique de Kaspersky Embedded Systems Security.
Protection contre les menaces réseau	`NetworkThreatProtection`	Ce module analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau ciblant votre ordinateur, Kaspersky Embedded Systems Security bloque l'activité réseau de l'ordinateur attaquant.
Contrôle du lancement des applications	`ApplicationControl`	Ce module surveille les tentatives des utilisateurs de lancer des applications et autorise ou interdit le lancement des applications conformément aux règles spécifiées du Contrôle du lancement des applications.
Contrôle des appareils	`DeviceControl`	Ce module suit les tentatives de connexion d'appareils externes à un appareil protégé et autorise ou interdit l'utilisation de ces appareils conformément aux règles de contrôle des appareils spécifiées.
Module d'intégration de l'Agent d'administration de Kaspersky Security Center	`AdminKitConnector`	Ce module assure la connexion entre Kaspersky Embedded Systems Security et l Agent d'administration de Kaspersky Security Center. Vous pouvez installer ce module sur l'appareil protégé si vous avez l'intention d'administrer l'application via Kaspersky Security Center.
Inspection des journaux	`LogInspector`	Le module contrôle l'intégrité du milieu à protéger sur la base des résultats de l'inspection des journaux des événements Windows.
Contrôle de l'intégrité du système	`SystemIntegrityMonitor`	Ce module inclut toutes les fonctionnalités du Contrôle de l'intégrité des fichiers et permet également de surveiller les modifications apportées au registre et la connexion d'appareils externes.
Protection BadUSB	`BadUSBAttackPrevention`	Le module permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier.
Managed Detection and Response	`MDR`	Ce module facilite l'interaction avec la solution Kaspersky Managed Detection and Response.

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

Cette section décrit les paramètres d'installation et de restauration de Kaspersky Embedded Systems Security. Cette section contient également les clés pour modifier les paramètres d'installation et les valeurs de clé possibles. Vous pouvez utiliser ces arguments avec les arguments standard de l'instruction `msiexec` du service Windows Installer lors de l'installation de Kaspersky Embedded Systems Security via la ligne de commande.

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

- Acceptation des conditions du Contrat de licence utilisateur final.

  `EULA=<value>` peut prendre les valeurs suivantes.

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

- Acceptation des conditions de la politique de confidentialité.

  `PRIVACYPOLICY=<value>` peut prendre les valeurs suivantes.

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

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

  La valeur par défaut de l'option de ligne de commande `INSTALLDIR=<full path to the folder>` est la suivante :

  - Pour la version 32 bits de Microsoft Windows :
    - Kaspersky Embedded Systems Security : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
    - Kaspersky Embedded Systems Security Console : %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0
  - Pour la version 64 bits de Microsoft Windows : %ProgramFiles(x86)%, de même que pour les chemins d'accès des versions 32 bits de Microsoft Windows.

- Début de la tâche *Protection des fichiers en temps réel* immédiatement après le démarrage de Kaspersky Embedded Systems Security.

  `RUNRTP=<value>` peut prendre les valeurs suivantes.

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

- Chemin d'accès au fichier clé (`LICENSEKEYPATH`). Par défaut, le programme d'installation de Windows tente de trouver le fichier avec l'extension .key dans le dossier \exec du kit de distribution. Si le dossier \exec contient plusieurs fichiers clés, le programme d'installation de Windows sélectionne le fichier clé dont la date d'expiration est la plus éloignée dans le futur. Le fichier clé peut être enregistré au préalable dans le dossier \exec ou via un autre chemin d'accès que vous pouvez spécifier sous le paramètre `LICENSEKEYPATH`.

  `LICENSEKEYPATH` peut prendre les valeurs suivantes.

  - Chemin d'accès complet au fichier clé y compris son nom.
  - Chemin d'accès au dossier où sont stockés les fichiers clés.

Vous pouvez ajouter une clé après l'installation de Kaspersky Embedded Systems Security à l'aide de l'outil d'administration que vous aurez choisi, par exemple via la console de l'application. Si vous n'ajoutez pas la clé de l'application lors de son installation, Kaspersky Embedded Systems Security ne fonctionnera pas.

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

  La valeur par défaut pour le paramètre `CONFIGPATH=<configuration file name>` n'est pas définie.

- Mode *Analyse au démarrage du système d'exploitation* (`SCANSTARTUP_BLOCKING`). Si Kaspersky Embedded Systems Security a été installé sans clé `SCANSTARTUP_BLOCKING`, le paramètre **Zone d'analyse** dans la tâche *Analyse au démarrage du système d'exploitation* est défini comme suit :

  - Actions à exécuter sur les objets infectés et autres : **Informer**.
  - Action à exécuter sur les objets probablement infectés : **Informer**.

  Si Kaspersky Embedded Systems Security a été installé avec une clé `SCANSTARTUP_BLOCKING`, le paramètre **Zone d'analyse** dans la tâche *Analyse au démarrage du système d'exploitation* est défini comme suit :

  - Actions à exécuter sur les objets infectés et autres : **Perform recommended action**.
  - Action à exécuter sur les objets probablement infectés : **Perform recommended action**.

  La tâche *Analyse au démarrage du système d'exploitation* est créée automatiquement. Le mode **Informer** est appliqué par défaut. Dans ce cas, après avoir déployé Kaspersky Embedded Systems Security sur les appareils, vous pouvez activer la tâche *Analyse au démarrage du système d'exploitation* si aucun problème avec les services système n'a été détecté lors de l'analyse. Si l'application détecte des services système critiques infectés ou des objets probablement infectés, le mode **Informer** vous donne le temps d'en trouver la raison et de résoudre le problème. Si l'application applique le mode **Perform recommended action**, l'action **Disinfect. Delete if disinfection fails** est exécutée. La désinfection ou la suppression des fichiers système peut entraîner des problèmes critiques au démarrage du système d'exploitation.

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

  Les valeurs qui peuvent être attribuées au paramètre `SKIPPRODUCTCHECK=<value>` dans la ligne de commande sont les suivantes (vous pouvez également utiliser `SKIPINCOMPATIBLESW=<value>`) :

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

- Interdiction de la suppression automatique de l'application incompatible.

  Si l'option `SKIPPRODUCTUNINSTALL=1` est spécifiée, Kaspersky Embedded Systems Security ne supprime pas les logiciels incompatibles. Si cette option n'est pas spécifiée, Kaspersky Embedded Systems Security tente automatiquement de supprimer les logiciels incompatibles.

Lors de l'installation de Kaspersky Embedded Systems Security à l'aide du programme d'installation msiexec, la suppression des logiciels incompatibles n'est pas effectuée. Pour supprimer automatiquement les logiciels qui peuvent poser des problèmes de compatibilité, utilisez le fichier setup_ess.exe.

- Désactivation de la vérification de la mise à jour KB5007186 du système d'exploitation.

  Après l'installation de la mise à jour KB5007186, l'application continue de fonctionner normalement et la sécurité du système n'est pas compromise, mais les mises à jour des versions mineures des applications deviennent impossibles. Avant d'installer l'application, le programme d'installation vérifie si des mises à jour du système d'exploitation ont été installées. Si la mise à jour KB5007186 est découverte, le programme d'installation interrompt l'installation. Vous pouvez utiliser la clé `SKIPKB5007186CHECK` sur la ligne de commande pour activer ou désactiver la vérification de la mise à jour KB5007186 du système d'exploitation.

  `SKIPKB5007186CHECK=<value>` peut prendre les valeurs suivantes.

  - `0` : le programme d'installation vérifie si la mise à jour KB5007186 du système d'exploitation est installée.
  - `1` : le programme d'installation ne vérifie pas si la mise à jour KB5007186 du système d'exploitation est installée.

  Par défaut, la clé n'est pas définie, sa valeur correspondant à 0.

- Configuration de la protection des fonctionnalités des services du système d'exploitation.

  Si cette fonction est activée, les applications tierces ne peuvent pas agir sur les processus du système d'exploitation. `PROTECTOSSERVICES=<value>` peut prendre les valeurs suivantes.

  - `1` signifie que la protection des services du système d'exploitation est activée (paramètre par défaut).
  - `0` signifie que la protection des services du système d'exploitation est désactivée.

- Configuration des ports utilisés pour la connexion à distance de la Console de l'application à l'ordinateur sur lequel l'application est installée :

  Pour configurer le port de connexion avec vos identifiants Windows, vous pouvez utiliser le paramètre `UIPORT=<port number>`. Plage de numéros de port possibles : 1–65535. Si le numéro se trouve en dehors de l'intervalle spécifié, le numéro de port par défaut est utilisé. La valeur par défaut est 13032.

  En cas de nécessité, vous pouvez fermer le port pour la connexion avec les identifiants des utilisateurs créés manuellement à l'aide du paramètre `ENABLEUIKLPORT=<value>` :

  - `1` ouvre le port (paramètre par défaut).
  - `0` ferme le port.

  La valeur par défaut pour ce port est 13031. Vous pouvez modifier le numéro de port en spécifiant le paramètre `UIKLPORT=<value>`. Plage de numéros de port possibles : 1–65535.

- Paramètre d'activation des connexions réseau pour l'administration à distance de Kaspersky Embedded Systems Security à l'aide de la Console de l'application installée sur un autre ordinateur.

ADDWFEXCLUSION=<value> peut prendre les valeurs suivantes.

- 1 Si cette valeur est définie, les ports TCP configurés pour la connexion à distance de la Console de l'application à un ordinateur sur lequel l'application est installée (les paramètres UIPORT=<value> et UIKLPORT=<value>) sont ouverts dans le Pare-feu Windows, et les connexions réseau sont autorisées pour le fichier exécutable du processus d'administration à distance de Kaspersky Embedded Systems Security, avp.exe.

  Informez-vous également sur les configurations supplémentaires lors de l'installation de l'application sur un autre appareil.

- 0 Si cette valeur est définie, rien ne se passe.

- Ignorez l'installation du certificat racine DigiCert Assured ID Root CA dans le stockage de certificats de confiance du système d'exploitation.

  Si l'option SKIPINSTALLROOTCACERTIFICATES est spécifiée lors de l'installation de l'application, le certificat racine DigiCert Assured ID Root CA n'est pas installé. Par défaut, le certificat est installé automatiquement à partir du paquet d'installation de l'application.

Paramètres de récupération et options de ligne de commande de Windows Installer

- Restauration du contenu de la quarantaine.

  RESTOREQTN=<value> peut prendre les valeurs suivantes.

  - 0 – suppression du contenu en quarantaine (valeur par défaut).

  - 1 : restaurer le contenu de la quarantaine dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \QB.

- Restauration du contenu de la Sauvegarde.

  RESTOREBCK=<value> peut prendre les valeurs suivantes.

  - 0 – suppression du contenu de la sauvegarde (valeur par défaut).

  - 1 : restaurer le contenu de la Sauvegarde dans le dossier défini par le paramètre RESTOREPATH, dans le sous-dossier \QB.

- Saisissez le mot de passe actuel pour confirmer la restauration (si la protection par mot de passe est activée).

  La valeur par défaut pour le paramètre UNLOCK_PASSWORD=<specified password> n'est pas définie.

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

  La valeur par défaut pour l'option RESTOREPATH=<full path to the folder> de la ligne de commande est %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.1.0\QB\Restored

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

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

Exécutez le fichier ess_win.msi du kit de distribution sur l'appareil protégé.

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

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

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés et sans intervention de l'utilisateur :

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

Pour installer les modules, tels que Contrôle des appareils :

```
\exec\setup_ess.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

Lors de l'installation de Kaspersky Embedded Systems Security sur des ordinateurs avec des appareils réseau et des appareils SCSI qui entraînent l'échec du système après l'installation, vous pouvez utiliser les options supplémentaires suivantes avec cette commande :

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

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

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

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

Pour installer et activer Kaspersky Embedded Systems Security à l'aide du fichier clé :

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

Pour modifier le port utilisé pour la connexion à distance de la Console de l'application à l'ordinateur sur lequel l'application est installée avec les identifiants utilisateur Windows :

```
setup_ess.exe /pUIPORT=<port number>
```

Plage de numéros de port possibles : 1–65535. La valeur par défaut est 13032.

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

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés et sans intervention de l'utilisateur :

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

Pour installer Kaspersky Embedded Systems Security selon les paramètres recommandés et afficher l'interface d'installation :

```
msiexec /i ess_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

Pour installer Kaspersky Embedded Systems Security avec les paramètres d'installation recommandés et activer la rotation des fichiers de traçage lorsque le nombre de fichiers de traçage atteint le nombre maximal indiqué :

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

Le paramètre `TRACE_FOLDER` est requis.

Les règles suivantes s'appliquent au paramètre `TRACE_MAX_ROLL_COUNT` :

- Dans le cas où ce paramètre est spécifié, la rotation des fichiers de traçage est activée lorsque le nombre de fichiers de traçage atteint le nombre maximal spécifié dans le paramètre. Plage de valeurs des paramètres disponible : de 1 à 999.
- Si le nombre maximal de fichiers de traçage est défini sur 0, la rotation des fichiers de traçage est désactivée.
- Si une valeur de paramètre a été indiquée, mais qu'elle est incorrecte ou qu'elle se trouve en dehors de la plage de valeurs disponibles (de 1 à 999), la rotation des fichiers de traçage est activée, le nombre maximal de fichiers de traçage étant défini par défaut sur 5.
- Si le paramètre n'est pas renseigné :
  - Si la rotation des fichiers de traçage est déjà configurée sur l'appareil, ses paramètres ne sont pas modifiés. L'application ignore les paramètres saisis.
  - Si la rotation des fichiers de traçage n'est pas configurée sur l'appareil, l'option de rotation est activée avec le nombre maximal de fichiers de traçage défini par défaut sur 5.

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

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

Pour installer Kaspersky Embedded Systems Security avec une analyse préalable des processus actifs et des secteurs d'amorçage des disques locaux, procédez comme suit :

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

Pour installer Kaspersky Embedded Systems Security dans le dossier d'installation C:\KESS :

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

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

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

Pour installer la Console de Kaspersky Embedded Systems Security :

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

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

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

Pour installer un correctif de l'application lorsque Kaspersky Embedded Systems Security est protégé par mot de passe :

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

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

Kaspersky Embedded Systems Security lance la tâche de protection et d'analyse juste après l'installation si vous avez activé l'application. Si la case **Activer la Protection des fichiers en temps réel après l'installation de l'application (recommandé)** est cochée lors de l'installation de Kaspersky Embedded Systems Security, l'application analyse les objets du système de fichiers de l'appareil lorsqu'ils sont consultés. Si le module Surveillance des scripts a été installé dans le cadre d'une installation personnalisée, Kaspersky Embedded Systems Security analyse le code source de tous les scripts lorsqu'ils sont lancés. Chaque vendredi à 20h00, Kaspersky Embedded Systems Security exécute la tâche *Analyse des zones critiques*.

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

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

  Par exemple, vous pouvez lancer la tâche *Mise à jour* à l'aide de la commande suivante :

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  Dans ce cas, les mises à jour des bases de données de Kaspersky Embedded Systems Security sont téléchargées depuis les serveurs de mise à jour de Kaspersky.

- Lancez la tâche *Analyse des zones critiques* si aucun logiciel antivirus avec fonction de protection des fichiers en temps réel n'était installé sur l'appareil avant l'installation de Kaspersky Embedded Systems Security.

  Vous pouvez démarrer la tâche *Analyse des zones critiques* à partir de la ligne de commande, en exécutant la commande suivante :

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

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

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

Ajout et suppression de modules. Exemples de commandes

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

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

ou

```
\exec\setup_ess.exe /s /p ADDLOCAL=Oas,Ods
```

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

Pour supprimer les modules installés, exécutez la commande suivante :

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

Pour installer de nouveaux modules, exécutez la commande suivante :

```
msiexec /i ess_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas,Ods,SnmpSupport,TrayApp,IDS,
EULA=1 PRIVACYPOLICY=1 /qn
```

Une fois que vous avez répertorié les modules que vous souhaitez installer et supprimer, Kaspersky Embedded Systems Security installe et supprime les modules correspondants.

Désinstallation de Kaspersky Embedded Systems Security. Exemples de commandes

Pour désinstaller Kaspersky Embedded Systems Security de l'appareil protégé en mode silencieux, exécutez la commande suivante :

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

ou

```
msiexec /x {6202AB29-4AC2-4A92-AF8E-977AADD4B27F} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

ou

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

où `<user name>` est le nom et l'identifiant d'un utilisateur disposant des droits suffisants pour procéder à une désinstallation.

Si un mot de passe Windows vide est défini pour le compte utilisateur qui effectue la suppression, désactivez la fonctionnalité **Demander un mot de passe pour confirmer les actions critiques** avant de commencer la suppression.

Pour désinstaller Kaspersky Embedded Systems Security Console en mode silencieux, exécutez la commande suivante :

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

ou

```
msiexec /x {E827CBBA-974C-4386-B50E-8F202D41E428} /qn
```

Codes de retour

Le programme d'installation de l'application peut renvoyer les codes de retour décrits dans cet article.

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

Codes de retour

Code	Description
27100	Des disques dotés de l'Agent d'authentification en mode de test ont été détectés sur cet ordinateur.
27101	Des disques dotés de l'Agent d'authentification en mode de test ont été détectés sur cet ordinateur.
27102	Impossible de trouver les disques chiffrés.
27200	Échec du déchargement de l'application de la mémoire vive.
27201	Erreur lors du démarrage du processus AVP.exe. Votre ordinateur est peut-être infecté.
27204	Échec de la mise en cache du paquet de distribution.
27205	Échec de la migration des informations de licence.
27206	Échec de la suppression des informations de licence.
27207	Échec de la suppression des logiciels incompatibles.
27208	Échec de la vérification des logiciels incompatibles.
27209	Échec de l'extraction des fichiers du cabinet.
27210	Échec de la configuration de l'autodéfense.
27211	Échec de l'activation de l'autodéfense.
27212	Échec de l'obtention des informations sur la version du système d'exploitation.
27213	Échec de la récupération du répertoire de démarrage.
27214	Échec de la vérification du répertoire d'installation.
27215	Échec de la configuration du service.
27216	Échec de la configuration de la mise à jour de klcp.
27217	Échec de la mise à jour de klcp.
27218	Échec de la configuration des paramètres du pilote kl1.
27219	Échec de la configuration des paramètres du pilote klelam.
27220	Échec de la configuration des paramètres du pilote klwfp.
27221	Échec de la configuration du mode de compatibilité des pilotes.
27222	Échec de la suppression de la clé du registre.
27223	Échec du redémarrage du système d'exploitation.
27224	Échec de l'installation du pilote.
27225	Échec de la migration des paramètres du pilote.
27226	Échec de l'arrêt du pilote.
27227	Échec du blocage du lancement du pilote.
27228	Échec de la vérification de la signature du fichier.
27230	Échec de la préparation des paramètres du pilote kldl.
27231	Échec de la configuration des paramètres du pilote kldl.
27300	Erreur d'installation du pilote.

Code	Description
27301	Erreur de suppression du pilote.
27302	Erreur d'installation des modules réseau.
27303	Les informations d'enregistrement du pilote sont incohérentes ou incomplètes. Veuillez redémarrer le système d'exploitation et réessayer.
27305	Erreur de désactivation du pilote.
27310	Échec de l'installation du fichier catalogue signé numériquement.
27311	Échec de la désinstallation du fichier catalogue signé numériquement.
27312	Échec de l'installation des certificats.
27313	Échec de la suppression des certificats.
27320	Échec de la configuration du service.
27321	Échec de la suppression de la protection du service.
27350	Le correctif<nom du correctif> n'est pas conçu pour la localisation de l'application <nom de l'application>.
27352	Le correctif de chiffrement du disque ne peut pas être supprimé.
27353	Le correctif <nom du correctif 1> peut être installé uniquement avec le correctif<nom du correctif 2>.
27354	Avant de modifier/restaurer l'application, il faut redémarrer l'ordinateur pour appliquer les correctifs.
27355	Échec du verrouillage de l'administration du chiffrement du disque. Échec du verrouillage de l'administration du chiffrement du disque. Vous devez terminer le chiffrement pour installer une mise à jour pour le chiffrement du disque.
27356	Impossible d'installer le correctif.
27357	Il s'est avéré que le paquet d'installation contient les correctifs rappelés. L'installation sera interrompue.
27360	Le correctif ne peut pas être enregistré.
27361	Échec de la définition des paramètres d'installation du correctif.
27363	Le correctif contient des bibliothèques de chiffrement incompatibles avec les bibliothèques de chiffrement installées.
27370	Erreur d'initialisation de la décompression de .NET 8.0.
27371	Erreur de décompression de .NET 8.0.
27372	Les informations d'enregistrement sur la version précédente de l'application ont été supprimées. Veuillez relancer l'installation.
27373	Échec de la suppression des informations d'enregistrement pour la version précédente de l'application.
27374	La mise à jour de l'application est en cours. Veuillez réessayer plus tard.
27375	Le mot de passe ou le nom d'utilisateur de désinstallation n'a pas été indiqué ou est incorrect.
27376	Échec de la désinstallation de Kaspersky Endpoint Agent. Veuillez désinstaller l'application vous-même ou désactiver la protection par mot de passe dans les paramètres. Relancez ensuite l'installation de l'application.
27377	Échec de la désinstallation de Kaspersky Security for Windows Server. Veuillez désinstaller l'application vous-même ou désactiver la protection par mot de passe dans les paramètres. Relancez ensuite l'installation de l'application.
27378	Plus d'espace disque.
27379	Échec de l'installation de l'application car des modules incompatibles ont été sélectionnés. Veuillez modifier l'ensemble de modules et redémarrer l'installation.
27380	Un fichier de configuration non valide a été sélectionné.
27381	Une clé de licence non valide a été sélectionnée.
27382	Échec de la création du groupe d'administration des applications.
27383	Le dossier que vous avez sélectionné n'est pas valide. Le nom du dossier de destination ne peut pas dépasser 160 caractères.
27384	Vous avez sélectionné un dossier ou un disque non valide. L'application doit être installée sur un disque dur local.
27385	Le dossier que vous avez sélectionné n'est pas valide. L'application ne peut pas être installée dans le dossier racine.
27386	Le dossier que vous avez sélectionné n'est pas valide. L'application ne peut pas être installée dans le dossier Windows ou ses sous-dossiers.

Code	Description
27387	Le dossier que vous avez sélectionné n'est pas valide. L'application ne peut pas être installée dans un dossier qui contient un sous-dossier temporaire.
27388	Le dossier que vous avez sélectionné n'est pas valide. L'application ne peut pas être installée directement dans le dossier Program Files.
27389	Le dossier que vous avez sélectionné n'est pas valide. L'application ne peut pas être installée sur un disque virtuel.
27390	Vous avez sélectionné un dossier ou un disque non valide. L'application ne peut pas être installée dans le dossier où la version précédente de l'application est installée.
27391	Le dossier ou le disque sélectionné contient déjà des fichiers. L'application ne peut pas être installée dans un dossier qui contient d'autres données, car ces données peuvent devenir inaccessibles une fois l'autodéfense activée.
27392	L'application ne peut pas être installée dans un dossier contenant des points d'analyse. Veuillez sélectionner un autre dossier d'installation.
27393	Impossible d'installer l'application dans un dossier dont le nom contient un point-virgule (;). Veuillez sélectionner un autre dossier d'installation.
27394	Le dossier que vous avez sélectionné n'est pas valide. Le dossier racine ne peut pas être défini.
27395	Le dossier que vous avez sélectionné n'est pas valide. Il est impossible de définir le dossier Windows ou ses sous-dossiers.
27396	Le dossier que vous avez sélectionné n'est pas valide. Le dossier Program Files ne peut pas être défini directement.
27397	Le dossier que vous avez sélectionné n'est pas valide. Un dossier qui contient un sous-dossier temporaire ne peut pas être défini.
27400	Erreur d'initialisation des mises à jour des fichiers.
27450	Le fichier CAB n'a pas pu être installé.
27451	Erreur de suppression.
27452	Erreur de suppression des fichiers.
27453	Erreur de déplacement des fichiers.
27454	Échec de création des fichiers du registre.
27455	Échec de l'obtention des informations sur la version du système d'exploitation.
27456	Échec de la planification du rétablissement des valeurs du registre.
27457	Échec de l'obtention des identifiants de sécurité (SID) connus.
27460	Erreur de création des descripteurs de sécurité.
27461	Erreur de restauration des descripteurs de sécurité.
27462	Échec de la création des règles pour le pare-feu Microsoft Windows.
27463	Échec de la suppression des règles pour le pare-feu Microsoft Windows.

Installation et suppression de l'application via Kaspersky Security Center

Cette section contient les informations concernant l'installation de Kaspersky Embedded Systems Security à l'aide de Kaspersky Security Center, la description de la procédure d'installation et de désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center, et les actions à entreprendre après avoir installé Kaspersky Embedded Systems Security pour Windows.

Informations générales sur l'installation via Kaspersky Security Center

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

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

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

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

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

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

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

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

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

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

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

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

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

Installation de Kaspersky Embedded Systems Security via Kaspersky Security Center

L'installation de Kaspersky Embedded Systems Security via Kaspersky Security Center comprend les étapes suivantes :

1. **Création du fichier d'installation**

   Le *fichier d'installation* désigne l'ensemble de fichiers formé pour l'installation à distance de l'application de Kaspersky à l'aide de Kaspersky Security Center. Le fichier d'installation contient l'ensemble de paramètres indispensables à l'installation de l'application et à la garantie de son fonctionnement immédiatement après l'installation. Le fichier d'installation est créé sur la base des fichiers portant l'extension kpd et kud qui figurent dans la distribution de l'application.

   Comment créer un paquet d'installation dans la Console d'administration de Kaspersky Security Center

   1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le dossier **Avancé** → **Installation à distance** → **Paquets d'installation**.
   2. Dans le panneau des résultats, cliquez sur le bouton **Créer un paquet d'installation**.

   L'Assistant de création du fichier d'installation démarre. Suivez les instructions de l'Assistant.

Étape 1. Sélection du type de fichier d'installation

Choisissez l'option **Créer un paquet d'installation pour une application Kaspersky**.

Étape 2. Sélection du nom du fichier d'installation

Saisissez le nom du paquet d'installation, par exemple, *Kaspersky Embedded Systems Security*.

Étape 3 Sélection du paquet de distribution de l'application à installer

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

Si vous prévoyez d'installer l'application à l'aide de la configuration **Protéger l'ordinateur avec des bases antivirus** par-dessus la configuration de l'application qui n'utilise pas l'analyse des signatures et les bases de données antivirus pour protéger l'ordinateur, ou vice versa, vous devez d'abord préciser l'identifiant et le mot de passe du compte disposant des autorisations nécessaires pour installer l'application dans le fichier ess_win.kud. Pour ce faire, ouvrez le fichier ess_win.kud dans un éditeur de texte et ajoutez les paramètres suivants à la ligne `Params` : `/pKLLOGIN=<login>` et `/pKLPASSWD=<password>`.

Si nécessaire, cochez la case **Copier les mises à jour depuis le stockage vers le paquet d'installation** pour mettre à jour les bases antivirus dans le paquet d'installation.

Étape 4. Contrat de licence et Politique de confidentialité

Si vous acceptez les termes et conditions du Contrat de licence utilisateur final et de la Politique de confidentialité, cochez les cases **Je confirme que j'ai entièrement lu, que je comprends et que j'accepte les termes et les conditions de ce Contrat de licence utilisateur final** et **Je comprends et j'accepte que mes données peuvent être traitées et transmises (y compris vers des pays tiers) dans le respect de la Politique de confidentialité. Je confirme que j'ai entièrement lu et que je comprends la Politique de confidentialité**.

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

Le fichier d'installation est créé et ajouté dans Kaspersky Security Center. Le fichier d'installation permet d'installer Kaspersky Embedded Systems Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application.

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

1. Dans la Console d'administration de Kaspersky Security Center, développez le nœud **Installation à distance**.
2. Dans le panneau des résultats du nœud enfant **Paquets d'installation**, ouvrez le menu contextuel du paquet d'installation créé pour Kaspersky Embedded Systems Security et choisissez l'option **Propriétés**.
3. Ouvrez la section **Configuration** de la fenêtre **Propriétés : <nom du paquet d'installation>**.
4. Configurez la zone de confiance en cliquant sur le bouton **Configurer**.
5. Dans le groupe **Sélection des modules**, cochez les cases en regard des noms des modules de Kaspersky Embedded Systems Security que vous souhaitez installer.
6. Dans le groupe **Mode Protection des fichiers en temps réel**, cochez la case **Activer la Protection des fichiers en temps réel après l'installation de l'application (recommandé)** et sélectionnez le mode de fonctionnement du module.
7. Si nécessaire, modifiez les numéros de port TCP que la Console de l'application utilise pour la connexion à distance à l'ordinateur sur lequel l'application est installée.

   Le numéro de port par défaut pour la connexion avec les informations d'identification Windows est 13032, et le numéro de port par défaut pour la connexion avec les informations d'identification des utilisateurs créés manuellement est 13031. Plage de numéros de port possibles : 1–65535.

   Pour interdire la connexion avec les identifiants des comptes utilisateurs créés manuellement, décochez la case **Utilisation des identifiants d'utilisateurs créés manuellement**.

8. Pour désigner un dossier d'installation différent du dossier sélectionné par défaut, indiquez le nom du dossier et son chemin d'accès dans le groupe **Configurer les chemins d'installation de l'application**, en cliquant sur le bouton **Paramètres**.

9. Pour installer l'application avec les paramètres prédéfinis, chargez le fichier de configuration.

10. Enregistrez vos modifications.

Comment créer un paquet d'installation dans Web Console

1. Réalisez une des opérations suivantes :

   - Dans la fenêtre principale de Web Console, sélectionnez **Découverte et déploiement** → **Déploiement et attribution** → **Paquets d'installation**.

   - Dans la fenêtre principale de Web Console, sélectionnez **Opérations** → **Stockages** → **Paquets d'installation**.

   La liste des paquets d'installation téléchargés depuis Kaspersky Security Center s'affiche.

2. Cliquez sur **Ajouter**.

L'Assistant de création du fichier d'installation démarre. Suivez les instructions de l'Assistant.

Étape 1. Sélection du type de fichier d'installation

Choisissez l'option **Générer un paquet d'installation pour une application Kaspersky**.

L'Assistant créera un fichier d'installation à partir du kit de distribution situé sur les serveurs de Kaspersky. La liste se renouvelle automatiquement au fur et à mesure de l'édition de nouvelles versions de l'application.

Vous pouvez également créer un fichier d'installation à partir d'un fichier.

Étape 2. Paquets d'installation

Choisissez le fichier d'installation de Kaspersky Embedded Systems Security for Windows. Le processus de création du fichier d'installation démarre. Lors de la création du fichier d'installation, vous devez accepter les termes du Contrat de licence utilisateur final et de la Politique de confidentialité.

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

Le fichier d'installation est créé et ajouté dans Kaspersky Security Center. Le fichier d'installation permet d'installer Kaspersky Embedded Systems Security sur les ordinateurs du réseau de l'organisation ou de mettre à jour la version de l'application.

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

1. Dans la fenêtre **Paquets d'installation**, cliquez sur le nom du paquet d'installation de Kaspersky Embedded Systems Security créé.
2. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Paramètres**.
3. Sélectionnez la section **Modules de protection**.
4. Configurez la zone de confiance en cliquant sur le bouton **Configurer**.
5. Dans la section **Sélectionnez les modules à installer**, cochez les cases en regard des noms des modules de Kaspersky Embedded Systems Security que vous souhaitez installer.
6. Dans le groupe **Mode Protection des fichiers en temps réel**, cochez la case **Activer la Protection des fichiers en temps réel après l'installation de l'application (recommandé)** et sélectionnez le mode de fonctionnement du module.
7. Si nécessaire, modifiez les numéros de port TCP que la Console de l'application utilise pour la connexion à distance à l'ordinateur sur lequel l'application est installée.

   Le numéro de port par défaut pour la connexion avec les informations d'identification Windows est 13032, et le numéro de port par défaut pour la connexion avec les informations d'identification des utilisateurs créés manuellement est 13031. Plage de numéros de port possibles : 1–65535.

   Pour interdire la connexion avec les identifiants des comptes utilisateurs créés manuellement, décochez la case **Port pour la connexion à distance à l'aide des identifiants d'utilisateurs créés manuellement**.
8. Sélectionnez la section **Paramètres d'installation**.
9. Configurez les paramètres suivants dans la section **Paramètres avancés** :

   - **Ajouter le chemin de l'application dans la variable d'environnement %PATH%**. Vous pouvez ajouter le chemin de l'installation à la variable %PATH% afin de faciliter l'administration des applications à partir de la ligne de commande.
   - **Afficher l'icône de la barre d'état système dans la barre des tâches**. Si la case est cochée, après l'installation de Kaspersky Embedded Systems Security, l'icône de l'application s'affiche dans la zone de notifications de la barre des tâches Microsoft Windows.
10. Si nécessaire, désactivez la fonctionnalité **Protéger le processus d'installation**.
11. Le cas échéant, modifiez les dossiers par défaut créés lors de l'installation de l'application sur l'appareil protégé.
12. Pour installer l'application avec les paramètres prédéfinis, cliquez sur le lien **Ajouter un fichier de configuration** et chargez le fichier de configuration.

    Lorsque vous utilisez les paquets d'installation dans Kaspersky Security Center Web Console, la taille maximale prise en charge des fichiers de configuration chargés est de 4 Mo. Si vous utilisez des paquets d'installation dans la Console d'administration de Kaspersky Security Center, cette limite ne s'applique pas.
13. Enregistrez vos modifications.

2 Création de la tâche d'installation à distance

La tâche *Installation à distance d'une application* permet d'installer à distance Kaspersky Embedded Systems Security. La tâche *Installation à distance d'une application* permet de déployer le paquet d'installation de l'application sur tous les ordinateurs de l'organisation.

Comment créer une tâche d'installation à distance dans la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
3. Cliquez sur **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Sélection du type de tâche

Choisissez **Serveur d'administration de Kaspersky Security Center → Installation à distance d'une application**.

Étape 2. Sélection du fichier d'installation

Sélectionnez le fichier de Kaspersky Embedded Systems Security dans la liste des fichiers d'installation. Si le fichier d'installation de Kaspersky Embedded Systems Security ne figure pas dans la liste, vous pouvez le créer dans l'Assistant.

Vous pouvez configurer les paramètres des fichiers d'installation dans Kaspersky Security Center. Par exemple, vous pouvez sélectionner les modules de l'application qui seront installés sur un ordinateur.

L'Agent d'administration est installé en même temps que Kaspersky Embedded Systems Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

Étape 3. Avancé

Choisissez le fichier d'installation de l'Agent d'administration. La version sélectionnée de l'Agent d'administration est installée avec Kaspersky Embedded Systems Security.

Étape 4. Paramètres

Configurez les paramètres complémentaires suivants de l'application :

- **Forcer le téléchargement du paquet d'installation**. Sélectionnez le mode d'installation de l'application :

  - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Embedded Systems Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Kaspersky Embedded Systems Security est ensuite installé à l'aide de l'Agent d'administration.

  - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez l'aide de Kaspersky Security Center.

  - **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.

- **Comportement pour les appareils administrés via d'autres Serveurs d'administration**. Sélectionnez le mode d'installation de Kaspersky Embedded Systems Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.

- **Ne pas réinstaller l'application si elle est déjà installée**. Décochez cette case si vous voulez, par exemple, installer une version antérieure de l'application.

Étape 5. Sélection du paramètre de redémarrage du système d'exploitation

Sélectionnez l'action à exécuter quand le redémarrage de l'ordinateur est requis. Un redémarrage n'est pas requis lors de l'installation de Kaspersky Embedded Systems Security. Le redémarrage est requis uniquement s'il faut supprimer des applications incompatibles avant l'installation. Le redémarrage peut s'imposer également lors de la mise à jour de la version de l'application.

Étape 6. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels Kaspersky Embedded Systems Security sera installé. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'Agent d'administration n'est pas installé sur les appareils non distribués. Dans ce cas, la tâche est affectée à l'ensemble d'appareils. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 7. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'Assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Embedded Systems Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 8. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 9. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple, *Installation de Kaspersky Embedded Systems Security for Windows 4.1*.

Étape 10. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci. L'application est installée en mode silencieux. Après l'installation, l'icône est ajoutée à la zone de notification de l'ordinateur de l'utilisateur. Si l'icône ressemble à , confirmez que vous avez activé l'application.

Comment créer une tâche d'installation à distance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste **Application**, choisissez **Kaspersky Security Center**.
2. Dans la liste déroulante **Type de tâche**, choisissez **Installation à distance d'une application**.
3. Dans le champ **Nom de la tâche**, saisissez une brève description, par exemple *Installation de Kaspersky Embedded Systems Security for Windows pour les cadres*.
4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

Étape 2. Sélection d'ordinateurs pour l'installation

À cette étape, sélectionnez les ordinateurs sur lesquels Kaspersky Embedded Systems Security va être installé conformément à l'option de zone d'action de la tâche sélectionnée.

Étape 3. Configuration des paramètres du fichier d'installation

Cette étape permet de configurer le fichier d'installation :

1. Choisissez le fichier d'installation de Kaspersky Embedded Systems Security for Windows (4.1).
2. Choisissez le fichier d'installation de l'Agent d'administration.

   La version sélectionnée de l'Agent d'administration est installée avec Kaspersky Embedded Systems Security. L'*Agent d'administration* assure la coopération entre le Serveur d'administration et l'ordinateur client. Si l'ordinateur est déjà doté de l'Agent d'administration, l'installation n'est pas répétée.

3. Dans le groupe **Forcer le téléchargement du paquet d'installation**, sélectionnez le mode d'installation de l'application :

   - **En utilisant l'Agent d'administration**. L'Agent d'administration est chargé de déployer le paquet d'installation de Kaspersky Embedded Systems Security sur les ordinateurs clients. Si l'Agent d'administration n'est pas installé, la tâche se solde sur un échec. Dans ce cas, ajoutez le paquet d'installation de l'Agent d'administration à la tâche *Installation à distance d'une application* et activez la diffusion des fichiers via les ressources du système d'exploitation. L'Agent d'administration sera alors installé à l'aide des ressources du système d'exploitation. Kaspersky Embedded Systems Security est ensuite installé à l'aide de l'Agent d'administration.

   - **En utilisant les ressources du système d'exploitation via les points de distribution**. Le fichier d'installation est transmis aux ordinateurs client par les outils du système d'exploitation via des points de distribution. Cette option est disponible s'il y a au moins un point de distribution dans le réseau. Pour en savoir plus sur le fonctionnement des points de distribution, consultez l'aide de Kaspersky Security Center.

   - **En utilisant les ressources du système d'exploitation via le Serveur d'administration**. Les fichiers sont remis aux ordinateurs client à l'aide des outils du système d'exploitation via un Serveur d'administration. Sélectionnez cette option si l'ordinateur client n'est pas doté d'un Agent d'administration mais qu'il se trouve dans le même réseau que le Serveur d'administration.

4. Dans le champ **Nombre maximal de téléchargements simultanés**, définissez la limite du nombre de requêtes adressées au Serveur d'administration pour le téléchargement du fichier d'installation. La restriction des demandes permet d'éviter la surcharge du réseau.

5. Dans le champ **Nombre maximal de tentatives d'installation**, définissez la limite de tentatives d'installation de l'application. Si l'installation Kaspersky Embedded Systems Security se solde sur une erreur, la tâche lance à nouveau l'installation automatiquement.

6. Le cas échéant, décochez la case **Ne pas réinstaller l'application si elle est déjà installée**. Cela permet, par exemple, d'installer une application d'une version antérieure.

7. Le cas échéant, décochez la case **Vérifier le type de système d'exploitation avant le téléchargement**. Cela permet d'éviter le téléchargement du paquet de distribution de l'application si le système d'exploitation de l'ordinateur ne répond pas à la configuration logicielle requise. Si vous êtes certain que le système d'exploitation est conforme à la configuration logicielle requise, vous pouvez ignorer cette vérification.

8. Le cas échéant, cochez la case **Réparer l'installation du paquet d'installation dans les stratégies de groupe d'Active Directory**. L'installation de Kaspersky Embedded Systems Security s'opère à l'aide des outils de l'Agent d'administration ou des outils d'Active Directory manuellement. Pour installer l'Agent d'administration, la tâche d'installation à distance doit être lancée sous les privilèges de l'administrateur de domaine.

9. Le cas échéant, cochez la case **Demander aux utilisateurs de fermer les applications en cours d'exécution**. L'installation de Kaspersky Embedded Systems Security requiert des ressources de l'ordinateur. Pour le confort de l'utilisateur, l'Assistant d'installation de l'application propose de quitter les applications en cours d'exécution avant de lancer l'installation. Cela permettra d'éviter le ralentissement des autres applications et les échecs possibles de l'ordinateur.

10. Dans le groupe **Comportement pour les appareils administrés via d'autres Serveurs d'administration**, sélectionnez le mode d'installation de Kaspersky Embedded Systems Security. Si le réseau compte plus d'un Serveur d'administration, ces serveurs peuvent voir les mêmes ordinateurs client. Cela peut provoquer, par exemple, l'installation à distance de la même application sur le même ordinateur client depuis plusieurs Serveurs d'administration ainsi que d'autres conflits.

Étape 4. Sélection du compte utilisateur pour lancer la tâche

Choisissez le compte utilisateur pour l'installation de l'Agent d'administration à l'aide des outils du système d'exploitation. Dans ce cas, l'accès à l'ordinateur requiert les privilèges d'administrateur. Vous pouvez ajouter plusieurs comptes utilisateur. Si le compte n'a pas les privilèges requis, l'Assistant d'installation utilise le compte utilisateur suivant. Pour installer Kaspersky Embedded Systems Security à l'aide des outils de l'Agent d'administration, il n'est pas nécessaire de choisir un compte utilisateur.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant en cliquant sur le bouton **Terminer**. La nouvelle tâche apparaît dans la liste des tâches. Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**. L'application est installée en mode silencieux. Après l'installation, l'icône est ajoutée à la zone de notification de l'ordinateur de l'utilisateur. Si l'icône ressemble à , confirmez que vous avez activé l'application.

L'aide de Kaspersky Security Center contient des informations supplémentaires sur la génération d'un paquet d'installation et la création de la tâche d'installation à distance.

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

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

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

1. Créez la tâche *Mise à jour* pour le groupe d'appareils protégés sur lesquels vous avez installé Kaspersky Embedded Systems Security. Désignez le Serveur d'administration de Kaspersky Security Center comme source des mises à jour.

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

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

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

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

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

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

1. Dans la Console d'administration de Kaspersky Security Center, développez le nœud **Avancé**.
2. Développez le nœud enfant **Installation à distance**.
3. Créez un paquet d'installation :
   a. Dans le panneau des résultats du nœud enfant **Paquets d'installation**, cliquez sur le bouton **Créer un paquet d'installation**.
   b. Dans la fenêtre **Assistant Nouveau paquet d'installation**, sélectionnez **Créer un paquet d'installation pour le fichier exécutable défini** en tant que type de paquet.
   c. Saisissez le nom du nouveau paquet d'installation.
   d. Sélectionnez le fichier \client\setup_esstool.exe dans le dossier du kit de distribution de Kaspersky Embedded Systems Security, puis cochez la case **Copier tout le dossier dans le paquet d'installation**.
   e. Dans le champ **Paramètres de lancement du fichier exécutable (facultatif)**, indiquez les valeurs du paramètre EULA=1 et PRIVACYPOLICY=1:

      ```
      /s /p "EULA=1 PRIVACYPOLICY=1"
      ```

      Sinon, il est impossible d'installer les modules.
   f. Si nécessaire, dans le champ **Paramètres de lancement du fichier exécutable (facultatif)**, vous pouvez spécifier le paramètre de ligne de commande ADDLOCAL pour modifier l'ensemble des modules à installer et le paramètre de ligne de commande INSTALLDIR pour spécifier un dossier de destination autre que celui par défaut. Par exemple, pour effectuer une installation autonome de la Console de l'application dans le dossier C:\KasperskyConsole, utilisez l'option de ligne de commande suivante :

      ```
      /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
      ```
4. Dans le nœud **Paquets d'installation**, créez une tâche d'installation à distance de la Console de l'application sur les appareils protégés sélectionnés (groupe d'administration).
5. Configurez les paramètres de la tâche.
6. Lancez la tâche d'installation à distance.

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

Désinstallation de Kaspersky Embedded Systems Security via Kaspersky Security Center

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

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

Pour désinstaller Kaspersky Embedded Systems Security :

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

Modification de l'ensemble des modules d'application à l'aide de Kaspersky Security Center

Pour modifier l'ensemble des modules de Kaspersky Embedded Systems Security après l'installation de l'application, utilisez la tâche *Modification de la sélection des modules de l'application*.

Comment modifier l'ensemble des modules de l'application dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Sélection du type de tâche

Choisissez **Kaspersky Embedded Systems Security for Windows (4.1) → Modification de la sélection des modules de l'application**.

Étape 2. Paramètres de la tâche de modification des modules de l'application

Choisissez les modules de l'application qui seront accessibles sur l'ordinateur. Configurez les paramètres avancés de la tâche (cf. tableau ci-après).

Étape 3. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 4. Configuration de la planification du lancement de la tâche

Définissez une planification pour le lancement d'une tâche, par exemple manuellement ou lorsque l'ordinateur est inactif.

Étape 5. Définition du nom de la tâche

Saisissez un nom pour la tâche, par exemple, *Ajout du module Contrôle des applications*.

Étape 6. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment modifier l'ensemble des modules de l'application dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste déroulante **Application**, choisissez **Kaspersky Embedded Systems Security 4.1.0**.
2. Dans la liste déroulante **Type de tâche**, choisissez **Modifier les modules de Kaspersky Embedded Systems Security**.
3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Ajout du module Contrôle des applications*.
4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

Étape 2. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Par exemple, sélectionnez un groupe d'administration distinct ou effectuez une sélection.

Étape 3. Fin de la création de la tâche

1. Cochez la case **Ouvrir les détails de la tâche à la fin de la création** et quittez l'Assistant.
2. Dans les propriétés des tâches, sélectionnez l'onglet **Paramètres de l'application**.
3. Choisissez les modules de l'application qui seront accessibles sur l'ordinateur. Configurez les paramètres avancés de la tâche (cf. tableau ci-après).

Cette action entraîne la modification de la sélection de modules de Kaspersky Embedded Systems Security sur les ordinateurs des utilisateurs en mode silencieux.

Paramètres avancés des tâches

Paramètre	Description
Zone de confiance	Pour la tâche *Modification de la sélection des modules de l'application*, vous pouvez uniquement ajouter des exclusions de l'analyse et des applications approuvées à la zone de confiance.
Utiliser le mot de passe pour modifier la sélection de modules de l'application	Les administrateurs activent généralement la protection par mot de passe pour restreindre l'accès à Kaspersky Embedded Systems Security. Autrement dit, pour modifier la sélection des modules de l'application, vous devez entrer les identifiants d'un utilisateur disposant de l'autorisation **Supprimer/Modifier/Réparer l'application**. Par exemple, vous pouvez utiliser le compte KLAdmin.
Vérifier la présence d'applications incompatibles d'éditeurs tiers	Par défaut, Kaspersky Embedded Systems Security vérifie la compatibilité des applications installées. La liste des applications incompatibles figure dans le fichier incompatible.txt du kit de la distribution. Si la vérification des applications incompatibles est activée, Kaspersky Embedded Systems Security arrête la tâche dès la détection d'une application dans la liste. Vous pouvez désactiver l'analyse des logiciels installés si la documentation du fournisseur du logiciel tiers revendique la compatibilité avec Endpoint Protection Platform (EPP).
Supprimer les applications incompatibles d'éditeurs tiers	Suppression automatique des applications de la liste incompatible.txt avant la modification l'ensemble des modules. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security tente de supprimer les applications qui peuvent entraîner des problèmes de compatibilité afin de poursuivre la tâche. Cette option est activée par défaut.

Installation et suppression de l'application via les stratégies de groupe Active Directory

Cette section décrit les procédures d'installation et de désinstallation de Kaspersky Embedded Systems Security via les stratégies de groupe Active Directory, ainsi que les informations sur les actions à réaliser après l'installation de Kaspersky Embedded Systems Security via les stratégies de groupe Active Directory.

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

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

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

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

Vous devez posséder les autorisations d'administrateur de domaine.

Pour installer Kaspersky Embedded Systems Security, utilisez le paquet d'installation ess_win.msi. Pour installer la console de l'application, utilisez le paquet d'installation esstools.msi.

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

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

1. Enregistrez ess_win.msi dans un dossier partagé sur le contrôleur de domaine.
2. Enregistrer le fichier clé dans le même dossier partagé sur le contrôleur de domaine.
3. Dans le même dossier partagé sur le contrôleur de domaine, créez un fichier install_props.json qui contient les lignes ci-dessous. Cela signifie que vous êtes d'accord avec les conditions du Contrat de licence utilisateur final et de la Politique de confidentialité.

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

4. Sur le contrôleur de domaine, créez une stratégie pour groupe auquel appartiennent les appareils protégés.
5. À l'aide du **Group Policy Object Editor**, créez un nouveau paquet d'installation dans le nœud **Configuration ordinateur**. Saisissez le chemin d'accès au fichier msi pour Kaspersky Embedded Systems Security (de la Console de l'application) au format UNC (Universal Naming Convention).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Sélectionnez la stratégie créée pour l'installation de Kaspersky Embedded Systems Security et dans **Éditeur des stratégies de groupe**, nœud **Installation des logiciels** (**Configuration ordinateur** > **Configuration des programmes** > **Installation des logiciels**) ouvrez le menu contextuel du paquet d'installation de Kaspersky Embedded Systems Security (de la console de l'application) et sélectionnez la commande **Toutes les tâches** > **Supprimer**.

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

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

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

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

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

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

Pour installer Kaspersky Embedded Systems Security et créer le fichier journal sur le disque C:\, exécutez la commande suivante :

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

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

Lorsque Kaspersky Embedded Systems Security et la Console de Kaspersky Embedded Systems Security sont installés ensemble, le service Windows Installer procède aux modifications suivantes sur l'appareil protégé :

- création des dossiers de Kaspersky Embedded Systems Security sur l'appareil protégé et sur l'appareil protégé sur lequel la Console de l'application est installée ;
- enregistrement des services Kaspersky Embedded Systems Security ;
- création d'un groupe d'utilisateurs de Kaspersky Embedded Systems Security.
- Les clés de Kaspersky Embedded Systems Security sont enregistrées dans la base de registres.
- La tâche système de détection de la mise à jour du système d'exploitation de Kaspersky Embedded Systems Security qui s'affiche dans le Planificateur de tâches Windows est créée.

Ces modifications sont décrites ci-dessous.

Dossiers de Kaspersky Embedded Systems Security sur un appareil protégé

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

- Dossier d'installation par défaut de Kaspersky Embedded Systems Security contenant les fichiers exécutables de Kaspersky Embedded Systems Security. Le dossier d'installation suivant est utilisé par défaut :

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0

- Les fichiers Management Information Base (MIB) contenant une description des compteurs et les pièges publiés par Kaspersky Embedded Systems Security selon le protocole SNMP :

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0\mibs

- Fichiers de service de Kaspersky Embedded Systems Security :

  - %ProgramData%\Kaspersky Lab\KESS.4.1\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Dskm

- Fichiers contenant les paramètres pour les sources de mise à jour :

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data

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

  %ProgramData%\Kaspersky Lab\KESS.4.1\Update distribution

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

  %ProgramData%\Kaspersky Lab\KESS.4.1\Reports

- Ensemble de bases de données utilisées actuellement :

  %ProgramData%\Kaspersky Lab\KESS.4.1\Bases

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

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

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

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data\temp\temporaryFolder

- Objets en quarantaine (dossier par défaut) :

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

- Objets dans la sauvegarde (dossier par défaut) :

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB

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

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB\Restored

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

Le dossier d'installation par défaut de la Console de l'application dépend du nombre de bits du système d'exploitation. Le dossier d'installation suivant est utilisé par défaut :

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0

Services de Kaspersky Embedded Systems Security

Les services Kaspersky Embedded Systems Security suivants s'exécutent sous le compte SYSTEM :

- Kaspersky Embedded Systems Security Service (AVP.KESS.4.1). Le service système principal de Kaspersky Embedded Systems Security, qui protège les appareils contre les virus et autres menaces
- Kaspersky Embedded Systems Security Side-by-Side Service (AVP.KESS.4.1.SbS). Le service système qui assure la protection des appareils pendant la mise à jour, la restauration ou la modification de composants de Kaspersky Embedded Systems Security
- Kaspersky Seamless Update Service (avpsus.KESS.4.1). Le service système qui installe et annule les mises à jour critiques et approuvées des modules de l'application
- Kaspersky Embedded Systems Security Remote Control Service (avpcos.KESS.4.1). Service système permettant de redémarrer et d'arrêter à distance Kaspersky Embedded Systems Security Service depuis la Console de l'application

Groupe Kaspersky Embedded Systems Security

Administrateurs ESS désigne un groupe sur l'appareil protégé dont les membres ont un accès total à toutes les fonctions de Kaspersky Embedded Systems Security.

Clés du registre système

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

- Paramètres de Kaspersky Embedded Systems Security :

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.1]

- Paramètres du journal des événements de Kaspersky Embedded Systems Security (journal des événements Kaspersky) :

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]

- Paramètres du fichier de traçage :
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\Trace]
- Paramètres des tâches et fonctions de l'application :
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\environment]

Tâche système de mise à jour du système d'exploitation de Kaspersky Embedded Systems Security

Le service d'installation de Windows crée une tâche Kaspersky Embedded Systems Security OS Upgrade Detect lors de l'installation de l'application. La tâche démarre immédiatement après sa création, puis à chaque démarrage du système d'exploitation. La tâche vérifie la version des pilotes utilisée par l'application : en cas de mise à jour de la version du système d'exploitation, l'application met à jour les pilotes pour la version correspondante du système d'exploitation.

La tâche n´affecte pas l'application et peut être supprimée. Nous vous recommandons de garder à l'esprit le scénario de mise à jour du système d'exploitation.

Règles du Pare-feu Windows

Selon les paramètres d'installation spécifiés, des règles du Pare-feu Windows autorisant les connexions entrantes décrites dans le tableau ci-dessous peuvent être créées sur l'appareil protégé.

Règles du Pare-feu Windows

Nom de la règle	Description de la règle	Condition de création de la règle
AVP.KESS.4.1	Règle d'autorisation pour le fichier exécutable avp.exe.	Toujours créée.
Connexion à l'interface utilisateur distante AVP.KESS.4.1	Règle d'autorisation pour le port TCP 13032.	Installation de l'application avec le paramètre `ADDWFEXCLUSION=1`.
Connexion à l'interface utilisateur distante AVP.KESS.4.1	Règle d'autorisation pour le port TCP 13031. Ce numéro de port est utilisé par défaut. Vous pouvez modifier le numéro de port en spécifiant le paramètre `UIKLPORT=<port>`. Dans ce cas, l'application crée une règle pour le numéro de port spécifié.	Installation de l'application avec les paramètres `ADDWFEXCLUSION=1` et `UIKLPORT=13031`. La règle n'est pas créée si le paramètre `ENABLEUIKLPORT=0` est transmis

Processus de Kaspersky Embedded Systems Security

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

Processus de Kaspersky Embedded Systems Security

Nom du fichier	Fonction
avp.exe	Flux de travail de Kaspersky Embedded Systems Security
avpsus.exe	Ce processus permet d'installer et annuler les mises à jour critiques et approuvées des modules d'application.

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

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

À propos du virus d'essai EICAR

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

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

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

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

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

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

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

Préfixe des fichiers EICAR

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

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

Après l'installation de Kaspersky Embedded Systems Security, vous pouvez confirmer que Kaspersky Embedded Systems Security détecte les objets qui contiennent du code malveillant. Pour ce faire, utilisez le virus test EICAR.

Pour vérifier la fonction Protection des fichiers en temps réel :

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

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

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

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

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

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

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

La Protection des fichiers en temps réel fonctionne correctement si les conditions suivantes sont remplies :

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

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

- Un message du service Windows Messenger sur l'appareil d'où vous avez copié le fichier (service de terminal dans la session terminal sur l'appareil) dont le texte est : Kaspersky Embedded Systems Security a interdit l'accès à <chemin d'accès au fichier eicar.com sur l'appareil>\eicar.com sur l'appareil <nom réseau de l'appareil> à <heure de l'événement>. Reason: Threat detected. Virus : EICAR-Test-File. User name: <user name>. Computer name: <network name of the device from which you copied the file>.

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

Pour vérifier la fonction Analyse à la demande :

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

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

2. Ouvrez la Console de l'application et développez le nœud **Analyse à la demande** dans l'arborescence de la Console de l'application.

3. Sélectionnez le nœud enfant **Analyse des zones critiques**.

4. Ajoutez **Tous les disques réseau** à la zone d'action de la tâche Analyse à la demande.

5. Lancer la tâche Analyse des zones critiques.

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

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

Mise à jour des anciennes versions de Kaspersky Embedded Systems Security vers la version 4.1

Lors de la mise à jour d'une version antérieure de Kaspersky Embedded Systems Security vers la version 4.1, suivez les recommandations suivantes :

- Anticipez et programmez la mise à jour. Choisissez un moment où les serveurs fonctionnent avec la charge la plus faible, par exemple pendant le week-end.
- Après la mise à jour, activez les modules de l'application un par un. C'est-à-dire, par exemple, commencez par activer le module Protection des fichiers en temps réel seul, puis activez d'autres modules de protection, puis activez les modules de surveillance, etc. Il est conseillé de tester l'application à chaque étape.
- Exécutez la mise à jour étape par étape. Mettez d'abord à jour un ordinateur, puis plusieurs ordinateurs, puis tous les ordinateurs de l'organisation.

Étapes de la procédure de mise à jour

Effectuez une mise à jour de Kaspersky Embedded Systems Security vers la version 4.1 dans l'ordre suivant :

1. **Mettre à jour Kaspersky Security Center**

   Mettez à jour tous les modules de Kaspersky Security Center vers la version 14.2 ou une version ultérieure, y compris l'Agent d'administration, sur les ordinateurs des utilisateurs et Kaspersky Security Center Web Console.

2. **Mettez à jour le plug-in Web de Kaspersky Embedded Systems Security**

   Dans Kaspersky Security Center Web Console, mettez à jour le plug-in Web de Kaspersky Embedded Systems Security vers la version 4.1.

3. **Migrez les tâches et les stratégies de Kaspersky Embedded Systems Security**

   Après la migration des stratégies et des tâches, vous devez configurer les paramètres que l'assistant de migration ne peut pas migrer, et qui n'existaient pas dans les anciennes versions de l'application. Nous vous recommandons également de vérifier si l'Assistant de migration a correctement migré tous les paramètres.

4. **Installer Kaspersky Embedded Systems Security 4.1**

   La version 4.1 de Kaspersky Embedded Systems Security utilise le protocole HTTPS au lieu du protocole DCOM. Par conséquent, avant d'installer la nouvelle version de Kaspersky Embedded Systems Security, il est nécessaire de configurer l'appareil sur lequel l'application sera mise à jour afin d'activer le démarrage à distance du service KESS. Si cette configuration n'est pas effectuée, le démarrage du service à distance ne sera pas disponible.

   Vous pouvez installer Kaspersky Embedded Systems Security 4.1 après la suppression d'une version antérieure de l'application ou par-dessus.

Lors de l'installation par-dessus une ancienne version de l'application, le même ensemble de modules d'application est installé, en tenant compte des nouveaux noms et contenus de certains modules.

Lors d'une installation à distance, le programme d'installation installe les modules que vous sélectionnez dans les propriétés du paquet d'installation.

5. **En cas de nécessité, activez Kaspersky Embedded Systems Security 4.1**

   Lors de l'installation de Kaspersky Embedded Systems Security 4.1 sur une ancienne version de l'application, la licence actuelle est automatiquement appliquée à l'application, et les nouveaux modules et tâches de l'application sont entièrement disponibles. La durée de l'abonnement reste inchangée.

6. **Assurez-vous que l'application fonctionne**

   Après la mise à jour de Kaspersky Embedded Systems Security, assurez-vous que l'application fonctionne comme prévu. Assurez-vous qu'aucune erreur n'est signalée pour l'application, vérifiez également l'heure de la dernière connexion au Serveur d'administration, l'heure de la dernière mise à jour et l'état de la protection de l'ordinateur.

   Faites attention à la migration des listes d'exclusions, des applications de confiance, des règles de contrôle des appareils et des règles de contrôle du lancement des applications.

Mise à jour de Kaspersky Embedded Systems Security

La mise à jour vers Kaspersky Embedded Systems Security 4.1 est prise en charge à partir de la version 2.3, 3.1 et des versions ultérieures. Pour mettre à jour l'application à partir d'une version antérieure, vous devez supprimer la version installée et installer la version 4.1.

La mise à jour s'effectue via l'installation d'une nouvelle version de l'application sur la version installée de l'application et ne nécessite pas le redémarrage de l'ordinateur.

Par défaut, l'application crée un nouveau dossier d'installation portant le nom de la nouvelle version de l'application sur la base du chemin d'accès au dossier d'installation de l'application existant. Vous pouvez spécifier manuellement un nouveau chemin pour le dossier d'installation de l'application.

Lors de la mise à jour de Kaspersky Embedded Systems Security vers la version 4.1, la version précédemment installée de l'application est supprimée automatiquement.

Lors de la mise à jour d'une installation protégée par mot de passe de Kaspersky Embedded Systems Security, communiquez le mot de passe au programme d'installation en procédant de l'une des manières suivantes :

- En cas d'installation locale via l'interface de l'Assistant d'installation ou en mode CLI interactif, indiquez le mot de passe lorsqu'il vous est demandé.
- En cas d'installation locale en mode CLI non interactif, indiquez le mot de passe dans la clé `UNLOCK_PASSWORD`.
- Si vous procédez à l'installation via les stratégies de groupe Active Directory, spécifiez la valeur de la clé `UNLOCK_PASSWORD` dans le fichier de configuration install_props.json.

Lorsque l'application mise à jour à distance avec Kaspersky Security Center est protégée par un mot de passe, désactivez d'abord la protection par mot de passe à l'aide d'une stratégie de Kaspersky Security Center.

Lors de la mise à jour de l'application, la licence actuelle est automatiquement appliquée à la version 4.1 de Kaspersky Embedded Systems Security, et les nouveaux modules et tâches de l'application sont entièrement accessibles. La durée de l'abonnement reste inchangée.

Si une application est mise à jour avec une licence expirée, la nouvelle version de l'application s'exécute en mode de fonctionnalités limitées après l'installation (par exemple, les mises à jour des bases de données de l'application ne sont pas disponibles).

Mise à jour des outils d'administration de Kaspersky Embedded Systems Security

Vous pouvez mettre à jour le plug-in d'administration pour gérer l'application à l'aide de Kaspersky Security Center vers la version 4.1 à partir des versions 2.3, 3.1, 3.2, 3.3, 3.4 ou ultérieures. Pour mettre à jour des versions antérieures du plug-in d'administration et de la Console de l'application, il faut supprimer la version installée, puis installer la version 4.1.

Lors de la mise à jour, une nouvelle version du Plug-in d'administration est installée sur la version installée précédemment et ne nécessite pas le redémarrage de l'ordinateur.

Pour plus d'informations sur la migration des paramètres du plug-in d'administration, veuillez consulter cet article.

Migration des stratégies et des tâches

Vous pouvez migrer les paramètres des stratégies et des tâches des versions précédentes de l'application vers la version 4.1 des façons suivantes :

- En utilisant l'Assistant de conversion de masse des stratégies et des tâches (uniquement disponible dans la Console d'administration de Kaspersky Security Center).
- En utilisant l'Assistant de migration des stratégies et des tâches de Kaspersky Embedded Systems Security 4.1 (uniquement disponible dans Kaspersky Security Center Web Console).

Il est recommandé de commencer par migrer les stratégies et les tâches de Kaspersky Embedded Systems Security sur un seul ordinateur, puis sur un groupe d'ordinateurs et pour conclure, de réaliser la migration sur l'ensemble des ordinateurs de l'organisation.

Comment utiliser l'Assistant de conversion de masse des stratégies et des tâches pour migrer les paramètres des stratégies et des tâches

1. Dans la Console d'administration de Kaspersky Security Center, sélectionnez le Serveur d'administration et faites un clic droit pour ouvrir le menu contextuel.
2. Choisissez **Toutes les tâches → Assistant de conversion de masse des stratégies et des tâches**.

Cette opération lance l'Assistant de conversion de masse des stratégies et des tâches. Suivez les instructions de l'Assistant.

Étape 1. Sélectionnez l'application dont il faut convertir les stratégies et les tâches

Sélectionnez Kaspersky Embedded Systems Security 4.1. Passez à l'étape suivante.

Étape 2. Conversion des stratégies

Sélectionnez les stratégies de la version de l'application en cours de mise à jour que vous souhaitez créer pour Kaspersky Embedded Systems Security 4.1. Passez à l'étape suivante.

Étape 3. Conversion des tâches

Sélectionnez les tâches de la version de l'application en cours de mise à jour que vous voulez créer pour Kaspersky Embedded Systems Security 4.1.

Les tâches hors groupe (tâches attribuées à des appareils individuels) ne sont pas affichées à l'étape actuelle.

Pour convertir des tâches non groupées depuis votre version de l'application vers Kaspersky Embedded Systems Security 4.1, procédez comme suit :

1. Cliquez sur **Suivant**.

   La fenêtre **Migrez également les planifications et les tâches non liées à un groupe** s'ouvre.

2. Cochez la case **Migrer les tâches non liées à un groupe**.

3. Indiquez les paramètres de connexion au Serveur d'administration de Kaspersky Security Center.

4. Cliquez sur **OK**.

Étape 4. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- Les nouvelles stratégies pour Kaspersky Embedded Systems Security 4.1 sont créées.

  Les nouvelles stratégies contiennent les paramètres des stratégies Kaspersky Embedded Systems Security sélectionnées, ainsi que les nouveaux paramètres introduits dans Kaspersky Embedded Systems Security 4.1. Les noms des nouvelles stratégies sont les mêmes que les noms des stratégies Kaspersky Embedded Systems Security avant la conversion, suivis par « (conversion) ». Les nouvelles stratégies portent l'état *Stratégie inactive*.

- Les nouvelles tâches pour Kaspersky Embedded Systems Security 4.1 sont créées.

  Les nouvelles tâches contiennent les paramètres des tâches sélectionnées de Kaspersky Embedded Systems Security ainsi que les nouveaux paramètres introduits dans Kaspersky Embedded Systems Security 4.1. Les noms des nouvelles tâches sont les mêmes que les noms des tâches Kaspersky Embedded Systems Security avant la conversion, suivis par « (conversion) ».

- Les stratégies et tâches sélectionnées pour la conversion restent inchangées.

Utilisation de l'Assistant de migration pour migrer les paramètres des stratégies et des tâches

Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Migration vers KESS 4.1.0**.

Cela lance l'Assistant de migration de stratégies et de tâches. Suivez les instructions de l'Assistant.

Étape 1. Migration de stratégie

Sélectionnez les stratégies Kaspersky Embedded Systems Security que vous souhaitez créer pour Kaspersky Embedded Systems Security 4.1. Passez à l'étape suivante.

Étape 2. Migration d'une tâche

Dans la liste des tâches, choisissez les tâches de Kaspersky Embedded Systems Security que vous souhaitez créer pour Kaspersky Embedded Systems Security 4.1. Passez à l'étape suivante.

Étape 3. Fin de l'Assistant

Quittez l'Assistant. L'Assistant effectue alors les opérations suivantes :

- Les nouvelles stratégies pour Kaspersky Embedded Systems Security 4.1 sont créées.

  Les nouvelles stratégies contiennent les paramètres des stratégies migrées depuis Kaspersky Embedded Systems Security, ainsi que les nouveaux paramètres introduits dans Kaspersky Embedded Systems Security 4.1. Les noms des nouvelles stratégies sont les mêmes que les noms des stratégies Kaspersky Embedded Systems Security avant la fusion, plus l'expression « copié depuis KESS ». Les nouvelles stratégies portent l'état *Stratégie inactive*.

- Les nouvelles tâches pour Kaspersky Embedded Systems Security 4.1 sont créées.

  Les nouvelles tâches contiennent les paramètres des tâches migrées de Kaspersky Embedded Systems Security, ainsi que les nouveaux paramètres introduits dans Kaspersky Embedded Systems Security 4.1. Les noms des nouvelles tâches sont les mêmes que les noms des tâches Kaspersky Embedded Systems Security avant la fusion, plus l'expression « copié depuis KESS ».

Migration des paramètres de la version de l'application en cours de mise à jour

Ce qui suit est migré sans changement après la mise à jour de l'application et de ses plug-ins de gestion vers la version 4.1 :

- Paramètres des modules et tâches excepté ceux dont les valeurs par défaut sont rétablies et de la liste dans la section « Limitations de la migration des paramètres et modules »
- Journaux des tâches et journaux des audits système, et enregistrements dans le journal des événements Windows
- Paramètres de notifications des tâches
- Comptes utilisateurs sous lesquels les tâches sont lancées
- Autorisations d'accès de l'utilisateur pour l'administration de l'application
- Mot de passe de connexion au serveur proxy
- État de l'attribut

Les paramètres suivants sont réinitialisés ou définis aux valeurs par défaut pour la nouvelle version de l'application après la mise à jour de l'application et de ses plug-ins vers la version 4.1 :

- Tous les compteurs, y compris les états des bases antivirus
- Données sur les mises à jour installées des modules d'application et des bases antivirus
- États des tâches
- Autorisations d'accès utilisateur pour gérer le Kaspersky Embedded Systems Security Service
- Paramètres de l'application et des tâches configurés via le registre
- Paramètres de l'application et des tâches qui ont été modifiés lors de l'installation des correctifs critiques
- Configuration d'événement
- Paramètres de transfert des données vers le Serveur d'administration de Kaspersky Security Center : par défaut, le transfert de toutes les données est activé
- Paramètres de traçage et vidage
- Paramètres des tâches locales de l'application, situés sous l'onglet **Notifications**.

Les valeurs des paramètres introduits lors d'une mise à jour de l'application sont définies par défaut.

Restrictions de la migration des paramètres et modules

- Le contenu de la quarantaine de la version en cours de mise à jour est déplacé vers la sauvegarde de la version 4.1. En parallèle, la taille maximale de la sauvegarde est portée à 400 Mo et le seuil d'espace disponible à 100 Mo.

- Les paramètres suivants de Kaspersky Embedded Systems Security version 3.4 n'existent pas dans les versions 4.0 et ultérieures de Kaspersky Embedded Systems Security. Ils ne sont donc pas migrés : **Dossier de quarantaine**, **Dossier de sauvegarde** et **Dossier de restauration des objets**. Les autres paramètres qui existent dans l'ancienne version, mais pas dans la nouvelle version, ne sont pas non plus migrés.

- La liste des sessions réseau bloquées des ordinateurs clients n'est pas migrée. En même temps, les paramètres du déblocage automatique de l'accès aux ressources de fichiers réseau bloquées ne sont pas modifiés après la mise à jour d'une application.

- Les paramètres de protection par mot de passe ne font pas l'objet d'une migration. Dans Kaspersky Embedded Systems Security 4.0, la protection par mot de passe a été considérablement modifiée. Si nécessaire, activez la protection par mot de passe et définissez un mot de passe.

- Zone de confiance :

  - Le mode de sélection des objets de la zone de confiance a été modifié dans Kaspersky Embedded Systems Security 4.1. Les exclusions définies comme fichiers individuels ou chemins de fichiers ou de dossiers peuvent être migrées. Les exclusions définies comme une zone prédéfinie (comme les disques durs) ou une URL de script ne sont pas migrées. Après la migration, vous devez ajouter ces exclusions manuellement.

  - Les exclusions d'analyse et les applications de confiance prédéfinies qui aident à configurer l'application sur les serveurs ont été ajoutées à la zone de confiance.

- Les modules Contrôle du lancement des applications et Contrôle des appareils ont été remaniés en profondeur. Les paramètres des modules de la version en cours de mise à jour sont migrés en tenant compte de la nouvelle structure des paramètres de Kaspersky Embedded Systems Security 4.1. Cela signifie que vous aurez peut-être besoin de davantage d'espace sur le Serveur d'administration pour stocker les paramètres de l'application.

- Les paramètres des modules Contrôle de l'intégrité des fichiers et Surveillance de l'accès au registre de la version de l'application mise à jour sont migrés vers les paramètres du module Contrôle de l'intégrité du système.

- Le module Gestion du pare-feu a été retravaillé pour devenir le module Pare-feu qui, en plus d'assurer l'interface avec le pare-feu Windows, fonctionne désormais comme un pare-feu. Une fois la migration terminée, vous devez configurer le mode module depuis le début.

- Pour utiliser KSN, veuillez lire et accepter de nouveau la Déclaration de KSN.

- Les versions 4.0 et les versions ultérieures de l'application ne prennent pas en charge la planification individuelle des modules. Si les modules sont activés, ils tourneront tant que l'application est exécutée.

- Lors de la migration des tâches, l'heure de lancement de la tâche est décalée du nombre d'heures correspondant au fuseau horaire configuré dans les paramètres du système d'exploitation de l'ordinateur sur lequel s'opère la migration. Par exemple, supposons que l'heure de lancement de la tâche dans la version antérieure de l'application soit 7h00 et que le fuseau horaire configuré pour le système d'exploitation soit UTC +3. Une fois la tâche migrée, l'heure de début deviendra donc 10h00.

- La section définissant les actions à exécuter sur les objets infectés a été supprimée des paramètres du module Protection des fichiers en temps réel et des tâches Analyse à la demande. Ces paramètres ne sont pas migrés vers la version la plus récente de l'application.

- Kaspersky Security Center Web Console ou la Console d'administration ne peut pas être utilisée pour envoyer à Kaspersky des objets de la Sauvegarde pour analyse s'ils ont été migrés après une mise à jour de la version 3.4 ou une version antérieure de l'application vers la version 4.0 ou une version ultérieure.

- Lors de la migration des tâches d'analyse à la demande, le niveau de sécurité par défaut pour les zones d'analyse prédéfinies passe de *Informer* à *Personnalisé*.

- Si un module précédemment inclus dans l'installation n'est pas installé lors d'une mise à jour locale de Kaspersky Embedded Systems Security, les paramètres de ce module ne sont pas conservés. Si vous installez ce module ultérieurement, les paramètres par défaut lui seront appliqués.

Correspondance des modules et des tâches dans les versions 3.4 et 4.1 de Kaspersky Embedded Systems Security

Lors de la mise à jour de l'application Kaspersky Embedded Systems Security 3.4 vers la version 4.1, l'ensemble des modules et des tâches ne sont migrés que si l'installation est effectuée localement.

Correspondance des modules dans les versions 3.4 et 4.1 de Kaspersky Embedded Systems Security

Module de Kaspersky Embedded Systems Security 3.4	Module de Kaspersky Embedded Systems Security 4.1
Exclusions de l'analyse pour l'application	Zone de confiance
Protection des fichiers en temps réel	Protection des fichiers en temps réel
Utilisation du KSN	Utilisation de KSN
Protection contre les Exploits	Protection contre les Exploits
Analyseur AMSI	Scanner AMSI
Contrôle du lancement des applications	Contrôle du lancement des applications
Contrôle des appareils	Contrôle des appareils
Gestion du pare-feu	Pare-feu Le pare-feu Windows agit comme le pare-feu de Kaspersky Embedded Systems Security 3.4, tandis que l'application gère le pare-feu Windows. Dans Kaspersky Embedded Systems Security 4.1, un module distinct est responsable de la fonctionnalité pare-feu.
Protection contre les menaces réseau	Protection contre les menaces réseau
Contrôle de l'intégrité des fichiers	Contrôle de l'intégrité du système Les fonctionnalités des modules Contrôle de l'intégrité des fichiers et Surveillance de l'accès au registre ont été fusionnées dans le module Contrôle de l'intégrité du système.
Inspection des journaux	Inspection des journaux
Surveillance d'accès au registre	Contrôle de l'intégrité du système Les fonctionnalités des modules Contrôle de l'intégrité des fichiers et Surveillance de l'accès au registre ont été fusionnées dans le module Contrôle de l'intégrité du système.
(aucun)	Détection comportementale
(aucun)	Réparation des actions malicieuses

Module de Kaspersky Embedded Systems Security 3.4	Module de Kaspersky Embedded Systems Security 4.1
Tâche de Kaspersky Embedded Systems Security 3.4	**Tâche de Kaspersky Embedded Systems Security 4.1**
Activation de l'application	Activation de l'application
Copie des mises à jour	Mise à jour Les fonctionnalités de la tâche Copie des mises à jour ont été fusionnées dans la tâche Mise à jour.
Surveillance de l'intégrité des fichiers	Contrôle de l'intégrité du système par rapport à une référence
Mise à jour des bases de l'application	Mise à jour Les fonctionnalités de la tâche Mise à jour de la base de données ont été fusionnées dans la tâche Mise à jour.
Mise à jour des modules de l'application	Mise à jour Les fonctionnalités de la tâche Mise à jour des modules de l'application ont été fusionnées dans la tâche Mise à jour.
Annulation de la mise à jour des bases de l'application	Annulation de la mise à jour
Analyse à la demande	Analyse à la demande
Vérification de l'intégrité de l'application	Vérification de l'intégrité de l'application
Génération des règles du Contrôle du lancement des applications	Générateur de règles pour le Contrôle du lancement des applications
Générateur de règles pour le Contrôle des appareils	Générateur de règles pour le Contrôle des appareils
(aucun)	Protection de la connexion au Serveur d'administration
(aucun)	Modifier les modules de Kaspersky Embedded Systems Security
(aucun)	Réinitialisation de l'état d'intégrité du système

Interface de l'application

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

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

Console d'administration de Kaspersky Security Center

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

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

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (ci-après également appelé Web Console) est une application Web destinée à l'exécution centralisée des principales tâches d'administration et de maintenance du système de sécurité du réseau d'une organisation. Kaspersky Security Center Web Console est un module de Kaspersky Security Center qui fournit une interface utilisateur. Pour obtenir de plus amples informations sur Kaspersky Security Center Web Console, veuillez consulter l'aide de Kaspersky Security Center.

Les actions suivantes sont disponibles pour Web Console :

- Surveiller l'état du système de sécurité de votre organisation.
- installer des applications de Kaspersky sur les appareils de votre réseau ;
- administrer les applications installées ;
- consulter les rapports sur l'état du système de la sécurité.

Utilisation du plug-in d'administration

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

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

Vous pouvez gérer de manière centralisée plusieurs appareils protégés dotés de Kaspersky Embedded Systems Security et inclus dans le même groupe d'administration via le Plug-in d'administration de Kaspersky Embedded Systems Security. Kaspersky Security Center vous permet également de configurer séparément les paramètres de fonctionnement de chaque appareil protégé inclus dans le groupe d'administration.

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

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

Aucune action supplémentaire n'est requise pour lancer le plug-in Kaspersky Embedded Systems Security dans Kaspersky Security Center. Après l'installation du plug-in d'administration sur l'appareil protégé de l'administrateur, le lancement s'opère en même temps que n'importe quel type de Console d'administration de Kaspersky Security Center.

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

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

  Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches de protection en temps réel de l'ordinateur, les tâches de contrôle des activités sur les appareils, les tâches de protection du stockage réseau et les paramètres de lancement planifié des tâches du système local.

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

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

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

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

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Embedded Systems Security dans la Console d'administration de Kaspersky Security Center.

Configuration des paramètres généraux de l'application dans Kaspersky Security Center

Vous pouvez configurer les paramètres généraux de Kaspersky Embedded Systems Security depuis Kaspersky Security Center pour un groupe d'appareils protégés ou pour un appareil protégé individuel.

Configuration de l'interface et de l'analyse dans Kaspersky Security Center

Pour configurer les paramètres d'optimisation et l'interface de l'application, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer les paramètres d'une tâche ou d'une application pour un appareil protégé particulier, sélectionnez l'onglet **Appareils** et accédez aux paramètres locaux de la tâche ou de l'application.
4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Paramètres** dans la sous-section **Paramètres de l'interface**.

5. Configurez les paramètres suivants dans la fenêtre **Paramètres de l'interface**, sous l'onglet **Général** :

   - Dans la section **Interaction avec l'utilisateur**, décidez si l'icône de l'application doit apparaître dans l'Icône de la barre d'état système après le lancement de l'application.

     - **Afficher l'interface utilisateur**. Sur l'ordinateur client, l'icône est disponible dans la barre d'état système Windows. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer des opérations avec Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security affiche également des notifications au-dessus de l'icône de l'application. Le menu contextuel de l'icône dans la barre d'état système de Windows permet d'ouvrir l'interface de diagnostic compacte. Un lien dans l'interface de diagnostic compacte ouvre la Console de l'application.

     - **Ne pas afficher l'interface utilisateur**. L'ordinateur client n'affiche aucun élément pouvant indiquer le fonctionnement de Kaspersky Embedded Systems Security. De même, l'icône dans la zone de notification Windows et les notifications ne sont pas disponibles.

   - Dans la section **États**, vous pouvez spécifiez les avertissements que vous souhaitez voir sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security.

6. Cliquez sur le bouton **OK**.

Les paramètres d'application définis seront enregistrés.

Configuration des paramètres de sécurité dans Kaspersky Security Center

Pour configurer manuellement les paramètres de sécurité :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

   - Pour configurer les paramètres d'une tâche ou d'une application pour un appareil protégé particulier, sélectionnez l'onglet **Appareils** et accédez aux paramètres locaux de la tâche ou de l'application.

4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Paramètres** dans la sous-section **Sécurité et fiabilité**.

5. Configurez les paramètres suivants dans la fenêtre **Paramètres de sécurité**, sous l'onglet **Sécurité** :

   - Dans la section **Général**, nous vous recommandons de laisser la fonctionnalité **Lancer l'application au démarrage de l'ordinateur (recommandé)** activée (par défaut).

   - Dans la section **Autodéfense**, activez ou désactivez la fonctionnalité **Protéger les processus d'application contre les menaces externes**.

   - La section **Actions lors du passage à la source d'alimentation de secours** permet de limiter la charge de Kaspersky Embedded Systems Security sur l'appareil protégé dans le cadre de l'alimentation de secours :

     - **Ne pas lancer les tâches d'analyse programmées**

- Arrêter d'exécuter les tâches d'analyse

- Dans la section **État de l'ordinateur à l'application des paramètres**, configurez l'affichage de l'état des ordinateurs clients sur lesquels l'application est installée si des erreurs surviennent lors de l'application d'une stratégie ou de l'exécution d'une tâche.

- Configurez le paramètres **Compatibilité avec les logiciels d'administration à distance** dans la section **Paramètres de compatibilité**.

6. Sous l'onglet **Paramètres d'analyse**, configurez les paramètres de la tâche suivants :

   - **Limiter l'utilisation du processeur pour les tâches d'analyse**. Kaspersky Embedded Systems Security n'utilise jamais le processeur de l'appareil protégé dans les tâches d'analyse à la demande au-delà de la valeur du champ **Limite supérieure**. L'activation de cette option peut avoir une incidence négative sur les performances de Kaspersky Embedded Systems Security.

   - **Céder les ressources aux autres applications**. La consommation des ressources de l'ordinateur par Kaspersky Embedded Systems Security lors de l'analyse de l'ordinateur peut augmenter la charge des sous-systèmes du processeur et du disque dur. Ce processus peut ralentir d'autres applications. Pour optimiser les performances, Kaspersky Embedded Systems Security propose un mode de transfert des ressources vers d'autres applications. Dans ce mode, le système d'exploitation peut réduire la priorité des tâches d'analyse de Kaspersky Embedded Systems Security lorsque la charge du processeur est élevée. Cette fonction permet de redistribuer les ressources du système d'exploitation à d'autres applications. Le processeur consacrera donc moins de ressources aux tâches d'analyse. Par conséquent, Kaspersky Embedded Systems Security mettra plus de temps à analyser l'ordinateur. Le mode de transfert des ressources vers d'autres applications est activé par défaut.

7. Cliquez sur **OK**.

Les paramètres définis de sécurité et de fiabilité sont enregistrés.

Configuration des paramètres de connexion dans Kaspersky Security Center

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Embedded Systems Security et les serveurs de mise à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services Kaspersky Security Network.

Pour configurer les paramètres de la connexion, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.

3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :

   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**

   - Pour configurer les paramètres d'une tâche ou d'une application pour un appareil protégé particulier, sélectionnez l'onglet **Appareils** et accédez aux paramètres locaux de la tâche ou de l'application.

4. Dans la section **Paramètres de l'application**, cliquez sur le bouton **Paramètres** dans la sous-section **Paramètres de connexion**.

   La fenêtre **Paramètres de connexion** s'ouvre.

5. Dans la section **Serveur proxy**, cliquez sur **Paramètres**.

6. Une fenêtre s'ouvre. Dans cette fenêtre, dans le **Paramètres du serveur proxy**, sélectionnez une option de gestion des paramètres de proxy :

   - **Ne pas utiliser de serveur proxy**. Si cette option est sélectionnée, Kaspersky Embedded Systems Security n'utilise pas de serveur proxy.
   - **Définir automatiquement les paramètres du serveur proxy.** Si cette option est sélectionnée, Kaspersky Embedded Systems Security utilise les paramètres de proxy du système d'exploitation.
   - **Utiliser les paramètres indiqués du serveur proxy**. Si cette option est sélectionnée, Kaspersky Embedded Systems Security utilise les paramètres du serveur proxy indiqués manuellement. Saisissez l'adresse IP ou le nom symbolique du serveur proxy et le numéro de port

     Le cas échéant, décochez la case **Ne pas utiliser de serveur proxy pour les adresses locales**. Si la fonctionnalité est activée, les échanges avec les autres appareils du réseau auquel appartient l'appareil protégé disposant de Kaspersky Embedded Systems Security se font directement. Cette option est activée par défaut.

7. Dans la section **Paramètres d'authentification du serveur proxy**, sélectionnez, dans la liste déroulante, le mode d'authentification sur le serveur proxy :

   a. Si vous avez sélectionné **Définir automatiquement les paramètres du serveur proxy** :

      - **Ne pas utiliser l'authentification**.
      - **Authentification NTLM**. Authentification NTLM avec le compte utilisateur actuel (par défaut).
      - **Authentification Kerberos**. Authentification Kerberos avec le compte utilisateur actuel.

   b. Si vous avez sélectionné **Utiliser les paramètres indiqués du serveur proxy** :

      - **Ne pas utiliser l'authentification**.
      - **Authentification NTLM**. Authentification NTLM avec le compte utilisateur actuel (par défaut).
      - **Authentification NTLM avec nom d'utilisateur et mot de passe**. Authentification NTLM avec des identifiants spécifiés manuellement.
      - **Authentification Kerberos**. Authentification Kerberos avec le compte utilisateur actuel.

        Pour garantir le bon fonctionnement de l'authentification Kerberos lorsque vous utilisez des enregistrements CNAME pour l'adresse du serveur proxy, vous devez enregistrer un Service Principal Name (SPN) pour chaque enregistrement CNAME.

      - **Authentification Kerberos avec nom d'utilisateur et mot de passe**. Authentification Kerberos avec des identifiants spécifiés manuellement.
      - **Nom d'utilisateur et mot de passe**. Authentification avec des identifiants spécifiés manuellement.

Si nécessaire, saisissez un nom d'utilisateur et un mot de passe.

Si l'authentification Kerberos est sélectionnée, Kaspersky Embedded Systems Security peut, en fonction de la configuration du serveur proxy, procéder à l'authentification selon le protocole Kerberos ou NTLM.

8. Dans la section **Licence**, cochez ou décochez la case **Utiliser Kaspersky Security Center comme serveur proxy lors de l'activation de l'application**.

9. Cliquez sur **OK**.

10. Dans la section **Ports contrôlés**, spécifiez une option pour le port réseau :

    - **Contrôler tous les ports réseau**. Le mode de contrôle des ports de réseau via lesquels les modules de la protection contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur.

    - **Surveiller uniquement les ports réseau sélectionnés**. Dans ce mode de surveillance des ports réseau, les modules de la protection surveillent les ports sélectionnés de l'ordinateur ainsi que l'activité réseau des applications sélectionnées. La liste des ports qui sont normalement utilisés pour le transfert des messages électroniques et le trafic réseau, configurée conformément aux recommandations des experts de Kaspersky. Si nécessaire, vous pouvez modifier la liste des ports réseau.

11. Cliquez sur le bouton **Paramètres** et modifiez les paramètres suivants :

    - **Contrôler tous les ports pour les applications de la liste recommandée par Kaspersky**. Kaspersky Embedded Systems Security surveille les ports réseau des applications à partir de la liste prédéfinie. Par exemple, cette liste comprend Google Chrome, Adobe Reader, Java et d'autres applications.

    - **Contrôler tous les ports pour les applications indiquées**. Kaspersky Embedded Systems Security surveille les ports réseau des applications ajoutées à la liste.

12. Cliquez sur **OK**.

Les paramètres de la connexion définis seront enregistrés.

Configuration du mode d'exécution des tâches locales

Vous pouvez utiliser des stratégies pour autoriser ou interdire le lancement de la tâche locale du système d'analyse à la demande et de la tâche de mise à jour. Cela s'opère selon la planification configurée localement sur chaque appareil protégé du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'appareil protégé selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.

- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Le lancement des tâches locales du système est interdit par défaut par la stratégie.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont administrées via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de mise à jour de groupe ou d'analyse à la demande, autorisez le lancement des tâches locales du système dans la stratégie : Kaspersky Embedded Systems Security réalise la mise à jour des bases de l'application et des modules et lance également toutes les tâches locales du système d'analyse à la demande conformément à la programmation par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâche d'analyse à la demande : *Analyse des zones critiques*, *Analyse au démarrage du système d'exploitation*, *Vérification de l'intégrité de l'application*, *Contrôle de l'intégrité du système par rapport à une référence*.
- Tâches de mise à jour : *Mise à jour des bases et des modules d'application*, *Mise à jour de l'application*.

Si vous excluez l'appareil protégé du groupe d'administration, la planification des tâches locales du système sera automatiquement activée.

Pour autoriser ou interdire la gestion de la planification du lancement des tâches locales de l'application dans une stratégie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, ouvrez le groupe souhaité, puis dans le panneau des résultats, sélectionnez l'onglet **Stratégies**.
2. Sous l'onglet **Stratégies**, ouvrez le menu contextuel de la stratégie pour laquelle vous souhaitez configurer le lancement planifié des tâches locales du système de Kaspersky Embedded Systems Security sur le groupe d'appareils protégés et choisissez **Propriétés**.
3. Dans la stratégie des propriétés de l'ordinateur, sélectionnez la section **Paramètres de l'application**.
4. Cliquez sur **Paramètres** dans la sous-section **Exécuter les tâches du système local**.
5. Cochez la case **Autoriser l'utilisation des tâches locales**.
6. Cochez la case **Autoriser la gestion de la planification** pour autoriser ou interdire l'administration de la planification du lancement des tâches locales de l'application.

Configuration des paramètres de la Sauvegarde dans Kaspersky Security Center

Pour configurer les paramètres de la Sauvegarde dans Kaspersky Security Center, procédez comme suit :

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
3. Dans le panneau de détails du groupe d'administration sélectionné, exécutez une des actions suivantes :
   - Pour configurer les paramètres de l'application pour un groupe d'appareils protégés, sélectionnez l'onglet **Stratégies** et ouvrez la fenêtre **Propriétés : <Nom de la stratégie>**
   - Pour configurer les paramètres d'une tâche ou d'une application pour un appareil protégé particulier, sélectionnez l'onglet **Appareils** et accédez aux paramètres locaux de la tâche ou de l'application.

4. Passez à la section **Complémentaire**.

5. Cliquez sur le bouton **Paramètres** dans la sous-section **Stockages**.

6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres du stockage

Paramètre	Description
Sous l'onglet **Rapports**, spécifiez les paramètres des rapports suivants :	
Supprimer les rapports après	Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des rapports est de 30 jours. À l'issue de cette période, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport.
Limiter la taille du fichier des rapports à	Si la case est cochée, la taille maximale du fichier de rapport est limitée par la valeur renseignée. Par défaut, la taille maximale du fichier est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale.
Sous l'onglet **Sauvegarde**, spécifiez les paramètres de sauvegarde suivants :	
Supprimer les objets après	Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Embedded Systems Security supprime les fichiers les plus anciens de la sauvegarde.
Limiter la taille de la Sauvegarde à	Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 400 Mo. Une fois que la Sauvegarde a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les fichiers les plus anciens dans afin que le volume de la Sauvegarde ne dépasse plus la valeur maximale.
Valeur du seuil de l'espace disponible	La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (100 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil, Kaspersky Embedded Systems Security consigne l'événement *Dépassement du seuil d'espace libre disponible dans la sauvegarde* 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 **Valeur du seuil de l'espace disponible** est active si la case **Limiter la taille de la Sauvegarde à** est cochée.

Création et configuration des stratégies

Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Embedded Systems Security sur plusieurs appareils protégés.

Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs appareils sur lesquels Kaspersky Embedded Systems Security est installé.

Une stratégie applique les paramètres de Kaspersky Embedded Systems Security ainsi que ses fonctions et ses tâches spécifiées à l'ensemble des appareils protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans la Console d'administration, la stratégie active dans le groupe en ce moment possède l'état *Actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Embedded Systems Security. Vous pouvez les consulter dans la console de l'application dans le nœud **Inspection des journaux**.

Kaspersky Security Center offre une méthode pour appliquer les stratégies aux appareils protégés : *Interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Embedded Systems Security utilise les valeurs des paramètres pour lesquels vous avez sélectionné l'icône **Modification interdite** dans les propriétés de la stratégie. Dans ce cas, Kaspersky Embedded Systems Security n'utilise pas les valeurs des paramètres en vigueur avant l'application de la stratégie. Les paramètres de la stratégie active pour lesquels vous avez sélectionné l'icône **Modification autorisée** ne sont pas appliqués par Kaspersky Embedded Systems Security.

Si une stratégie est active, les paramètres dans la Console de l'application qui sont accompagnés de l'icône dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres peuvent être modifiées dans la Console de l'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône empêchent également la modification des paramètres dans Kaspersky Security Center pour un appareil protégé dans la fenêtre **Propriétés : <Nom de l'appareil protégé>**.

Les paramètres configurés et transmis à l'appareil protégé à l'aide de la stratégie active sont enregistrés dans les paramètres de tâche locale après la désactivation de la stratégie active.

Si une stratégie définit les paramètres d'une tâche de protection en temps réel de l'ordinateur ou de protection des stockages réseau, les paramètres définis par la stratégie sont modifiés immédiatement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

Création d'une stratégie

Avant de créer une stratégie, vous devez installer le plug-in d'administration klcfginst.exe.

Pour créer une stratégie pour un groupe d'appareils protégés où l'application est installée et exécutée :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration contenant les appareils protégés pour lesquels vous souhaitez créer une stratégie.

2. Dans le panneau de résultats du groupe d'administration sélectionné, choisissez l'onglet **Stratégies** et cliquez sur le lien **Nouvelle stratégie** pour démarrer l'Assistant de création d'une stratégie.

   La fenêtre **Assistant de création de la stratégie** s'ouvre.

3. Dans la fenêtre **Sélection d'une application pour créer une stratégie de groupe**, sélectionnez Kaspersky Embedded Systems Security.

4. Cliquez sur **Suivant**.

5. Entrez un nom de stratégie de groupe dans le champ **Nom**.

   Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ |` .

6. Pour appliquer une configuration de stratégie employée dans une version antérieure de l'application :

   a. Cochez la case **&Utiliser les paramètres de stratégie d'une version antérieure de l'application**.

   b. Cliquez sur **Parcourir**.

   c. Sélectionnez la stratégie que vous souhaitez appliquer.

   d. Cliquez sur **Suivant**.

7. Dans la fenêtre **Sélection du type d'opération**, dans le groupe **Configurer la Protection des fichiers en temps réel**, cochez la case **Activer la Protection des fichiers en temps réel** et indiquez le niveau de sécurité.

   Si le mode d'exécution de la tâche n'est pas sélectionné, vous ne pouvez pas passer à l'étape suivante de l'Assistant de nouvelle stratégie.

8. Configurez la Protection en temps réel de l'ordinateur.

9. Configurez les exclusions d'analyse prédéfinies et les applications de confiance.

10. Sélectionnez l'un des états de stratégie suivants dans la fenêtre **Création d'une stratégie de groupe pour l'application** :

    - **Stratégie active**, si vous voulez que la stratégie entre en vigueur immédiatement après sa création. Si le groupe contient déjà une stratégie active, celle-ci est désactivée et une nouvelle stratégie est appliquée.
    - **Stratégie inactive**, si vous ne voulez pas appliquer immédiatement la stratégie créée. Vous pourrez activer cette stratégie plus tard.
    - **Stratégie pour les utilisateurs autonomes**, la stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.
    - Cochez la case **Ouvrez les propriétés de la stratégie immédiatement après sa création** pour fermer automatiquement l'**Assistant de création de la stratégie** et configurez la stratégie créée après avoir cliqué sur le bouton **Suivant**.

11. Cliquez sur **Terminer**.

    La stratégie créée sera affichée dans la liste des stratégies sous l'onglet **Stratégies** du groupe d'administration sélectionné. La fenêtre **Propriétés : <nom de la stratégie>** permet de configurer d'autres paramètres, tâches et fonctions de Kaspersky Embedded Systems Security.

Après la création d'une stratégie, un ensemble de règles d'autorisation est créé pour empêcher le blocage des applications et garantir leur fonctionnement ininterrompu.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau entrant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le processus de partage du bureau Windows à l'aide de l'Agent d'administration de Kaspersky Security Center, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le port local 15000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau sortant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le service Kaspersky Embedded Systems Security Service, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le processus de travail de Kaspersky Embedded Systems Security, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le port local 13000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.

Configuration d'une stratégie

Pour configurer les paramètres d'une stratégie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**.
2. Développez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de la stratégie associée et ouvrez l'onglet **Stratégies** dans le panneau de détails.
3. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

   Ouvrez la fenêtre **Propriétés : <Nom de la stratégie>** à l'aide d'une des méthodes suivantes :

   - Dans le menu contextuel de la stratégie, sélectionnez l'option **Propriétés**.
   - Double-cliquez sur la stratégie sélectionnée.
4. Activez ou désactivez l'application de la stratégie dans la section **État de la stratégie** de l'onglet **Général**. Pour ce faire, sélectionnez l'une des options suivantes :

   - **Stratégie active**, si vous souhaitez que la stratégie s'applique à tous les appareils protégés appartenant au groupe d'administration sélectionné.
   - **Stratégie pour les utilisateurs autonomes**, la stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.
   - **Stratégie inactive**, si vous souhaitez activer la stratégie plus tard sur tous les appareils protégés appartenant au groupe d'administration sélectionné.
5. Configurez les paramètres de l'application dans les autres sections de la stratégie.

Vous pouvez activer ou désactiver l'exécution de n'importe quelle tâche sur tous les appareils protégés appartenant au groupe d'administration à l'aide d'une stratégie de Kaspersky Security Center.

Vous pouvez configurer l'application des paramètres définis dans la stratégie sur tous les appareils protégés du réseau pour chaque module distinct de l'application.

6. Cliquez sur le bouton **OK**.

Les paramètres définis seront appliqués dans la stratégie.

Indicateur du niveau de protection

L'indicateur de niveau de sécurité s'affiche en haut de la fenêtre des propriétés de la stratégie. L'indicateur peut prendre une des valeurs suivantes :

- **Niveau de protection élevé**. L'indicateur prend cette valeur et passe au vert si tous les modules appartenant aux catégories suivantes sont activés et marqués d'un :
  - **Critique**. Cette catégorie contient les modules suivants :
    - Protection des fichiers en temps réel.
    - Détection comportementale.
    - Protection contre les Exploits.
    - Réparation des actions malicieuses.
    - Activer les notifications de la fonctionnalité Bureau sécurisé.
  - **Important**. Cette catégorie contient le module Utilisation de KSN.
- **Niveau de protection moyen**. L'indicateur prend cette valeur et passe au jaune si un module important est désactivé ou marqué d'un .
- **Niveau de protection faible**. L'indicateur prend cette valeur et passe au rouge si un ou plusieurs modules critiques sont désactivés ou marqués d'un .

Si l'indicateur affiche la valeur **Niveau de protection moyen** ou **Niveau de protection faible**, un lien à droite de l'indicateur ouvre la fenêtre **Modules de protection recommandés**. Cette fenêtre permet d'activer et d'interdire la désactivation des modules de protection recommandés.

Création et configuration de tâches via Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Embedded Systems Security, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

À propos de la création de tâches dans Kaspersky Security Center

Vous pouvez créer des tâches de groupe pour des groupes d'administration et pour des sélections d'appareils protégés. Vous pouvez créer les types de tâches suivants via Kaspersky Security Center :

- *Activation de l'application*
- *Protection de la connexion au Serveur d'administration*
- *Modifier les modules de Kaspersky Embedded Systems Security*
- *Contrôle de l'intégrité du système par rapport à une référence*
- *Mise à jour*
- *Annulation de la mise à jour*
- *Analyse à la demande*
- *Vérification de l'intégrité de l'application*
- *Suppression de la clé*
- *Générateur de règles pour le Contrôle du lancement des applications*
- *Générateur de règles pour le Contrôle des appareils*.

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- Pour un appareil protégé donné dans la section **Tâches**.
- Pour un groupe d'administration : dans le panneau de détails du nœud du groupe d'appareils protégés sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'appareils protégés : dans le panneau de détails du nœud **Sélections d'appareils**.

Les stratégies permettent de désactiver les planifications pour les tâches système locales *Mise à jour* et *Analyse à la demande* sur tous les appareils protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le *Système d'aide de Kaspersky Security Center*.

Création d'une tâche dans Kaspersky Security Center

Pour créer une tâche dans la console d'administration de Kaspersky Security Center, procédez comme suit :

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :

   - Pour créer une tâche locale :

     a. Dans l'arborescence de la Console d'administration, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient le serveur protégé.

     b. Dans le panneau des résultats, sous l'onglet **Appareils**, ouvrez le menu contextuel de l'appareil protégé et sélectionnez **Propriétés**.

     c. Dans la fenêtre qui s'ouvre, dans la section **Tâches**, cliquez sur le bouton **Ajouter**.

   - Pour créer une tâche de groupe :

     a. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.

     b. Sélectionnez le groupe d'administration pour lequel vous souhaitez créer une tâche.

     c. Dans le panneau des résultats, ouvrez l'onglet **Tâches** et sélectionnez **Nouvelle tâche**.

   La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la fenêtre **Sélection du type de tâche**, sous le titre **Kaspersky Embedded Systems Security**, sélectionnez le type de la tâche à créer.

3. Les paramètres peuvent varier en fonction du type de tâche :

   - Création d'une tâche d'analyse à la demande.

   - Si vous créez une des tâches de mise à jour, définissez les paramètres de la tâche conformément à vos exigences :

     a. Dans le groupe **Source des mises à jour**, vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.

     Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

     b. Configurez les paramètres d'une fonctionnalité qui réduit la charge sur le sous-système de disque :

c. Vous pouvez spécifier les actions que Kaspersky Embedded Systems Security exécutera si des mises à jour critiques des modules de l'application sont nécessaires et après l'installation des mises à jour critiques. En outre, vous pouvez indiquer si Kaspersky Embedded Systems Security recevra des informations sur les mises à jour planifiées disponibles.

d. Spécifiez l'ensemble des mises à jour à copier et le chemin d'accès au dossier qui sera utilisé par Kaspersky Embedded Systems Security pour stocker les mises à jour copiées.

- Pour créer la tâche *Activation de l'application*, procédez comme suit :

  a. Dans la fenêtre **Paramètres d'activation**, désignez le fichier clé ou le code d'activation que vous souhaitez utiliser pour activer l'application.

  b. Cochez la case **Utiliser comme clé supplémentaire** si vous souhaitez créer une tâche pour renouveler la licence.

- Créez la tâche Générateur de règles pour le Contrôle du lancement des applications.

- Créez la tâche Générateur de règles pour le Contrôle des appareils.

4. Programmez l'exécution de la tâche.

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

6. Si la tâche est créée pour une sélection d'appareils protégés, sélectionnez le réseau (ou le groupe) d'appareils protégés sur lesquels elle sera exécutée.

7. Dans la fenêtre **Sélection du compte utilisateur pour exécuter la tâche**, désignez le compte que vous souhaitez utiliser pour exécuter la tâche.

8. Dans la fenêtre **Définition du nom de la tâche**, saisissez le nom de la tâche (100 caractères maximum, et ne peut pas contenir les caractères `" * < > ? \ | :`).

   Nous vous conseillons d'ajouter le type de tâche à son nom (par exemple, « Analyse à la demande des dossiers partagés »).

9. Dans la fenêtre **Fin de la création de la tâche**, réalisez une des opérations suivantes :

   a. Cochez la case **&Lancer la tâche à la fin de l'Assistant** si vous souhaitez que la tâche démarre dès sa création.

   b. Cliquez sur **Terminer**.

La tâche créée apparaît dans la liste **Tâches**.

Accès aux paramètres locaux de la tâche et aux paramètres généraux de l'application pour un ordinateur

Si l'application est soumise à une stratégie de Kaspersky Security Center et que celle-ci interdit la modification des paramètres de l'application, vous ne pourrez pas modifier ces paramètres pour un ordinateur individuel.

Pour accéder aux paramètres des tâches locales pour un ordinateur individuel :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareil s administrés**.
2. Sélectionnez le groupe auquel appartient l'appareil protégé.
3. Dans le panneau des résultats, choisissez l'onglet **Appareils**.
4. Ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - dans le menu contextuel du nom de l'appareil protégé, sélectionnez **Propriétés**.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
5. Passez à la section **Tâches**.
6. Dans la liste des tâches, sélectionnez une tâche locale à configurer d'une des manières suivantes :
   - double-cliquez sur le nom de la tâche
   - sélectionnez une tâche dans la liste et cliquez sur le bouton **Propriétés**
   - dans le menu contextuel du nom de la tâche, sélectionnez l'**option Propriétés**.

   La fenêtre **Propriétés : <Nom de la tâche>** s'ouvre.

Pour accéder aux paramètres généraux de l'application pour un ordinateur individuel :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe auquel appartient l'appareil protégé.
2. Dans le panneau des résultats, choisissez l'onglet **Appareils**.
3. Ouvrez la fenêtre **Propriétés : <Nom de l'appareil>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de l'appareil protégé.
   - dans le menu contextuel du nom de l'appareil protégé, sélectionnez **Propriétés**.

   La fenêtre **Propriétés : <Nom de l'appareil protégé>** s'ouvre.
4. Passez à la section **Applications**.
5. Dans la liste des applications installées, sélectionnez Kaspersky Embedded Systems Security à l'aide d'une des méthodes suivantes :
   - double-cliquez sur le nom de Kaspersky Embedded Systems Security ;
   - sélectionnez Kaspersky Embedded Systems Security dans la liste, puis cliquez sur le bouton **Propriétés** ;
   - dans le menu contextuel du nom de Kaspersky Embedded Systems Security, sélectionnez l'élément **Propriétés**.

La fenêtre **Paramètres** de **Kaspersky Embedded Systems Security** s'ouvre.

Configuration des tâches de groupe dans Kaspersky Security Center

Pour configurer une tâche de groupe pour plusieurs appareils protégés, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Sélectionnez le nom de la tâche dans la liste des tâches créées et cliquez sur le lien **Configurer les paramètres de la tâche** ;
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.
5. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.
6. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
   - Pour configurer la tâche *Analyse à la demande*, procédez comme suit :
     - Dans la section **Zone d'analyse**, créez une zone d'analyse.
     - Dans la section **Paramètres**, configurez l'intégration aux autres modules de l'application et le niveau de priorité de la tâche.
   - Pour configurer la tâche *Mise à jour*, procédez comme suit :
     - Rendez-vous dans la section **Paramètres** et définissez le paramètre **Paramètres de la mise à jour des bases et des modules de l'application**.
     - Choisissez une action à effectuer : copiez et installez les mises à jour critiques des modules de l'application ou uniquement vérifier leur présence.

- Pour configurer la tâche *Activation de l'application*, procédez comme suit :
  - Dans la section **Paramètres**, désignez le fichier clé ou le code d'activation que vous souhaitez utiliser pour activer l'application.
  - Cochez la case **Utiliser comme clé supplémentaire** si vous souhaitez ajouter un code d'activation ou un fichier clé pour renouveler la licence.
- Pour configurer la tâche *Générateur de règles pour le Contrôle des appareils*, dans la section **Paramètres**, spécifiez les paramètres que vous souhaitez utiliser pour créer la liste des règles du Contrôle des appareils.

7. Configurez la planification des tâches dans la section **Planification**.
8. Dans la section **Compte**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.
9. Si nécessaire, dans la section **Exclusions de la zone d'action de la tâche**, spécifiez les objets que vous souhaitez exclure de la zone d'action de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.
10. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Les paramètres configurables des tâches de groupe sont listés ci-dessous.

- Générateur de règles pour le Contrôle du lancement des applications

  Lors de la configuration des paramètres de la tâche *Générateur de règles pour le Contrôle du lancement des applications*, vous pouvez choisir comment créer les règles d'autorisation sous l'onglet **Règles** :

  - **Créer des règles d'autorisation basées sur les applications lancées**
  - **Créer des règles d'autorisation pour les applications à partir des dossiers**

  Vous pouvez spécifier les actions suivantes à effectuer lors de la création des règles d'autorisation du Contrôle du lancement des applications sous l'onglet **Paramètres** :

  - **Utiliser le certificat numérique**
  - **Utiliser l'objet et l'empreinte du certificat numérique**
  - **Si le certificat est manquant, utiliser**
  - **Utiliser le hachage SHA256**
  - **Générer des règles pour les utilisateurs et/ou groupes d'utilisateurs**.

  Vous pouvez configurer les paramètres pour les fichiers de configuration contenant les listes de règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.

  Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

- Générateur de règles pour le Contrôle des appareils
  - Sélectionnez le mode de fonctionnement :tenir compte des données système relatives à tous les appareils de stockage de masse jamais connectés ou tenir compte uniquement des appareils externes connectés actuellement.
  - Configurez les paramètres pour les fichiers de configuration contenant les listes de règles d'autorisation que Kaspersky Embedded Systems Security crée à la fin des tâches.
  - Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
- Activation de l'application
  - Pour activer l'application ou renouveler la licence, vous pouvez ajouter un fichier clé ou un code d'activation.
  - Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
- Mise à jour des bases et des modules de l'application
  - Dans le groupe de paramètres **Source des mises à jour**, vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.

    Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.
  - Vous pouvez configurer les paramètres d'une fonctionnalité qui réduit la charge sur le sous-système de disque :
    - **Réduire la charge sur les I/O du disque**
    - **RAM utilisée pour l'optimisation, Mo**.
  - Vous pouvez spécifier les actions que Kaspersky Embedded Systems Security exécutera si des mises à jour critiques des modules de l'application sont nécessaires et après l'installation des mises à jour critiques. En outre, vous pouvez indiquer si Kaspersky Embedded Systems Security recevra des informations sur les mises à jour planifiées disponibles.
  - Vous pouvez spécifier l'ensemble des mises à jour à copier et le chemin d'accès au dossier qui sera utilisé par Kaspersky Embedded Systems Security pour stocker les mises à jour copiées.
  - Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.
- Analyse à la demande
  - Vous pouvez définir une zone d'analyse pour la tâche d'analyse à la demande et accéder à la configuration du niveau de sécurité.
  - Le groupe de paramètres **Heuristic analyzer** permet d'activer ou de désactiver l'utilisation de l'analyse heuristique pour la tâche d'analyse à la demande et de définir le niveau d'analyse à l'aide d'un curseur.

- Le groupe **Integration with other components** permet de configurer les paramètres suivants :
  - Lancer la tâche d'analyse en arrière-plan.
  - Considérer l'exécution de la tâche comme une analyse rapide.
  - Désactiver le lancement simultané de plusieurs tâches d'analyse.
- Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

- Vérification de l'intégrité de l'application
  - Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

- Contrôle de l'intégrité du système par rapport à une référence
  - Vous pouvez configurer le mode de surveillance et les règles qui spécifient les actions à entreprendre sur les fichiers, le registre et les appareils.
  - Vous pouvez configurer les paramètres pour lancer la tâche selon une programmation.

Tâche d'activation de l'application

Pour configurer la tâche Activation de l'application, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.
2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.
3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.
4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :
   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

   Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.
5. Dans la section **Paramètres d'activation**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser comme clé supplémentaire** si vous souhaitez ajouter une clé pour renouveler la licence.
6. Dans la section **Planification**, configurez les paramètres de la planification de la tâche.

7. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le Système d'aide de Kaspersky Security Center.

8. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Tâche Mise à jour

Pour configurer la tâche Mise à jour, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.

4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

   - Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
   - Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

5. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.

6. Dans la fenêtre **Paramètres**, effectuez les actions suivantes :

   a. Sélectionnez une source des mises à jour à l'aide du bouton **Paramètres** dans la section **Paramètres de la mise à jour des bases et des modules de l'application** :

      - Serveur d'administration de Kaspersky Security Center.
      - Serveurs de mise à jour de Kaspersky.
      - Serveurs HTTP, FTP ou dossiers réseau personnalisés.

      Pour utiliser un dossier SMB partagé comme source de mise à jour, vous devez renseigner un compte utilisateur pour démarrer une tâche.

      Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

b. Configurez les paramètres d'une fonctionnalité qui réduit la charge sur le sous-système de disque :

- **Réduire la charge sur les I/O du disque**. La case active ou désactive la fonction d'optimisation du sous-système disque grâce au placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive. Par défaut, la case est décochée.
- **RAM utilisée pour l'optimisation, Mo**

c. Spécifiez les actions que Kaspersky Embedded Systems Security doit effectuer lorsque des mises à jour critiques des modules de l'application sont disponibles ou lorsqu'il existe des informations sur les mises à jour planifiées.

d. Spécifiez les paramètres de copie des mises à jour.

7. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche Annulation de la mise à jour).

8. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le Système d'aide de Kaspersky Security Center.

9. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

S'agissant de la tâche *Annulation de la mise à jour*, vous pouvez configurer uniquement les paramètres de tâche standard contrôlée par Kaspersky Security Center dans les sections **Notifications** et **Exclusions de la zone d'analyse**. Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le Système d'aide de Kaspersky Security Center.

Vérification de l'intégrité de l'application

Pour configurer la tâche de groupe Vérification de l'intégrité de l'application :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés** et sélectionnez le groupe d'administration dont vous souhaitez configurer les tâches d'application.

2. Dans le panneau de détails d'un groupe d'administration sélectionné, ouvrez l'onglet **Tâches**.

3. Dans la liste des tâches de groupe précédemment créées, sélectionnez une tâche que vous souhaitez configurer.

4. Ouvrez la fenêtre **Propriétés : <Nom de la tâche>** à l'aide d'une des méthodes suivantes :

- Double-cliquez sur le nom de la tâche dans la liste des tâches créées.
- Ouvrez le menu contextuel du nom de la tâche dans la liste des tâches créées, puis choisissez l'option **Propriétés**.

5. Dans la section **Notification**, configurez les paramètres de notification sur les événements de la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.

6. Dans la section **Appareils**, choisissez les appareils pour lesquels vous souhaitez configurer la tâche *Vérification de l'intégrité de l'application*.

7. Dans la section **Planification**, configurez les paramètres de la planification de la tâche.

8. Dans la section **Compte utilisateur**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche.

9. Si nécessaire, indiquez dans la section **Exclusions de la zone d'action de la tâche** les objets que vous souhaitez exclure de la zone d'action de la tâche.

   Vous trouverez plus d'informations sur la configuration des paramètres de ces sections dans le Système d'aide de Kaspersky Security Center.

10. Dans la fenêtre **Propriétés : <Nom de la tâche>**, cliquez sur le bouton **OK**.

Planification des tâches

Pour planifier des tâches à l'aide du plug-in d'administration :

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client requis.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Ouvrez les propriétés de l'ordinateur d'un double clic.

4. Passez à la section **Tâches**.

5. Double-cliquez pour ouvrir la fenêtre des propriétés de la tâche dont vous souhaitez configurer la planification.

6. Sélectionnez la section **Programmation**.

7. Configurez les paramètres de la planification (cf. tableau ci-après).

   Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée de ces tâches est interdite par une stratégie de Kaspersky Security Center.

8. Cliquez sur le bouton **Appliquer** pour enregistrer les paramètres de lancement de la tâche.

Si vous souhaitez configurer les paramètres de l'application pour une tâche unique à l'aide de Kaspersky Security Center, consultez la section Configuration des tâches locales dans la fenêtre des paramètres de l'application dans Kaspersky Security Center.

Paramètres de planification de la tâche

Paramètre	Description
Lancement planifié	Sélectionnez le mode de fonctionnement de la tâche : • **Toutes les N heures**. La tâche sera exécutée périodiquement toutes les quelques heures. Spécifiez l'heure de lancement de la tâche et la période en heures. • **Tous les N jours**. La tâche sera exécutée périodiquement tous les quelques jours. Spécifiez l'heure de lancement de la tâche et la période en jours. • **Toutes les N minutes**. La tâche sera exécutée périodiquement toutes les quelques minutes. Spécifiez l'heure de lancement de la tâche et la période en minutes. • **Chaque semaine**. La tâche sera exécutée un certain jour de la semaine. Indiquez le jour de la semaine et l'heure de début. • **Chaque mois**. La tâche sera exécutée un certain jour du mois. Spécifiez la date et l'heure de lancement. • **Une fois**. La tâche sera exécutée une fois à la date et à l'heure indiquées. • **Manuellement**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. • **Lors du téléchargement des mises à jour sur les stockages**. La tâche sera exécutée chaque fois que des mises à jour seront téléchargées dans le stockage. • **À la fin d'une autre tâche**. La tâche sera exécutée dès qu'une autre tâche aura terminé. Sélectionnez la tâche et son état d'achèvement. Kaspersky Embedded Systems Security ne prend pas en charge le mode **À la fin d'une autre tâche** pour la planification des tâches locales. • **Lors de la détection d'une propagation de virus**. La tâche sera exécutée si une attaque de virus est détectée. • **Au lancement de l'application**. La tâche sera exécutée à chaque lancement de Kaspersky Embedded Systems Security.
Lancer les tâches non exécutées	Si la case est cochée, Kaspersky Embedded Systems Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Embedded Systems Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Adopter un décalage aléatoire automatique pour les lancements de tâche	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche	Si la case est cochée, le système d'exploitation de l'ordinateur dispose d'un délai déterminé pour terminer le lancement avant l'exécution de la tâche. Le délai par défaut est de 5 minutes. Cochez la case si vous souhaitez exécuter la tâche sur tous les ordinateurs, y compris sur les ordinateurs éteints.
Arrêter les appareils après la fin de la tâche	Si cette case est cochée, l'ordinateur s'éteint une fois la tâche terminée. Par exemple, vous pouvez activer cette fonctionnalité pour analyser l'ordinateur le vendredi après les heures de travail. Une fois la tâche terminée, l'application éteint l'ordinateur pour le week-end.
Arrêter la tâche si elle prend plus de	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Embedded Systems Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Embedded Systems Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.

Paramètre	Description
Suspendre la tâche	Vous pouvez définir un intervalle de temps pendant lequel l'exécution d'une tâche précédemment planifiée sera suspendue. Une fois la période définie écoulée, la tâche reprend. Cela peut s'avérer nécessaire, par exemple, pour limiter l'impact de Kaspersky Embedded Systems Security sur les performances de votre ordinateur pendant les périodes de forte utilisation. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.
Désactiver la planification à partir du	Si la case est cochée, Kaspersky Embedded Systems Security arrêtera l'exécution de la tâche planifiée à partir de la date indiquée. La tâche sera définie en mode **Manuellement**. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.

Rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils sont basés sur les informations stockées sur le serveur d'administration.

À partir de la version Kaspersky Security Center 11, les types de rapport suivants sont disponibles pour Kaspersky Embedded Systems Security :

- Rapport sur l'état des modules de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Pour en savoir plus sur l'utilisation des rapports de Kaspersky Security Center, consultez l'aide de Kaspersky Security Center.

Rapport sur l'état des modules de Kaspersky Embedded Systems Security

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée de l'ensemble de modules défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque module : *Exécution en cours*, *En pause*, *Arrêté*, *Non couvert par la licence*.

L'état *Non installé* fait référence au module, et non à l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de modules et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de modules et leur état.

Cf. Aide de Kaspersky Security Center pour plus de détails sur la création et l'utilisation de sélections.

Pour consulter les états de module dans les paramètres de l'application :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**, puis sélectionnez le groupe d'administration pour lequel vous souhaitez configurer les paramètres de l'application.
2. Sélectionnez l'onglet **Appareils**, puis ouvrez la fenêtre **Paramètres de l'application**.
3. Sélectionnez la section **Modules**.
4. Consultez le tableau d'état.

Pour consulter un rapport standard Kaspersky Security Center :

1. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.
2. Sélectionnez l'onglet **Rapports**.
3. Double-cliquez sur l'élément de liste **Rapport sur l'état des modules de l'application**.

   Un rapport est généré.
4. Consultez les détails de rapport suivants :
   - Diagramme graphique.
   - Tableau récapitulatif des modules et nombres totaux d'appareils de réseau où chacun des modules est installé et groupes auxquels ils appartiennent.
   - Tableau détaillé spécifiant l'état des modules, la version, l' et le groupe.

Rapports sur les applications interdites dans les modes actifs et d'essai

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications, deux types de rapports peuvent être générés : un rapport sur les applications interdites (si la tâche est démarrée en mode Actif) et un rapport sur les applications interdites en mode test (si la tâche est démarrée en mode Statistiques seulement). Ces rapports affichent des informations sur les applications interdites sur les appareils protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky installées sur les appareils protégés.

Pour afficher un rapport sur les applications interdites en mode Informer :

1. Lancez la tâche Contrôle du lancement des applications en mode Informer.
2. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.

3. Sélectionnez l'onglet **Rapports**.
4. Double-cliquez sur l'élément **Rapport sur les applications interdites en mode test**.

   Un rapport est généré.
5. Consultez les détails de rapport suivants :

   - Diagramme graphique qui affiche les dix applications avec le plus grand nombre de démarrages bloqués.
   - Tableau récapitulatif des interdictions d'applications spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
   - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

Pour afficher un rapport sur les applications interdites en mode Actif :

1. Exécutez la tâche Contrôle du lancement des applications en mode Actif.
2. Sélectionnez le nœud **Serveur d'administration <nom du Serveur d'administration>** dans l'arborescence de la Console d'administration.
3. Sélectionnez l'onglet **Rapports**.
4. Double-cliquez sur l'option **Rapport sur les applications interdites**.

   Un rapport est généré.

Ce rapport comprend les mêmes données au sujet des blocs que le rapport sur les applications interdites en mode test.

État de la Protection en temps réel

Kaspersky Embedded Systems Security transmet le paramètre **État de la protection en temps réel** au Serveur d'administration de Kaspersky Security Center. La valeur de ce paramètre dépend de l'état actuel des modules de protection de l'application sur l'appareil protégé (consultez le tableau ci-dessous).

Kaspersky Embedded Systems Security détermine l'état de la protection en temps réel en fonction de l'état des modules suivants de l'application :

- Protection des fichiers en temps réel
- Contrôle des appareils
- Pare-feu
- Protection contre les menaces réseau
- Scanner AMSI
- Protection BadUSB
- Réparation des actions malicieuses
- Protection contre les Exploits.

Vous pouvez vérifier l'état de la protection en temps réel de l'application dans une console de Kaspersky Security Center.

Comment connaître l'état de la protection en temps réel dans la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Appareils administrés**.

L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de la protection en temps réel**. Si la colonne **État de la protection en temps réel** est absente, gérez les paramètres des colonnes en cliquant sur le lien **Ajouter ou supprimer des colonnes**.

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Appareils administrés**.

L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de la protection en temps réel**. Si la colonne **État de la protection en temps réel** est absente, gérez les paramètres des colonnes en cliquant sur le lien **Ajouter ou supprimer des colonnes**.

Comment connaître la Protection en temps réel de l'ordinateur dans Web Console

Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.

L'état actuel de la Protection en temps réel est affiché dans la liste des appareils, dans la colonne **État de protection en temps réel ;**. Si la colonne **État de protection en temps réel ;** est absente, gérez les paramètres des colonnes (⚙).

Valeurs possibles du paramètre État de la protection en temps réel

Valeur	Description
Inconnu	Le Serveur d'administration ne dispose d'aucune information sur l'état de la protection en temps réel de cet appareil.
Non installé(e)	Aucun module n'est installé.
Non pris en charge par la licence	L'application n'est pas activée ou la licence ne permet pas aux modules installés de fonctionner.
Échec	Un ou plusieurs modules présentent un dysfonctionnement.
Arrêté(e)	Un ou plusieurs modules sont désactivés.
Suspendu(e)	Un ou plusieurs modules sont suspendus.
En cours de démarrage	Un ou plusieurs modules sont en cours d'activation.
En cours d'exécution	Les modules de l'application sont opérationnels.

Si la valeur du paramètre **État de la protection en temps réel** dans Kaspersky Security Center est différente de *En cours d'exécution*, vérifiez que les modules installés de Kaspersky Embedded Systems Security figurant dans la liste sont activés et que l'application est activée.

Utilisation de la console de Kaspersky Embedded Systems Security

Cette section fournit des informations sur la console de Kaspersky Embedded Systems Security et décrit comment gérer l'application à l'aide de la Console de l'application installée sur l'appareil protégé ou sur un autre appareil.

Ouverture de la Console de l'application

Pour démarrer la Console de l'application :

1. Ouvrez l'Interface de diagnostic compacte d'une des manières suivantes :

   - Exécutez le fichier avpui.exe situé dans le dossier d'installation de l'application sur l'appareil protégé. Par défaut, le fichier se trouve dans C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.

   - Cliquez sur l'icône de l'application dans la zone de notification de la barre des tâches.

2. Dans la fenêtre de l'Interface de diagnostic compacte qui s'ouvre, cliquez sur le lien **Kaspersky Embedded Systems Security Console**.

   Si vous avez déjà configuré une connexion à l'appareil protégé, la Console de l'application s'ouvre.

   Si vous lancez la Console de l'application pour la première fois, vous êtes dirigé vers la fenêtre **Sélectionner un appareil protégé**, dans laquelle vous devez configurer la connexion de la Console de l'application à l'ordinateur protégé.

   La version 4.0 de la Console de l'application n'est pas compatible avec Kaspersky Embedded Systems Security version 4.1 et ultérieure. Lorsque vous tenterez de vous connecter, vous serez invité à installer le pack de compatibilité de la Console de l'application. Le pack de compatibilité sera téléchargé depuis l'appareil auquel vous vous connectez.

Interface de la console de Kaspersky Embedded Systems Security

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

Fenêtre de la console de Kaspersky Embedded Systems Security

Après l'établissement d'une connexion à Kaspersky Embedded Systems Security installé sur un autre appareil protégé, le nom du nœud reprend le nom de l'appareil protégé sur lequel l'application est installée ainsi que le nom du compte utilisateur sous les privilèges duquel la connexion a été établie : **Kaspersky Embedded Systems Security <nom de l'appareil protégé> sous <nom du compte utilisateur>**. Lors de la connexion à Kaspersky Embedded Systems Security installé sur le même appareil protégé avec Kaspersky Embedded Systems Security Console, le nom du nœud est Kaspersky Embedded Systems Security.

Arborescence de la Console

L'arborescence de la console de l'application affiche le nœud **Kaspersky Embedded Systems Security** et les nœuds enfants correspondant aux modules opérationnels de l'application.

Le nœud **Kaspersky Embedded Systems Security** inclut les nœuds enfants suivants :

- **Protection en temps réel de l'ordinateur** permet de configurer les tâches suivantes :
  - **Protection des fichiers en temps réel**
  - **Kaspersky Security Network**
  - **Protection contre les Exploits**
  - **Protection contre les menaces réseau**
  - **Détection comportementale**
  - **Réparation des actions malicieuses**
  - **Scanner AMSI**.
- **Contrôle de l'ordinateur** : contrôle les applications lancées sur l'appareil protégé et sur les appareils connectés.
  - **Contrôle du lancement des applications**
  - **Contrôle des appareils**
  - **Pare-feu**.
- **Génération automatique de règles** : configuration de la génération automatique des règles de groupe et des règles système pour les modules Contrôle du lancement des applications et Contrôle des appareils.
  - **Générateur de règles pour le Contrôle du lancement des applications**
  - **Générateur de règles pour le Contrôle des appareils**

- Tâches de groupe de génération de règles **<Nom des tâches>** (le cas échéant).

  Des tâches de groupe sont créées dans Kaspersky Security Center. Il est impossible d'administrer des tâches de groupe via Kaspersky Embedded Systems Security Console.

- **Diagnostic du système** : configuration des paramètres du Contrôle de l'intégrité du système et de l'analyse du journal des événements Windows.

  - **Inspection des journaux**
  - **Contrôle de l'intégrité du système**.

- **Analyse à la demande** : gère les tâches d'analyse à la demande. Un nœud séparé existe pour chacune des tâches :

  - **Analyse des zones critiques**
  - **Vérification de l'intégrité de l'application**
  - **Analyse des disques amovibles**
  - **Analyse complète**
  - Tâches définies par l'utilisateur **<Nom des tâches>** (le cas échéant)

  Le nœud affiche les tâches système créées lors de l'installation de l'application, les tâches définies par l'utilisateur et les tâches d'analyse à la demande de groupe créées et transmises à un appareil protégé à l'aide de Kaspersky Security Center.

- **Mise à jour** : gère les mises à jour pour les bases de données et les modules de l'application Kaspersky Embedded Systems Security, et offre la possibilité de rétablir la dernière mise à jour :

  - **Mise à jour des bases et des modules d'application**
  - **Annulation de la dernière mise à jour**
  - **Mise à jour de l'application**.

  Le nœud affiche toutes les tâches définies par l'utilisateur et les tâches de groupe de mise à jour créées et transmises à l'appareil protégé via Kaspersky Security Center.

- **Stockages** : gère les paramètres de la Sauvegarde et la liste des sessions réseau bloquées.

  - **Sauvegarde**
  - **Sessions réseau bloquées**.

- **Journaux et notifications** : gère les journaux des tâches locales et le journal d'audits système de Kaspersky Embedded Systems Security.

  - **Audit système**
  - **Contrôle du lancement des applications**
  - **Contrôle des appareils**

- **Vérification de l'intégrité de l'application**
- **Inspection des journaux**
- **Contrôle de l'intégrité du système**
- **Protection contre les menaces réseau**
- **Analyse à la demande**
- **Pare-feu**
- **Protection contre les Exploits**
- **Détection comportementale**
- **Scanner AMSI**
- **Mise à jour**
- **Protection des fichiers en temps réel**
- **Sauvegarde**.

- **Licence** : ajout ou suppression de clés de licence pour Kaspersky Embedded Systems Security, consultation des informations relatives aux licences.

Panneau des résultats

Le panneau de détails reprend les informations relatives au nœud sélectionné. Si vous avez choisi le nœud **Kaspersky Embedded Systems Security**, le panneau de détails affiche les informations relatives à l'état actuel de la protection de l'appareil, les informations relatives à Kaspersky Embedded Systems Security, l'état de la protection de ses modules fonctionnels et l'état de la clé.

Menu contextuel du nœud Kaspersky Embedded Systems Security

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

- **Suspendre la protection**.
- **Configurer les paramètres de la zone de confiance**. Consultez et configurez les paramètres de la zone de confiance.
- **Analyse des disques amovibles**. Configurez l'analyse des disques amovibles connectés via le port USB à l'appareil protégé.
- **Autorisations d'accès des utilisateurs pour la gestion des applications**. Consultez et configurez les privilèges d'accès aux fonctions de Kaspersky Embedded Systems Security.

- **Autorisations d'accès utilisateur pour l'administration du Service KESS**. Consultez et configurez les privilèges d'accès à l'administration du Kaspersky Embedded Systems Security Service.
- **Stockages**
- **Exporter les paramètres**. Enregistrez les paramètres de l'application dans un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Importer les paramètres**. Importez les paramètres de l'application depuis un fichier de configuration au format XML. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Actualiser**. Actualisez le contenu de la fenêtre de Kaspersky Embedded Systems Security Console. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.
- **Propriétés de l'application**. Consultez et configurez les paramètres de fonctionnement de Kaspersky Embedded Systems Security ou d'une tâche sélectionnée. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

  Pour ce faire, vous pouvez également utiliser le lien **Propriétés de l'application** dans le panneau d'informations du nœud Kaspersky Embedded Systems Security.

- **Aide**. Consultez les informations reprises dans l'aide de Kaspersky Embedded Systems Security. L'exécution de cette opération est également disponible dans les menus contextuels des tâches de l'application.

Barre d'outils et menu contextuel des tâches de Kaspersky Embedded Systems Security

Vous pouvez administrer les tâches de l'application à l'aide des éléments des menus contextuels de chaque tâche dans l'arborescence de la Console de Kaspersky Embedded Systems Security.

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

- **Rétablir/Suspendre**. Reprendre ou suspendre l'exécution de la tâche. Pour exécuter ces opérations, vous pouvez également utiliser les boutons de la barre d'outils. Cette action est disponible pour les tâches Protection en temps réel et Analyse à la demande.
- **Créer une tâche**. Créez une nouvelle tâche définie par l'utilisateur.
- **Supprimer la tâche**. Supprimez une tâche définie par l'utilisateur.
- **Exporter les paramètres** / **Importer les paramètres**. Exportez ou importez les paramètres de la tâche.
- **Propriétés**. Ouvrez la fenêtre des paramètres de la tâche.
- **Aide**. Ouvrez la section d'aide en ligne correspondante.

Icône de la barre d'état système dans la zone de notification

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

Si l'icône de l'application dans la zone de notification de la barre des tâches est masquée, cela signifie que l'administrateur a désactivé l'affichage de l'interface de l'application dans la stratégie.

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

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

Les états suivants de l'icône de l'application renseignent l'utilisateur sur le fonctionnement de l'application :

- L'icône indique que tous les modules de la protection de l'application critiques sont activés. Kaspersky Embedded Systems Security affiche un avertissement si l'utilisateur doit effectuer une action, par exemple, redémarrer l'ordinateur après la mise à jour de l'application.
- L'icône indique que le fonctionnement des modules de la protection de l'application critiques a été suspendu ou interrompu. Le fonctionnement des modules de la protection peut être interrompu, par exemple, si la licence a expiré ou si un dysfonctionnement est survenu dans l'application. Kaspersky Embedded Systems Security affiche un avertissement qui décrit le problème de protection de l'ordinateur.

Vous pouvez ouvrir le menu contextuel de l'icône de la barre d'état système d'un clic droit de la souris.

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

Commandes du menu contextuel de l'icône de la barre d'état système

Instruction	Description
Ouvrir la console de l'application	Ouvrez la console de Kaspersky Embedded Systems Security (si celle-ci est installée).
Ouvrir l'interface de diagnostic compacte	Ouvre l'interface de diagnostic compacte.
À propos de l'application	Ouvre la fenêtre **À propos de l'application** contenant des informations relatives à Kaspersky Embedded Systems Security. Si vous êtes un utilisateur enregistré de Kaspersky Embedded Systems Security, la fenêtre **À propos de l'application** contient des informations sur les mises à jour urgentes installées.
Masquer	Masque l'icône de la barre d'état système dans la zone de notification de la barre des tâches.

Vous pouvez à tout moment restaurer l'icône masquée de la barre d'état système.

Pour afficher à nouveau l'icône dans la barre d'état,

dans le menu **Démarrer** de Microsoft Windows, sélectionnez **Tous les programmes** > **Kaspersky Embedded Systems Security**. L'icône s'affiche dans la zone de notifications de la barre des tâches de Microsoft Windows.

Les noms des paramètres peuvent varier selon les versions du système d'exploitation installé.

Configuration des paramètres généraux via la Console de l'application

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 que Kaspersky Embedded Systems Security va utiliser, ils permettent d'activer la reprise des tâches de Kaspersky Embedded Systems Security après un arrêt inopiné de leur fonctionnement, de tenir un journal, d'activer la création d'un fichier de vidage 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 Kaspersky Embedded Systems Security Console n'est pas disponible si la modification de ces paramètres est interdite dans la stratégie active de Kaspersky Security Center.

Pour configurer les paramètres généraux de Kaspersky Embedded Systems Security :

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

   - Dans le panneau des résultats du nœud, cliquez sur le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez **Propriétés de l'application**.

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

2. Sous l'onglet **Interface**, spécifiez les avertissements que vous souhaitez voir sur l'icône de la barre d'état système de Kaspersky Embedded Systems Security.

3. Sous l'onglet **Paramètres de sécurité**, configurez les paramètres de la tâche suivants :

   - Configurez l'option **Lancer l'application au démarrage de l'ordinateur (recommandé)** dans la section **Général**.
   - Dans **Autodéfense**, configurez la protection des modules d'application et les services du système d'exploitation.
   - La section **Actions lors du passage à la source d'alimentation de secours** permet de limiter la charge de Kaspersky Embedded Systems Security sur l'appareil protégé dans le cadre de l'alimentation de secours :
     - **Ne pas lancer les tâches d'analyse programmées**
     - **Arrêter d'exécuter les tâches d'analyse**
   - Configurez le paramètres **Compatibilité avec les logiciels d'administration à distance** dans la section **Paramètres de compatibilité**.
   - Dans la section **Paramètres d'analyse**, vous pouvez configurer la limite d'utilisation du processeur pour les tâches d'analyse et céder des ressources aux autres applications.

4. Sous l'onglet **Paramètres du réseau**, configurez les paramètres de la tâche suivants :

   - Dans la section **Serveur proxy**, spécifiez les paramètres du serveur proxy, c'est-à-dire le type d'authentification et les informations requises pour l'authentification sur le serveur proxy.

   - Sous **Ports contrôlés**, spécifiez l'option de surveillance du port réseau :

     - **Contrôler tous les ports réseau**. Le mode de contrôle des ports de réseau via lesquels les modules de la protection contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur.

     - **Surveiller uniquement les ports réseau sélectionnés**. Dans ce mode de surveillance des ports réseau, les modules de la protection surveillent les ports sélectionnés de l'ordinateur ainsi que l'activité réseau des applications sélectionnées. La liste des ports qui sont normalement utilisés pour le transfert des messages électroniques et le trafic réseau, configurée conformément aux recommandations des experts de Kaspersky. Si nécessaire, vous pouvez modifier la liste des ports réseau.

   - Si nécessaire, sous **Port de connexion à distance**, vous pouvez modifier le port que la Console d'application utilise pour se connecter à un ordinateur sur lequel l'application est installée.

     Le numéro de port par défaut pour la connexion avec les informations d'identification Windows est 13032, et le numéro de port par défaut pour la connexion avec les informations d'identification des utilisateurs créés manuellement est 13031. Plage de numéros de port possibles : 1–65535.

     Les numéros de port précédemment enregistrés sont utilisés jusqu'au redémarrage de l'application.

5. Sous l'onglet **Diagnostic de dysfonctionnement**, cliquez sur **Paramètres**, et configurez le traçage et le vidage de la mémoire de l'application.

6. Cliquez sur **OK**.

Les paramètres de Kaspersky Embedded Systems Security sont enregistrés.

Administration des tâches de Kaspersky Embedded Systems Security

Cette section contient des informations sur la création, la configuration, le lancement et l'arrêt des tâches de Kaspersky Embedded Systems Security.

Catégories de tâche de Kaspersky Embedded Systems Security

Les fonctions Protection en temps réel de l'ordinateur, Contrôle de l'ordinateur, Génération automatique de règles, Diagnostic du système, Analyse à la demande, Protection du réseau industriel, Gestion du stockage et Mise à jour de Kaspersky Embedded Systems Security sont mises en œuvre sous la forme de tâches.

Ces tâches peuvent être administrées via les options du menu contextuel de la tâche dans l'arborescence de Kaspersky Embedded Systems Security Console, et du volet résultats. Vous pouvez consulter les informations sur l'état d'une tâche dans le panneau des résultats. Les opérations d'administration des tâches sont enregistrées dans le journal d'audit système.

Il existe deux types de tâches de Kaspersky Embedded Systems Security : *local* et *groupe*

Tâches locales

Les tâches locales ne peuvent être exécutées que sur l'appareil protégé pour lequel elles ont été créées. Il existe plusieurs types de tâches locales en fonction du mode de lancement :

- **Tâches locales du système**. Ces tâches sont créées automatiquement lors de l'installation de Kaspersky Embedded Systems Security. Vous pouvez modifier les paramètres de toutes les tâches système locales, à l'exception de la tâche *Annulation de la mise à jour*. Il est impossible de renommer ou de supprimer les tâches locales du système. Vous pouvez lancer les tâches locales du système d'analyse à la demande en même temps que les tâches définies par l'utilisateur.

- **Tâches locales définies par l'utilisateur**. La Console de l'application vous permet de créer les tâches Analyse à la demande, Mise à jour et Contrôle de l'intégrité du système par rapport à une référence. Kaspersky Security Center vous permet de créer les tâches Analyse à la demande, Mise à jour, etc. Vous pouvez renommer, configurer ou supprimer les tâches personnalisées. Vous pouvez exécuter simultanément plusieurs tâches définies par l'utilisateur.

Tâches de groupe

Vous pouvez gérer les tâches de groupe et les tâches pour des ensembles d'appareils protégés à partir de Kaspersky Security Center. Toutes les tâches de groupe sont des tâches définies par l'utilisateur. Les tâches de groupe sont également affichées dans la Console de l'application. La console de l'application permet uniquement de consulter l'état des tâches de groupe. Vous ne pouvez pas utiliser la Console de l'application pour administrer ou configurer des tâches de groupe.

Lancement, suspension, rétablissement et arrêt manuels des tâches

Vous pouvez lancer, suspendre, rétablir ou arrêter des tâches manuellement. Ces options ne sont pas disponibles pour toutes les tâches de Kaspersky Embedded Systems Security.

Pour démarrer, suspendre, reprendre ou arrêter une tâche :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel de la tâche.

2. Choisissez une des commandes suivantes : **Lancement** ou **Suspendre**.

L'opération sera réalisée et enregistrée dans le journal d'audit système.

Planification des tâches

Dans la Console de Kaspersky Embedded Systems Security, vous pouvez configurer la planification de l'exécution des tâches système et des tâches utilisateur locales. Cependant, vous ne pouvez pas configurer la planification de l'exécution des tâches de groupe.

Pour planifier une tâche :

1. Dans l'arborescence de la Console, sélectionnez la tâche pour laquelle vous souhaitez configurer la planification.
2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.
3. Dans la fenêtre qui s'ouvre dans la section **Mode d'exécution**, effectuez l'une des actions suivantes :
   - Cochez la case **Manuellement** pour exécuter la tâche manuellement à l'heure qui vous convient.
   - Cochez la case **Selon la planification** si vous souhaitez activer l'exécution planifiée d'une tâche.
4. Si vous sélectionnez l'option **Selon la planification**, configurez les paramètres de planification de la tâche (consultez le tableau ci-dessous).
5. Si nécessaire, cochez la case **Lancer la tâche avec les privilèges de l'utilisateur** et indiquez les identifiants du compte utilisateur qui exécutera la tâche.
6. Cliquez sur **OK**.

Les paramètres de la planification de la tâche sont enregistrés.

Paramètres de planification de la tâche

Paramètre	Description
Mode d'exécution	Sélectionnez le mode de fonctionnement de la tâche : • **Minutes**. La tâche sera exécutée périodiquement toutes les quelques minutes. Spécifiez l'heure de lancement de la tâche et la période en minutes. • **Heures**. La tâche sera exécutée périodiquement toutes les quelques heures. Spécifiez l'heure de lancement de la tâche et la période en heures. • **Jours**. La tâche sera exécutée périodiquement tous les quelques jours. Spécifiez l'heure de lancement de la tâche et la période en jours. • **Semaines**. La tâche sera exécutée les jours indiqués de la semaine, à intervalles d'un nombre défini de semaines. Spécifiez la planification, cochez les cases correspondant aux jours de la semaine où la tâche sera exécutée, puis indiquez l'heure de début de la tâche. • **Tous les mois**. La tâche sera exécutée un certain jour du mois. Spécifiez la date et l'heure de lancement. • **À l'heure indiquée**. La tâche sera exécutée une fois à la date et à l'heure indiquées. • **Après chaque mise à jour**. La tâche sera exécutée chaque fois que des mises à jour seront téléchargées dans le stockage. • **Après le lancement de l'application**. La tâche sera exécutée à chaque lancement de Kaspersky Embedded Systems Security.
Lancer les tâches non exécutées	Si la case est cochée, Kaspersky Embedded Systems Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Embedded Systems Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Adopter un décalage aléatoire automatique pour les lancements de tâche	Si la case est cochée, la tâche n'est pas exécutée strictement selon la planification, mais de manière aléatoire dans un certain intervalle, c'est-à-dire que les heures de lancement de la tâche sont étalées. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. La plage des heures de lancement aléatoires est calculée automatiquement lors de la création de la tâche, en fonction du nombre d'ordinateurs auxquels la tâche est assignée. Par la suite, la tâche est toujours exécutée à son heure de lancement calculée. Toutefois, lorsque les paramètres de la tâche sont modifiés ou que la tâche est exécutée manuellement, l'heure de lancement calculée change. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Décaler aléatoirement le lancement de la tâche dans un intervalle de (min.)	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.

Paramètre	Description
Suspendre la tâche	Vous pouvez définir un intervalle de temps pendant lequel l'exécution d'une tâche précédemment planifiée sera suspendue. Une fois la période définie écoulée, la tâche reprend. Cela peut s'avérer nécessaire, par exemple, pour limiter l'impact de Kaspersky Embedded Systems Security sur les performances de votre ordinateur pendant les périodes de forte utilisation. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.
Désactiver la planification à partir du	Si la case est cochée, Kaspersky Embedded Systems Security arrêtera l'exécution de la tâche planifiée à partir de la date indiquée. La tâche sera définie en mode **Manuellement**. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.

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.

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

Vous pouvez spécifier le compte pour exécuter les tâches de Kaspersky Embedded Systems Security suivantes :

- *Générateur de règles pour le Contrôle du lancement des applications*
- *Générateur de règles pour le Contrôle des appareils*
- *Inspection des journaux*
- *Vérification de l'intégrité de l'application*
- *Mise à jour*.

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

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

- Pour la tâche *Mise à jour* :
  - Si la source de mise à jour est un dossier partagé sur un autre appareil du réseau.
  - Si vous utilisez un serveur proxy avec authentification NTLM ou Kerberos pour accéder à la source des mises à jour.
- Pour la tâche *Générateur de règles pour le Contrôle du lancement des applications* : si les règles générées sont exportées vers un fichier de configuration inaccessible au compte système (par exemple, dans un des dossiers partagés de l'appareil protégé).

Vous pouvez lancer les tâches listées avec les privilèges du compte système. Kaspersky Embedded Systems Security exécute ces tâches et accède aux dossiers partagés sur l'autre appareil du réseau si cet appareil est enregistré dans le même domaine que l'appareil protégé. Dans ce cas, le compte système doit posséder les autorisations d'accès à ces dossiers. Kaspersky Embedded Systems Security accède à ce appareil avec les privilèges du compte **<Nom_de_domaine \ nom_appareil>**.

Définition du compte utilisateur pour l'exécution de la tâche

L'option permettant de spécifier un compte dans la Console de l'application n'est pas disponible pour toutes les tâches.

Pour désigner un compte pour démarrer une tâche :

1. Dans l'arborescence de la Console de l'application, sélectionnez la tâche que vous souhaitez lancer avec les privilèges d'un compte donné.
2. Dans le panneau des résultats, cliquez sur le lien **Mode d'exécution**.

   La fenêtre **Mode de programmation et d'exécution** s'ouvre.
3. Dans la fenêtre qui s'ouvre dans la section **Utilisateur**, effectuez les actions suivantes :
   a. Choisissez l'option **Lancer la tâche avec les privilèges de l'utilisateur**.
   b. Saisissez le nom et le mot de passe de l'utilisateur dont vous souhaitez utiliser le compte.

      L'utilisateur sélectionné doit être enregistré sur l'appareil protégé ou dans le même domaine que cet ordinateur.
4. Cliquez sur le bouton **OK**.

Les modifications apportées aux paramètres seront enregistrées.

Importation et exportation des paramètres

Cette section explique comment exporter les paramètres de Kaspersky Embedded Systems Security. Vous apprendrez également comment exporter les paramètres de certains modules de l'application vers un fichier de configuration XML et comment importer ces paramètres à partir d'un fichier de configuration dans l'application.

À 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 modules 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
- Protection contre les Exploits
- Protection contre les menaces réseau
- Détection comportementale
- Réparation des actions malicieuses
- Analyseur AMSI
- Contrôle du lancement des applications
- Contrôle des appareils
- Pare-feu
- Générateur de règles pour le Contrôle du lancement des applications
- Générateur de règles pour le Contrôle des appareils
- Inspection des journaux
- Contrôle de l'intégrité du système
- Analyse des zones critiques
- Vérification de l'intégrité de l'application
- Analyse des disques amovibles
- Analyse complète

- Mise à jour des bases de données et des modules de l'application
- Restauration de la dernière mise à jour
- Mise à jour

Vous pouvez également enregistrer les paramètres généraux de Kaspersky Embedded Systems Security dans un fichier, avec les privilèges des comptes utilisateur.

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 ne pouvez pas exporter les paramètres des tâches de groupe.

Kaspersky Embedded Systems Security exporte tous les mots de passe qui sont utilisés par l'application, par exemple, les paramètres du compte utilisateur sous lequel l'exécution des tâches ou la connexion au serveur proxy a lieu. Les mots de passe exportés dans le fichier de configuration sont chiffrés. Vous pouvez importer les mots de passe uniquement à l'aide d'une version de Kaspersky Embedded Systems Security installée sur ce appareil protégé, si elle n'a pas été réinstallée ou mise à jour.

Vous ne pouvez pas importer des mots de passe préalablement enregistrés à l'aide d'une version de Kaspersky Embedded Systems Security installée sur un autre appareil protégé. Après l'importation des paramètres sur l'appareil protégé, vous devez saisir tous les mots de passe manuellement.

Si la fonctionnalité **Demander un mot de passe pour confirmer les actions critiques** a été activée lors de l'exportation des paramètres, le mot de passe défini sur l'appareil est exporté, puis automatiquement appliqué à l'autre appareil lors de l'importation des paramètres.

Vous pouvez importer les paramètres à partir d'un fichier de configuration qui contient les paramètres de modules individuels de Kaspersky Embedded Systems Security (par exemple, à partir d'un fichier créé dans une version de Kaspersky Embedded Systems Security installé sans la totalité des modules). Après l'importation des paramètres, seuls les paramètres de Kaspersky Embedded Systems Security repris dans le fichier de configuration sont modifiés. Les autres paramètres demeurent inchangés.

Les paramètres verrouillés de la stratégie active de Kaspersky Security Center ne sont pas modifiés lors de l'importation des paramètres.

Exportation des paramètres

Pour exporter les paramètres vers un fichier de configuration :

1. Pour exporter l'ensemble des paramètres de Kaspersky Embedded Systems Security, dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**, sélectionnez la commande **Exporter les paramètres**.

   Pour exporter les paramètres d'un module distinct, cliquez sur **Exporter les paramètres** dans le panneau des résultats.

   Les paramètres de Kaspersky Security Network ne peuvent pas être exportés. Kaspersky Security Network doit être configuré manuellement.

2. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des paramètres et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

Vous pouvez utiliser des variables d'environnement système lors de la spécification du chemin, mais pas des variables d'environnement utilisateur.

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

3. Enregistrez le fichier.
4. Cliquez sur le bouton **OK** dans la fenêtre **L'exportation des paramètres a réussi**.

   Kaspersky Embedded Systems Security exporte la liste des paramètres dans un fichier XML.

Pour exporter la liste des applications de confiance :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Sélectionnez **Configurer les paramètres de la zone de confiance**.
3. La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.
4. Rendez-vous dans la section **Applications de confiance** et cliquez sur **Paramètres**.

   Une fenêtre reprenant la liste des applications de confiance s'ouvre.
5. Sélectionnez les applications de confiance que vous souhaitez exporter.

   Si vous ne sélectionnez aucune application de confiance, Kaspersky Embedded Systems Security exporte toutes les applications de confiance.
6. Cliquez sur la flèche et, dans la liste déroulante, sélectionnez **Exporter**.
7. Une fenêtre s'ouvre. Dans cette fenêtre, saisissez le nom du fichier XML vers lequel vous souhaitez exporter la liste des applications de confiance et sélectionnez le dossier dans lequel vous souhaitez enregistrer ce fichier.
8. Enregistrez le fichier.

   Kaspersky Embedded Systems Security exporte la liste des applications de confiance dans le fichier XML.

Vous pouvez également exporter les paramètres de Kaspersky Embedded Systems Security à l'aide de la ligne de commande.

Importation des paramètres

Pour importer des paramètres à partir d'un fichier de configuration enregistré :

1. Pour importer tous les paramètres de Kaspersky Embedded Systems Security, dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**, sélectionnez la commande **Importer les paramètres**.

   Pour importer les paramètres d'un module distinct, cliquez sur **Importer les paramètres** dans le panneau des résultats.

Une fois que les paramètres généraux de Kaspersky Embedded Systems Security ou de ses modules auront été importés sur l'appareil protégé, vous ne pourrez plus revenir aux paramètres antérieurs.

Les paramètres de Kaspersky Security Network ne peuvent pas être importés. Kaspersky Security Network doit être configuré manuellement.

2. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de configuration XML à partir duquel vous souhaitez importer les paramètres et cliquez sur **Ouvrir**.
3. Cliquez sur le bouton **OK** dans la fenêtre **L'importation des paramètres a réussi**.
4. Dans la barre d'outils de la Console de l'application, cliquez sur le bouton **Mise à jour**.

La fenêtre Console de l'application affiche les paramètres importés.

Kaspersky Embedded Systems Security n'importe pas les mots de passe (identifiants pour l'exécution de tâches ou la connexion au serveur proxy) d'un fichier créé sur un autre appareil protégé ou sur ce même appareil protégé après une réinstallation ou de mise à jour de Kaspersky Embedded Systems Security sur celui-ci. Après la fin de l'importation, il faudra saisir les mots de passe manuellement.

Pour importer la liste des applications de confiance :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
2. Sélectionnez **Configurer les paramètres de la zone de confiance**.
3. La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.
4. Rendez-vous dans la section **Applications de confiance** et cliquez sur **Paramètres**.
5. Cliquez sur la flèche et, dans la liste déroulante, sélectionnez **Importer**.
6. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications de confiance.
7. Ouvrez le fichier.

   Si l'ordinateur dispose déjà d'une liste d'applications de confiance, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. La liste s'affiche sous l'onglet **Applications de confiance**. Cliquez sur **OK**.

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

Pour lire les informations relatives à l'état de la protection de l'appareil dans Kaspersky Embedded Systems Security,

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

Par défaut, les informations du panneau de détails de Kaspersky Embedded Systems Security Console sont automatiquement actualisées :

- Toutes les 10 secondes en cas de connexion locale.
- Toutes les 15 secondes en cas de connexion distante.

Vous pouvez actualiser les informations manuellement.

*Pour actualiser manuellement les informations du nœud **Kaspersky Embedded Systems Security**,*

choisissez l'option **Actualiser** dans le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

Le panneau de détails de la console de l'application affiche les informations suivantes sur Kaspersky Embedded Systems Security Console :

- État d'utilisation de Kaspersky Security Network.
- État de la protection de l'appareil.
- Données sur la mise à jour des bases de données et des modules de l'application.
- Données de diagnostic réel.
- Données relatives aux tâches de contrôle des appareils protégés.
- Informations relatives à la licence.
- État de l'intégration à Kaspersky Security Center : données du serveur doté de Kaspersky Security Center auquel l'application est connectée ; informations sur les tâches de l'application contrôlées par la stratégie active.

L'affichage de l'état de la protection est indiqué par un code couleur :

- *Vert*. La tâche est exécutée conformément aux paramètres définis. La protection est active.
- *Jaune*. La tâche n'a pas été lancée, a été suspendue ou est arrêtée. Des menaces pour la sécurité peuvent apparaître. Il est conseillé de lancer la tâche.
- *Rouge*. La tâche s'est soldée sur une erreur ou une menace pour la sécurité a été détectée pendant l'exécution de la tâche. Il est conseillé de lancer la tâche ou d'adopter les mesures d'élimination de la menace détectée.

Une partie des informations du groupe (par exemple, les noms des tâches ou le nombre de menaces détectées) se présente sous la forme de liens qui permettent d'accéder au nœud de la tâche correspondante ou d'ouvrir le journal d'exécution de la tâche.

La section **Utilisation de KSN** affiche l'état actuel de la tâche, par exemple, *En cours*, *Arrêté* ou *Jamais exécuté*. L'indicateur peut prendre les valeurs suivantes :

- La couleur verte du panneau signifie que la tâche **Utilisation de KSN** est en cours d'exécution et les demandes de fichier pour les états sont envoyées à KSN.
- La couleur jaune du panneau signifie qu'une des déclarations est acceptée, mais que la tâche n'est pas en cours d'exécution ou qu'elle est en cours d'exécution, mais que les demandes de fichier ne sont pas envoyées à KSN.
- Couleur rouge du panneau : échec de la tâche.

Protection de l'ordinateur

La section **Protection de l'ordinateur** (cf. tableau ci-dessous) affiche les informations sur l'état de protection actuel de l'appareil.

Informations sur l'état de la protection de l'appareil

Section	Informations
Indicateur d'état de la protection de l'appareil	La couleur du volet avec le nom de la section reflète l'état des tâches en cours d'exécution dans la section. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : cette couleur s'affiche par défaut et indique que le module Protection des fichiers en temps réel est installé et que la tâche est en cours d'exécution. • Volet de couleur jaune : signifie que le module Protection des fichiers en temps réel n'est pas installé et la tâche *Analyse des zones critiques* n'a pas été exécutée depuis longtemps. • Couleur rouge du panneau : les tâches Protection des fichiers en temps réel ne sont pas en cours d'exécution.
Protection des fichiers en temps réel	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*.
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. *Jamais exécuté* : événement qui survient quand la tâche *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.
Protection contre les menaces réseau	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*.
Protection contre les Exploits	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*. **Mode de fonctionnement** : l'un des deux modes disponibles pour le module Protection contre les Exploits : **Bloquer** ou **Informer**.
Détection comportementale	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*. **Mode de fonctionnement** : l'un des trois modes disponibles pour la tâche Détection comportementale : **Supprimer**, **Bloquer** or **Informer**.

Mise à jour

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

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

Section	Informations
Témoin de l'état des bases et des modules de l'application	La couleur du volet avec le nom de la section reflète l'état des bases de données et les modules de l'application. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : cette couleur s'affiche par défaut et indique que les bases de l'application sont à jour et que la dernière tâche de mise à jour des bases et des modules de l'application a réussi. • Couleur jaune du panneau : signifie que les bases sont dépassées, ou que la dernière tâche de mise à jour des bases de données et des modules a échoué. • Couleur rouge du panneau : l'événement *Les bases sont fortement dépassées* ou *Les bases sont à jour* s'est produit.
État de la base de données	L'option peut prendre les valeurs suivantes : • **Les bases sont à jour** : les bases de l'application ont été mises à jour il y a 7 jours maximum (par défaut). • **Bases dépassées** : les bases de données de l'application ont été mises à jour il y a entre 7 et 14 jours (par défaut). • **Les bases sont fortement dépassées** : les bases de données de l'application ont été mises à jour il y a plus de 14 jours (par défaut). Vous pouvez modifier le seuil de déclenchement des événements *Bases dépassées* et *Les bases sont fortement dépassées*.
Date de publication des bases	Date et heure de la publication de la dernière mise à jour des bases de l'application. La date et l'heure sont exprimées en TU.
État de la tâche Mise à jour des bases de l'application la plus récente	Date et heure de la dernière mise à jour des bases. La date et l'heure sont exprimées selon l'heure locale de l'appareil protégé. La valeur du champ est rouge si l'événement *Erreur* se produit.

Contrôle

La section **Contrôle** (cf. tableau ci-après) affiche les informations relatives à l'état des tâches Contrôle du lancement des applications, Contrôle des appareils et Pare-feu.

Informations sur l'état du contrôle des appareils protégés

Section	Informations
Indicateur d'état pour le contrôle des appareils protégés	La couleur du volet avec le nom de la section reflète l'état des tâches en cours d'exécution dans la section. L'indicateur peut prendre les valeurs suivantes : • Volet de couleur verte : cette couleur s'affiche par défaut et indique que le module Contrôle du lancement des applications est installé, que la tâche est exécutée en mode Actif, et que le module Protection contre les Exploits est installé et actif. • Le panneau est jaune lorsque l'une ou plusieurs des conditions suivantes sont présentes : la Protection contre les Exploits n'est pas en cours d'exécution ; la tâche Contrôle du lancement des applications fonctionne en mode Informer ; la Protection contre les Exploits fonctionne en mode Actif, et la tâche Contrôle du lancement des applications n'est pas en cours d'exécution ou a échoué. • Couleur rouge du panneau : la tâche Contrôle du lancement des applications n'est pas en cours d'exécution ou a échoué, et la Protection contre les Exploits n'est pas en cours d'exécution ou est exécutée en mode **Informer**.
Contrôle du lancement des applications	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*. **Mode de fonctionnement** : l'un des modes disponibles pour la tâche Contrôle du lancement des applications : **Appliquer les règles** ou **Tester les règles**.
Contrôle des appareils	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*. **Mode de fonctionnement** : l'un des deux modes disponibles pour la tâche Contrôle des appareils : **Selon les règles** ou **Informer**.
Pare-feu	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*.

Diagnostic

La section **Diagnostic** (cf. tableau ci-après) affiche les informations relatives à l'état des tâches Contrôle de l'intégrité du système et Inspection des journaux.

Informations sur l'état du diagnostic du système

Section	Informations
Indicateur d'état du diagnostic	La couleur du volet avec le nom de la section reflète l'état des tâches en cours d'exécution dans la section. L'indicateur peut prendre les valeurs suivantes : • La couleur verte s'affiche par défaut et indique qu'un des modules de diagnostic du système ou les deux sont installés et que des tâches sont en cours d'exécution. • Jaune : les deux modules sont installés, mais l'une des tâches de diagnostic du système n'est pas en cours d'exécution ; l'événement *Ne fonctionne pas* se produit. • Rouge : l'une des tâches a échoué.
Contrôle de l'intégrité du système	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*.
Inspection des journaux	**État** : état actuel du module, par exemple, *En cours* ou *Désactivé*.

Les informations relatives à la licence de Kaspersky Embedded Systems Security sont affichées sur la ligne du coin inférieur gauche du panneau de détails du nœud **Kaspersky Embedded Systems Security**.

Vous pouvez configurer les propriétés de Kaspersky Embedded Systems Security en suivant le lien Propriétés de l'application.

Vous pouvez vous connecter à un autre appareil protégé en suivant le lien Se connecter à un ordinateur distant.

Comment configurer les paramètres de la Sauvegarde dans la Console de l'application

Pour configurer les paramètres généraux de la Sauvegarde :

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security** et sélectionnez **Stockages**.
2. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres du stockage

Paramètre	Description
Sous l'onglet **Rapports**, spécifiez les paramètres des rapports suivants :	
Supprimer les rapports après	Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des rapports est de 30 jours. À l'issue de cette période, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport.
Limiter la taille du fichier des rapports à	Si la case est cochée, la taille maximale du fichier de rapport est limitée par la valeur renseignée. Par défaut, la taille maximale du fichier est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale.
Sous l'onglet **Sauvegarde**, spécifiez les paramètres de sauvegarde suivants :	
Supprimer les objets après	Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Embedded Systems Security supprime les fichiers les plus anciens de la sauvegarde.

Paramètre	Description
Limiter la taille de la Sauvegarde à	Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 400 Mo. Une fois que la Sauvegarde a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les fichiers les plus anciens dans afin que le volume de la Sauvegarde ne dépasse plus la valeur maximale.
Valeur du seuil de l'espace disponible	La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (100 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil, Kaspersky Embedded Systems Security consigne l'événement *Dépassement du seuil d'espace libre disponible dans la sauvegarde* 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 **Valeur du seuil de l'espace disponible** est active si la case **Limiter la taille de la Sauvegarde à** est cochée.

Utilisation du Plug-in Web depuis Web Console et Cloud Console

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

Gestion de Kaspersky Embedded Systems Security à partir de Web Console ou de Cloud Console

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

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

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

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

- **À l'aide de stratégies de Kaspersky Security Center**. Les stratégies de Kaspersky Security Center permettent de configurer à distance des paramètres de protection uniques pour un groupe d'appareils. Les paramètres de la tâche, définis dans la stratégie active, ont priorité sur les paramètres des tâches définis localement dans la console de l'application ou à distance dans la fenêtre Propriétés : <nom de l'appareil protégé> de Kaspersky Security Center Web Console. Les stratégies permettent de configurer les paramètres généraux de l'application, les paramètres des tâches de protection en temps réel de l'ordinateur, les tâches de contrôle des activités sur les appareils, les tâches de protection du stockage réseau et les paramètres de lancement planifié des tâches du système local.

- **À l'aide de tâches de groupe de Kaspersky Security Center**. Les tâches de groupe de Kaspersky Security Center permettent de configurer à distance des paramètres uniques pour les tâches ayant un délai d'exécution limité pour un groupe d'appareils. Les tâches de groupe permettent d'activer l'application, de configurer les paramètres des tâches d'analyse à la demande, les paramètres des tâches de mise à jour, les paramètres de la tâche Générateur de règles pour le Contrôle du lancement des applications.

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

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

Kaspersky Security Center Web Console et Cloud Console permettent de configurer les paramètres de l'application ainsi que les possibilités additionnelles. Elles donnent également accès aux journaux et notifications. Vous pouvez configurer ces paramètres aussi bien pour un groupe d'appareils protégés que pour des appareils protégés individuels.

Limitations du Plug-in Web

Le plug-in Web de Kaspersky Embedded Systems Security présente les limitations suivantes par rapport au plug-in Kaspersky Embedded Systems Security :

- Les règles du module Contrôle du lancement des applications ne peuvent pas être créées à l'aide d'un certificat numérique ou d'événements Kaspersky Security Center.

- Les règles du module Contrôle des appareils ne peuvent pas être générées en fonction des appareils connectés ou des données système.

Administration des paramètres de l'application

Cette section contient les informations sur la configuration des paramètres généraux du fonctionnement de Kaspersky Embedded Systems Security dans Kaspersky Security Center Web Console.

Configuration des paramètres généraux de l'application dans le Plug-in Web

Vous pouvez configurer les paramètres généraux de Kaspersky Embedded Systems Security dans Web plug-in pour un groupe d'appareils protégés ou pour un appareil protégé individuel.

Configuration de l'interface et de l'analyse dans plug-in Web

Pour configurer les paramètres de l'interface de l'application, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.

3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configurer** dans la sous-section **Paramètres de l'interface**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres d'interaction avec l'utilisateur et paramètres d'analyse

Paramètre	Description
Interaction avec l'utilisateur	**Ne pas afficher l'interface utilisateur**. L'ordinateur client n'affiche aucun élément pouvant indiquer le fonctionnement de Kaspersky Embedded Systems Security. De même, l'icône dans la zone de notification Windows et les notifications ne sont pas disponibles. **Afficher l'interface utilisateur**. Sur l'ordinateur client, l'icône est disponible dans la barre d'état système Windows. Le menu contextuel de l'icône permet à l'utilisateur d'effectuer des opérations avec Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security affiche également des notifications au-dessus de l'icône de l'application. Le menu contextuel de l'icône dans la barre d'état système de Windows permet d'ouvrir l'interface de diagnostic compacte. Un lien dans l'interface de diagnostic compacte ouvre la Console de l'application.
Afficher l'état de l'application dans la zone de notifications	Sélectionnez les cases en regard des catégories d'événements pour lesquels vous souhaitez voir des notifications dans la zone de notification de Microsoft Windows.

Configuration des paramètres de sécurité et de fiabilité dans le plug-in Web

Pour configurer les paramètres de sécurité manuellement, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configurer** dans la sous-section **Sécurité et fiabilité**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de sécurité et de fiabilité

Paramètre	Description
Lancer l'application au démarrage de l'ordinateur (recommandé)	Si la case est cochée, Kaspersky Embedded Systems Security se lance après le démarrage du système d'exploitation et protège l'ordinateur de l'utilisateur tout au long de la session d'utilisation. Lorsque la case est décochée, Kaspersky Embedded Systems Security ne démarre pas après le chargement du système d'exploitation, tant que l'utilisateur ne le démarre pas manuellement. La protection de l'ordinateur est désactivée et les données des utilisateurs peuvent être exposées à des menaces.
Protéger les processus de l'application contre les menaces externes	Lorsque cette case est cochée, Kaspersky Embedded Systems Security empêche la modification ou la suppression des fichiers d'application sur le disque dur, les processus de mémoire et les entrées dans le registre système.
Protéger les services du système d'exploitation	Si la protection des services du système d'exploitation est activée, les applications tierces ne peuvent pas agir sur les processus du système d'exploitation. Si la protection des services du système d'exploitation est désactivée, des applications tierces peuvent agir sur les processus du système d'exploitation.

Paramètre	Description
Reporter les tâches planifiées en cas d'alimentation par batterie	Si cette option est sélectionnée, le mode d'économie d'énergie est activé. Kaspersky Embedded Systems Security reporte les tâches planifiées. Vous pouvez démarrer manuellement une analyse ou les tâches de mise à jour, si nécessaire. Quand le mode d'économie d'énergie est activé, les tâches suivantes ne sont pas exécutées quand un ordinateur est alimenté par la batterie, mais si elles sont programmées : • *Mise à jour des bases et des modules de l'application* • *Analyse complète* • *Analyse des zones critiques* • *Analyse personnalisée* • *Vérification de l'intégrité de l'application* • *Analyse IOC*.
État de l'ordinateur à l'application des paramètres	Les paramètres de l'affichage des états des ordinateurs client doté de l'application Kaspersky Embedded Systems Security dans Web Console en cas d'erreur d'application de la stratégie ou d'exécution de la tâche. Les états suivants sont disponibles : *OK*, *Avertissement* et *Critique*.
Compatibilité avec les logiciels d'administration à distance	Si l'utilisation de Kaspersky Embedded Systems Security avec les outils d'administration à distance Remote Administration Tool (RAT) pose des problèmes, vous pouvez activer le mode de compatibilité. Les problèmes peuvent être liés à l'incompatibilité des RAT avec la fonctionnalité Secure Desktop de l'application. Le but de cette fonctionnalité est de confirmer les actions susceptibles de réduire le niveau de sécurité de l'ordinateur. Cette fonctionnalité permet à une application d'afficher une boîte de dialogue de confirmation isolée des autres processus. Cette fonctionnalité utilise des droits élevés pour sécuriser la demande. De cette façon, seul l'utilisateur peut confirmer l'action et non le programme malveillant. Si cette option est sélectionnée, le mode de compatibilité RAT est activé. L'application affiche une boîte de dialogue de confirmation sans cette fonctionnalité. Le niveau de sécurité de l'ordinateur peut s'en trouver réduit. Nous vous déconseillons d'activer le mode de compatibilité si Kaspersky Embedded Systems Security ne pose pas de problèmes avec votre RAT. Si cette option est désélectionnée, le mode de compatibilité RAT est désactivé. Par défaut, la case est décochée. Exemple : lors de l'utilisation du navigateur en mode RemoteApp, Kaspersky Embedded Systems Security peut ne pas afficher de fenêtre de confirmation lors de la visite d'un site Web avec un certificat non fiable, car RemoteApp ne prend pas en charge la fonctionnalité Bureau sécurisé de l'application. Le navigateur peut alors ne plus répondre. Pour que le navigateur fonctionne correctement en mode RemoteApp, vous devez activer le mode de compatibilité. Vous pouvez également essayer d'activer le mode de compatibilité si vous rencontrez des problèmes avec la fonctionnalité Bureau sécurisé lors de l'utilisation d'un autre logiciel tiers.
Limiter l'utilisation du processeur pour les tâches d'analyse	Kaspersky Embedded Systems Security n'utilise jamais le processeur de l'appareil protégé dans les tâches d'analyse à la demande au-delà de la valeur du champ **Limite supérieure**. Cependant, l'application peut utiliser beaucoup plus de temps processeur à cause d'autres modules. L'activation de cette fonctionnalité peut avoir une incidence négative sur les performances de Kaspersky Embedded Systems Security. Cette fonction est désactivée par défaut.
Céder les ressources aux autres applications	La consommation des ressources de l'ordinateur par Kaspersky Embedded Systems Security lors de l'analyse de l'ordinateur peut augmenter la charge des sous-systèmes du processeur et du disque dur. Ce processus peut ralentir d'autres applications. Pour optimiser les performances, Kaspersky Embedded Systems Security propose un mode de transfert des ressources vers d'autres applications. Dans ce mode, le système d'exploitation peut réduire la priorité des tâches d'analyse de Kaspersky Embedded Systems Security lorsque la charge du processeur est élevée. Cette fonction permet de redistribuer les ressources du système d'exploitation à d'autres applications. Le processeur consacrera donc moins de ressources aux tâches d'analyse. Par conséquent, Kaspersky Embedded Systems Security mettra plus de temps à analyser l'ordinateur. Le mode de transfert des ressources vers d'autres applications est activé par défaut.

Configuration des paramètres de connexion dans le plug-in Web

Les paramètres de connexion configurés servent à établir une connexion entre Kaspersky Embedded Systems Security et les serveurs de mise à jour et d'activation. Ils interviennent également dans l'intégration des applications aux services Kaspersky Security Network.

Pour configurer les paramètres de la connexion, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configurer** dans la sous-section **Paramètres de connexion**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de connexion

Paramètre	Description
Restreindre le trafic sur les connexions limitées	Si la case est cochée, l'application limite son propre trafic réseau si la connexion à Internet est limitée. Kaspersky Embedded Systems Security définit la connexion mobile à Internet à haut débit comme limitée, la connexion via Wi-Fi comme illimitée. Le Contrôle du trafic Internet fonctionne sur les ordinateurs exécutant Windows 8 ou une version ultérieure.
Ne pas utiliser de serveur proxy	Si cette option est sélectionnée, Kaspersky Embedded Systems Security n'utilise pas de serveur proxy.
Définir automatiquement les paramètres du serveur proxy	Si cette option est sélectionnée, Kaspersky Embedded Systems Security utilise les paramètres de proxy du système d'exploitation.
Utiliser les paramètres indiqués du serveur proxy	Si cette option est sélectionnée, Kaspersky Embedded Systems Security utilise les paramètres du serveur proxy indiqués manuellement. Saisissez l'adresse IP ou le nom symbolique du serveur proxy et le numéro de port
Ne pas utiliser de serveur proxy pour les adresses locales	Si la fonctionnalité est activée, les échanges avec les autres appareils du réseau auquel appartient l'appareil protégé disposant de Kaspersky Embedded Systems Security se font directement. Cette option est activée par défaut.

Paramètre	Description
Paramètres d'authentification du serveur proxy	Pour authentifier l'application sur le serveur proxy d'accès à Internet, vous devez saisir les identifiants de l'utilisateur. Kaspersky Embedded Systems Security prend en charge l'authentification automatique sur le serveur proxy. Si l'authentification automatique échoue, l'application vous invite à saisir les identifiants. **Ne pas utiliser l'authentification** **Authentification NTLM**. Authentification NTLM avec le compte utilisateur actuel (par défaut). **Authentification NTLM avec nom d'utilisateur et mot de passe**. Authentification NTLM avec des identifiants spécifiés manuellement. **Nom d'utilisateur et mot de passe**. Authentification avec des identifiants spécifiés manuellement. **Authentification Kerberos**. Authentification Kerberos avec le compte utilisateur actuel. Pour garantir le bon fonctionnement de l'authentification Kerberos lorsque vous utilisez des enregistrements CNAME pour l'adresse du serveur proxy, vous devez enregistrer un Service Principal Name (SPN) pour chaque enregistrement CNAME. **Authentification Kerberos avec nom d'utilisateur et mot de passe**. Authentification Kerberos avec des identifiants spécifiés manuellement. Si l'authentification Kerberos est sélectionnée, Kaspersky Embedded Systems Security peut, en fonction de la configuration du serveur proxy, procéder à l'authentification selon le protocole Kerberos ou NTLM.
Contrôler tous les ports réseau	Le mode de contrôle des ports de réseau via lesquels les modules de la protection contrôlent les flux des données transmis via n'importe quel port réseau ouvert de l'ordinateur.
Surveiller uniquement les ports réseau sélectionnés	Dans ce mode de surveillance des ports réseau, les modules de la protection surveillent les ports sélectionnés de l'ordinateur ainsi que l'activité réseau des applications sélectionnées. La liste des ports qui sont normalement utilisés pour le transfert des messages électroniques et le trafic réseau, configurée conformément aux recommandations des experts de Kaspersky.
Utiliser Kaspersky Security Center comme serveur proxy lors de l'activation de l'application	Indiquez si Kaspersky Security Center doit être utilisé en guise de serveur proxy pour l'activation de l'application.

Configuration du lancement planifié des tâches locales dans le plug-in web

Vous pouvez utiliser des stratégies pour autoriser ou interdire le lancement de la tâche locale du système d'analyse à la demande et de la tâche de mise à jour. Cela s'opère selon la planification configurée localement sur chaque appareil protégé du groupe d'administration :

- Si le lancement programmé pour les tâches locales du système du type indiqué est interdit dans la stratégie, ces tâches ne sont pas exécutées sur l'appareil protégé selon la programmation. Vous pouvez lancer les tâches locales du système manuellement.

- Si le lancement programmé pour les tâches locales du système du type indiqué est autorisé dans la stratégie, ces tâches sont exécutées conformément à la programmation définie localement pour cette tâche.

Le lancement des tâches locales du système est interdit par défaut par la stratégie.

Il est conseillé de ne pas autoriser le lancement des tâches locales du système si les mises à jour ou l'analyse à la demande sont administrées via des tâches de groupe de Kaspersky Security Center.

Si vous n'utilisez pas les tâches de mise à jour de groupe ou d'analyse à la demande, autorisez le lancement des tâches locales du système dans la stratégie : Kaspersky Embedded Systems Security réalise la mise à jour des bases de l'application et des modules et lance également toutes les tâches locales du système d'analyse à la demande conformément à la programmation par défaut.

Les stratégies permettent d'autoriser ou d'interdire le lancement planifié des tâches locales du système suivantes :

- Tâche d'analyse à la demande : *Analyse des zones critiques*, *Analyse au démarrage du système d'exploitation*, *Vérification de l'intégrité de l'application*, *Contrôle de l'intégrité du système par rapport à une référence*.
- La tâche *Mise à jour*.

Si vous excluez l'appareil protégé du groupe d'administration, la planification des tâches locales du système sera automatiquement activée.

Pour autoriser ou interdire le lancement planifié des tâches locales du système de Kaspersky Embedded Systems Security dans une stratégie :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur **Configurer** dans la sous-section **Exécuter les tâches du système local**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de lancement des tâches locales

Paramètre	Description
Autoriser l'utilisation des tâches locales	Si la case est cochée, les tâches locales sont affichées dans l'interface locale de Kaspersky Embedded Systems Security. L'utilisateur, en l'absence de restrictions complémentaires de la stratégie, peut configurer les tâches et les lancer. Cependant, la configuration de la planification de l'exécution des tâches reste indisponible pour l'utilisateur. L'utilisateur ne peut exécuter des tâches que manuellement. Si la case est décochée, l'utilisation des tâches locales est interrompue. Dans ce mode, les tâches locales ne sont pas lancées selon une planification. Les tâches locales ne peuvent être lancées ou modifiées depuis l'interface locale de Kaspersky Embedded Systems Security ou via la ligne de commande.
Autoriser la gestion de la planification	La case est active si la case **Autoriser l'utilisation des tâches locales** est cochée. Si la case est cochée, la gestion des planifications devient accessible dans les propriétés de la tâche locale dans la Console de l'application. Par défaut, la case est décochée.
Autoriser l'affichage des tâches de groupe	Si la case est cochée, les tâches de groupe sont affichées dans l'interface locale de Kaspersky Embedded Systems Security. L'utilisateur peut consulter la liste complète des tâches dans la Console de l'application. Si cette case n'est pas cochée, Kaspersky Embedded Systems Security affiche une liste de tâches vide.
Autoriser la gestion des tâches de groupe	Si la case est cochée, l'utilisateur peut lancer et arrêter les tâches de groupe définies dans Kaspersky Security Center. L'utilisateur peut lancer et arrêter des tâches dans la Console de l'application ou dans l'interface simplifiée de l'application. Si cette case n'est pas cochée, Kaspersky Embedded Systems Security lance automatiquement les tâches selon la planification ou l'administrateur les lance manuellement dans Kaspersky Security Center.

Configuration des paramètres de la Sauvegarde dans le plug-in Web

Pour configurer les paramètres de la Sauvegarde dans Kaspersky Security Center, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie que vous souhaitez configurer.
3. Dans la fenêtre **<Nom de la stratégie>** qui s'ouvre, sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Complémentaire**.
5. Cliquez sur **Configurer** dans la sous-section **Stockages**.
6. Configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres du stockage

Paramètre	Description
Sous l'onglet **Rapports**, spécifiez les paramètres des rapports suivants :	
Supprimer les rapports après	Si la case est cochée, la limite de conservation maximale des rapports est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des rapports est de 30 jours. À l'issue de cette période, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport.
Limiter la taille du fichier des rapports à	Si la case est cochée, la taille maximale du fichier de rapport est limitée par la valeur renseignée. Par défaut, la taille maximale du fichier est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille ne dépasse plus la valeur maximale.
Sous l'onglet **Sauvegarde**, spécifiez les paramètres de sauvegarde suivants :	
Supprimer les objets après	Si la case est cochée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Embedded Systems Security supprime les fichiers les plus anciens de la sauvegarde.
Limiter la taille de la Sauvegarde à	Si la case est cochée, la taille maximale de la Sauvegarde est limitée par la valeur renseignée. Par défaut, la taille maximale est limitée à 400 Mo. Une fois que la Sauvegarde a atteint sa taille maximale, Kaspersky Embedded Systems Security supprime automatiquement les fichiers les plus anciens dans afin que le volume de la Sauvegarde ne dépasse plus la valeur maximale.
Valeur du seuil de l'espace disponible	La case active ou désactive la surveillance de l'espace minimum disponible dans la sauvegarde (100 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil, Kaspersky Embedded Systems Security consigne l'événement Dépassement du seuil d'espace libre disponible dans la sauvegarde 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 **Valeur du seuil de l'espace disponible** est active si la case **Limiter la taille de la Sauvegarde à** est cochée. Cette case est cochée par défaut.

Création et configuration des stratégies

Cette section fournit des explications sur l'application des stratégies de Kaspersky Security Center à l'administration de Kaspersky Embedded Systems Security sur plusieurs appareils protégés.

Vous pouvez créer des stratégies de Kaspersky Security Center globales pour l'administration de la protection de plusieurs appareils sur lesquels Kaspersky Embedded Systems Security est installé.

Une stratégie applique les paramètres de Kaspersky Embedded Systems Security ainsi que ses fonctions et ses tâches spécifiées à l'ensemble des appareils protégés au sein d'un groupe d'administration.

Vous pouvez créer plusieurs stratégies pour un groupe d'administration et les appliquer alternativement. Dans Web Console, la stratégie active dans le groupe en ce moment possède l'état *Actif*.

Les informations relatives à l'application de la stratégie sont consignées dans le journal d'audit système de Kaspersky Embedded Systems Security. Vous pouvez les consulter dans la console de l'application dans le nœud **Journaux et notifications**.

Kaspersky Security Center offre une méthode pour appliquer les stratégies aux appareils protégés : *interdire la modification des paramètres*. Après l'application de la stratégie, Kaspersky Embedded Systems Security applique aux appareils protégés les paramètres pour lesquels vous avez sélectionné l'icône dans les propriétés de la stratégie. Dans ce cas, les paramètres sélectionnés sont utilisés à la place des paramètres en vigueur avant l'application de la stratégie. Les paramètres de la stratégie active accompagnés de l'icône dans les propriétés de la stratégie ne sont pas appliqués par Kaspersky Embedded Systems Security.

Si une stratégie est active, les paramètres dans la Console de l'application qui sont accompagnés de l'icône dans la stratégie peuvent être consultés, mais pas modifiés. Les valeurs des autres paramètres (accompagnés de l'icône dans la stratégie) peuvent être modifiées dans la console de l'application.

Les paramètres configurés dans la stratégie active et accompagnés de l'icône empêchent également la modification des paramètres dans Kaspersky Security Center pour un appareil protégé dans la fenêtre **Propriétés : <Nom de l'appareil protégé>**.

Les paramètres configurés et transmis à l'appareil protégé à l'aide de la stratégie active sont enregistrés dans les paramètres de tâche locale après la désactivation de la stratégie active.

Si une stratégie définit des paramètres d'une tâche de protection de l'ordinateur en temps réel ou d'une tâche de protection des stockages réseau, les paramètres définis par la stratégie sont modifiés immédiatement après l'application de la stratégie. Si la tâche n'est pas en cours d'exécution, les paramètres sont appliqués à son lancement.

Comment créer une stratégie dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur **Ajouter**.
3. La fenêtre **Nouvelle stratégie** s'ouvre.
4. Dans la section **Sélectionnez l'application**, sélectionnez Kaspersky Embedded Systems Security.
5. Spécifiez les modes de Kaspersky Embedded Systems Security sur les appareils protégés.
6. Si nécessaire, spécifiez les fichiers ou les dossiers ainsi que les noms des objets (selon l'Encyclopédie des virus) que vous souhaitez exclure de l'analyse de tous les modules de l'application ou de certains d'entre eux.
7. Sous l'onglet **Général**, exécutez les actions suivantes :
   - modifier le nom de la stratégie ;

     Le nom de la stratégie ne peut pas contenir les caractères `" * < : > ? \ |` .

- Sélectionner l'état d'une stratégie :
  - **Actif**. Lors de la synchronisation suivant, la stratégie sera utilisée sur l'ordinateur en tant que stratégie active.
  - **Inactive**. Stratégie de sauvegarde. Le cas échéant, la stratégie inactive peut être transformée en stratégie active.
  - **Pour les utilisateurs itinérants**. La stratégie commence à agir quand l'ordinateur quitte le périmètre du réseau de l'organisation.
- configurer l'héritage des paramètres :
  - **Hériter des paramètres de la stratégie parent**. Si le commutateur est activé, les paramètres de la stratégie sont hérités de la stratégie du niveau supérieur de la hiérarchie. Les paramètres de la stratégie ne peuvent être modifiés si est activé dans la stratégie parent.
  - **Imposer l'héritage des paramètres aux stratégies enfants**. Si le commutateur est activé, les paramètres de la stratégie sont appliqués aux stratégies enfants. Dans les paramètres de contrôle parental, la case **Hériter des paramètres de la stratégie parent** est automatiquement cochée. Les paramètres de stratégie enfant sont hérités de la stratégie parent, à l'exception des paramètres accompagnés de . Les paramètres des stratégies enfant ne peuvent pas être modifiés si est activé dans la stratégie parent.

8. Dans l'onglet **Paramètres de l'application**, configurez les paramètres de la stratégie selon vos besoins.
9. Cliquez sur **Enregistrer**.

Après la création d'une stratégie, un ensemble de règles d'autorisation est créé pour empêcher le blocage des applications et garantir leur fonctionnement ininterrompu.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau entrant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le processus de partage du bureau Windows à l'aide de l'Agent d'administration de Kaspersky Security Center, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le port local 15000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.

Par défaut, Kaspersky Embedded Systems Security crée un ensemble de règles pour le trafic réseau sortant lorsque vous créez une stratégie :

- Deux règles d'autorisation pour le service Kaspersky Embedded Systems Security Service, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le processus de travail de Kaspersky Embedded Systems Security, qui se trouve dans les dossiers %Program Files% et %Program Files (x86)%. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.
- Deux règles d'autorisation pour le port local 13000. État : activé. Adresses externes autorisées : toutes. Protocoles : TCP et UDP, une règle par protocole.

Création et configuration de tâches via Kaspersky Security Center

Cette section contient des informations sur les tâches de Kaspersky Embedded Systems Security, leur création, la configuration des paramètres d'exécution, leur lancement et leur arrêt.

À propos de la création de tâches dans le Plug-in Web

Vous pouvez utiliser une des méthodes suivantes pour créer des tâches locales et des tâches de groupe :

- Pour un appareil protégé : dans la fenêtre **Propriétés <nom de l'appareil protégé>** dans la section **Tâches**.
- Pour un groupe d'administration : dans le panneau de détails du nœud du groupe d'appareils protégés sélectionné sous l'onglet **Tâches**.
- Pour une sélection d'appareils protégés : dans le panneau de détails du nœud **Sélections d'appareils**.

Les stratégies permettent de désactiver les planifications pour les tâches système locales *Mise à jour* et *Analyse à la demande* sur tous les appareils protégés du même groupe d'administration.

Vous trouverez toutes les informations générales sur les tâches de Kaspersky Security Center dans le Système d'aide de Kaspersky Security Center.

Création d'une tâche dans le Plug-in Web

Pour créer une tâche dans Kaspersky Security Center Web Console, procédez comme suit :

1. Lancez l'Assistant de création de tâche d'une des manières suivantes :
   - Pour créer une tâche locale :
     a. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.
     b. Cliquez sur le nom de l'appareil protégé.
     c. Dans la fenêtre **<Nom de l'appareil>** qui s'ouvre, sélectionnez l'onglet **Tâches**.
     d. Cliquez sur **Ajouter**.
   - Pour créer une tâche de groupe :
     a. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Tâches**.
     b. Cliquez sur **Ajouter**.

La fenêtre de l'Assistant de création d'une tâche s'ouvre.

2. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.

3. Dans la liste déroulante **Type de tâche**, sélectionnez le type de la tâche à créer.

4. En fonction du type de tâche sélectionné, réalisez une des opérations suivantes :

   - Création d'une tâche d'analyse à la demande.

   - Si vous créez une des tâches de mise à jour, définissez les paramètres de la tâche conformément à vos exigences :

     a. Dans le groupe **Sources des mises à jour**, vous pouvez indiquer le Serveur d'administration de Kaspersky Security Center ou les serveurs de mise à jour de Kaspersky en tant que source des mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.

     Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

     b. Configurez les paramètres d'une fonctionnalité qui réduit la charge sur le sous-système de disque :

     c. Vous pouvez spécifier les actions que Kaspersky Embedded Systems Security exécutera si des mises à jour critiques des modules de l'application sont nécessaires et après l'installation des mises à jour critiques. En outre, vous pouvez indiquer si Kaspersky Embedded Systems Security recevra des informations sur les mises à jour planifiées disponibles.

     d. Spécifiez l'ensemble des mises à jour à copier et le chemin d'accès au dossier qui sera utilisé par Kaspersky Embedded Systems Security pour stocker les mises à jour copiées.

   - Pour créer la tâche Activation de l'application, procédez comme suit :

     a. Dans la fenêtre **Sélection d'une clé de licence**, désignez le fichier clé ou le code d'activation que vous souhaitez utiliser pour activer l'application.

     b. Cochez la case **Utiliser la clé en tant que clé de réserve** si vous souhaitez créer une tâche pour renouveler la licence.

   - Créez et configurez la tâche Générateur de règles pour le Contrôle du lancement des applications.

   - Créez et configurez la tâche Générateur de règles pour le Contrôle des appareils.

5. Cliquez sur **Suivant**.

6. Si la tâche est créée pour une sélection d'appareils protégés, sélectionnez le réseau (ou le groupe) d'appareils protégés sur lesquels elle sera exécutée.

7. Cliquez sur **Suivant**.

8. Dans la fenêtre **Fin de la création de la tâche**, sélectionnez la case **Ouvrir les détails de la tâche à la fin de la création** si vous souhaitez configurer les paramètres de la tâche.

9. Cliquez sur **Terminer**.

La tâche créée apparaît dans la liste **Tâches**.

Configuration des tâches de groupe dans le Plug-in Web

Pour configurer une tâche de groupe pour plusieurs appareils protégés, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.
3. Rendez-vous dans l'onglet **Paramètres de l'application**.
4. En fonction du type de la tâche à configurer, exécutez l'une des actions suivantes :
   - Pour configurer la tâche *Analyse à la demande*, procédez comme suit :
     a. Dans la section **Zone d'analyse**, créez une zone d'analyse.
     b. Dans la section **Options**, configurez le niveau de l'analyse heuristique et l'intégration aux autres modules de l'application.
   - Si vous configurez la tâche *Mise à jour*, définissez les paramètres de la tâche en fonction de vos besoins :
     a. Dans la section **Sources des mises à jour**, configurez les paramètres de la source des mises à jour.
     b. Dans la section **Paramètres de la mise à jour**, gérez les paramètres d'optimisation du sous-système de disque, spécifiez les actions que Kaspersky Embedded Systems Security doit effectuer si des mises à jour critiques des modules de l'application sont disponibles ou si des informations sur les mises à jour planifiées sont disponibles, et définissez les paramètres de copie des mises à jour.
   - Pour configurer la tâche *Activation de l'application*, appliquez le fichier clé ou le code d'activation que vous souhaitez utiliser pour activer l'application. Cochez la case **Utiliser comme clé supplémentaire** si vous souhaitez ajouter un code d'activation ou un fichier clé pour renouveler la licence.
   - Pour configurer la génération automatique des règles d'autorisation pour le Contrôle des appareils, définissez les valeurs qui seront utilisées pour créer la liste des règles d'autorisation.
5. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche *Annulation de la mise à jour*).
6. Dans la section **Compte** de l'onglet **Configuration**, désignez le compte sous les privilèges duquel vous allez exécuter la tâche. Vous trouverez plus d'informations sur la configuration des paramètres de cette section dans le Système d'aide de Kaspersky Security Center.
7. Cliquez sur **Enregistrer**.

Les paramètres de la tâche de groupe définis seront enregistrés.

Configuration de la tâche Activation de l'application dans le plug-in Web

Pour configurer la tâche Activation de l'application, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.
3. Dans la section **Paramètres de l'application**, désignez le fichier clé à l'aide duquel vous souhaitez activer l'application. Cochez la case **Utiliser la clé en tant que clé de réserve** si vous souhaitez ajouter une clé pour renouveler la licence.
4. Configurez la planification des tâches dans la section **Planification**.
5. Dans la fenêtre **<Nom de la tâche>**, cliquez sur le bouton **Enregistrer**.

Configuration de la tâche Mise à jour dans le plug-in Web

Pour configurer la tâche Mise à jour, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Appareils** → **Tâches**.
2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre <Nom de la tâche> s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Dans la section **Sources des mises à jour**, configurez les paramètres de la source des mises à jour :

   a. Indiquez le Serveur d'administration de Kaspersky Security Center ou les Serveurs de mise à jour de Kaspersky en tant que source de mises à jour de l'application. Vous pouvez également composer une liste personnalisée de sources de mise à jour : ajouter manuellement d'autres serveurs HTTP ou FTP ou d'autres ressources réseau et les désigner comme source de mises à jour.

   Vous pouvez configurer l'utilisation des serveurs de mise à jour de Kaspersky en cas d'indisponibilité des serveurs personnalisés manuellement.

   b. Configurez les paramètres d'une fonctionnalité qui réduit la charge sur le sous-système de disque :

   - **Réduire la charge sur les I/O du disque**
   - **RAM utilisée pour l'optimisation, Mo**

   c. Spécifiez les actions que Kaspersky Embedded Systems Security doit effectuer lorsque des mises à jour critiques des modules de l'application sont disponibles ou lorsqu'il existe des informations sur les mises à jour planifiées.

   d. Spécifiez les paramètres de copie des mises à jour.

5. Dans la section **Planification**, configurez les paramètres de programmation de la tâche (vous pouvez configurer la programmation pour tous les types de tâche à l'exception de la tâche *Annulation de la mise à jour*).

6. Dans la fenêtre **<Nom de la tâche>**, cliquez sur le bouton **OK**.

Planification des tâches

Vous pouvez planifier des tâches système locales et personnalisées dans Web Console.

Pour planifier des tâches de groupe à l'aide de Web Console :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

2. Cliquez sur le nom de la tâche dans la liste des tâches de Kaspersky Security Center.

   La fenêtre **<Nom de la tâche>** s'ouvre.

3. Accédez à la section **Programmation** et configurez selon vos besoins les paramètres de la planification (cf. tableau ci-après).

   Les champs des paramètres de planification d'une tâche d'analyse à la demande ou d'une tâche de mise à jour ne sont pas accessibles si l'exécution planifiée de ces tâches est interdite par une stratégie de Kaspersky Security Center.

4. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres de lancement de la tâche.

Paramètres de planification de la tâche

Paramètre	Description
Lancement planifié	Sélectionnez le mode de fonctionnement de la tâche : • **Toutes les N heures**. La tâche sera exécutée périodiquement toutes les quelques heures. Spécifiez l'heure de lancement de la tâche et la période en heures. • **Tous les N jours**. La tâche sera exécutée périodiquement tous les quelques jours. Spécifiez l'heure de lancement de la tâche et la période en jours. • **Toutes les N minutes**. La tâche sera exécutée périodiquement toutes les quelques minutes. Spécifiez l'heure de lancement de la tâche et la période en minutes. • **Par jours de la semaine**. La tâche sera exécutée les jours indiqués de la semaine. Sélectionnez les jours de la semaine et indiquez l'heure de début. Si vous devez exécuter la tâche à intervalles de plusieurs semaines, saisissez la valeur souhaitée dans le champ **Intervalle**. • **Chaque mois**. La tâche sera exécutée un certain jour du mois. Spécifiez la date et l'heure de lancement. • **Une fois**. La tâche sera exécutée une fois à la date et à l'heure indiquées. • **Mode manuel**. Mode d'exécution dans lequel vous pouvez démarrer l'analyse manuellement à tout moment. • **Lors du téléchargement des mises à jour sur les stockages**. La tâche sera exécutée chaque fois que des mises à jour seront téléchargées dans le stockage. • **À la fin d'une autre tâche**. La tâche sera exécutée dès qu'une autre tâche aura terminé. Sélectionnez la tâche et son état d'achèvement. Kaspersky Embedded Systems Security ne prend pas en charge le mode **À la fin d'une autre tâche** pour la planification des tâches locales. • **Lors de la détection d'une propagation de virus**. La tâche sera exécutée si une attaque de virus est détectée. • **Démarrer N minutes après le lancement de l'application**. Après une période définie, la tâche sera lancée à chaque démarrage de Kaspersky Embedded Systems Security. Indiquez le nombre de minutes dans le champ **Décalage du lancement de la tâche (min.)**.

Paramètre	Description
Lancer les tâches non exécutées	Si la case est cochée, Kaspersky Embedded Systems Security exécute la tâche manquée dès que cela est possible. La tâche peut être ignorée, par exemple, si l'ordinateur était éteint à l'heure prévue de lancement de la tâche. Quand l'application a la possibilité d'exécuter les tâches non exécutées, elle les lance de manière aléatoire dans un certain intervalle de temps afin de répartir la charge sur l'ordinateur. Si la case est décochée, Kaspersky Embedded Systems Security n'exécute pas les tâches ignorées. Au lieu de cela, il effectue la prochaine tâche conformément à la planification en cours.
Adopter un décalage aléatoire automatique pour les lancements de tâche	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Décaler aléatoirement et automatiquement le lancement de la tâche dans un intervalle de	Si cette case est cochée, la tâche est exécutée sur les ordinateurs à un moment aléatoire dans une période définie. Les heures de lancement aléatoires permettent d'éviter qu'un grand nombre d'ordinateurs accèdent simultanément au Serveur d'administration lorsque la tâche est exécutée selon la planification. Si la case est décochée, la tâche est exécutée exactement à l'heure planifiée.
Allumer les appareils en utilisant la fonctionnalité Wake-on-LAN avant le lancement de la tâche	Si la case est cochée, le système d'exploitation de l'ordinateur dispose d'un délai déterminé pour terminer le lancement avant l'exécution de la tâche. Le délai par défaut est de 5 minutes. Cochez la case si vous souhaitez exécuter la tâche sur tous les ordinateurs, y compris sur les ordinateurs éteints.
Arrêter les appareils après la fin de la tâche	Si cette case est cochée, l'ordinateur s'éteint une fois la tâche terminée. Par exemple, vous pouvez activer cette fonctionnalité pour analyser l'ordinateur le vendredi après les heures de travail. Une fois la tâche terminée, l'application éteint l'ordinateur pour le week-end.
Arrêter la tâche si elle prend plus de	Limitez le temps d'exécution de la tâche. À l'issue du temps indiqué, Kaspersky Embedded Systems Security arrête la tâche. La tâche n'est pas marquée comme terminée. La prochaine fois que Kaspersky Embedded Systems Security exécutera la tâche, elle sera exécutée depuis le début et à la date prévue.
Suspendre l'exécution de la tâche	Vous pouvez définir un intervalle de temps pendant lequel l'exécution d'une tâche précédemment planifiée sera suspendue. Une fois la période définie écoulée, la tâche reprend. Cela peut s'avérer nécessaire, par exemple, pour limiter l'impact de Kaspersky Embedded Systems Security sur les performances de votre ordinateur pendant les périodes de forte utilisation. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.
Date de fin	Si la case est cochée, Kaspersky Embedded Systems Security arrêtera l'exécution de la tâche planifiée à partir de la date indiquée. La tâche sera définie en mode **Manuellement**. Cette fonctionnalité est disponible uniquement pour les tâches d'analyse à la demande.

Rapports dans Kaspersky Security Center

Les rapports dans Kaspersky Security Center contiennent des informations sur l'état des appareils administrés. Ils sont basés sur les informations stockées sur le serveur d'administration.

À partir de la version Kaspersky Security Center 11, les types de rapport suivants sont disponibles pour Kaspersky Embedded Systems Security :

- Rapport sur l'état des modules de l'application
- Rapport sur les applications interdites
- Rapport sur les applications interdites en mode test

Consultez l'aide de Kaspersky Security Center pour obtenir des informations détaillées sur tous les rapports de Kaspersky Security Center et la manière de les configurer.

Rapport sur l'état des modules de Kaspersky Embedded Systems Security

Vous pouvez surveiller l'état de protection de tous les appareils du réseau et obtenir une présentation structurée de l'ensemble de modules défini sur chaque appareil.

Le rapport affiche un des états suivants pour chaque module : *Exécution en cours*, *En pause*, *Arrêté*, *Non couvert par la licence*.

L'état *Non installé* fait référence au module, et non à l'application proprement dite. Si l'application n'est pas installée, Kaspersky Security Center Web Console attribue l'état N/D (Non disponible).

Vous pouvez créer des sélections de modules et utiliser le filtrage pour afficher les appareils de réseau avec l'ensemble défini de modules et leur état.

Cf. Aide de Kaspersky Security Center pour plus de détails sur la création et l'utilisation de sélections.

Pour consulter l'état des modules dans Kaspersky Security Center Web Console, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Ressources (Appareils)** → **Appareils administrés**.
2. Cliquez sur le nom de l'appareil et rendez-vous dans la section **Applications**.
3. Cliquez sur le nom de l'application Kaspersky Embedded Systems Security.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, accédez à la section **Module**.
5. Consultez le tableau d'état.

Pour consulter un rapport standard dans Kaspersky Security Center Web Console, procédez comme suit :

1. Choisissez **Surveillance** → **Rapports**.
2. Dans la liste, sélectionnez **Rapport sur l'état des modules de l'application** et cliquez dessus.

   Un rapport est généré.

3. Consultez les détails de rapport suivants :

   - Diagramme graphique.
   - Tableau récapitulatif des modules et nombres totaux d'appareils de réseau où chacun des modules est installé et groupes auxquels ils appartiennent.
   - Tableau détaillé spécifiant l'état des modules, la version, l' et le groupe.

Rapports sur les applications interdites dans les modes actifs et d'essai

Sur la base des résultats de l'exécution de la tâche Contrôle du lancement des applications, deux types de rapports peuvent être générés : un rapport sur les applications interdites (si la tâche est démarrée en mode Actif) et un rapport sur les applications interdites en mode test (si la tâche est démarrée en mode Informer). Ces rapports affichent des informations sur les applications interdites sur les appareils protégés du réseau. Chaque rapport est généré pour tous les groupes d'administration et accumule des données de toutes les applications Kaspersky installées sur les appareils protégés.

Pour afficher un rapport sur les applications interdites en mode Informer :

1. Exécutez la tâche Contrôle du lancement des applications en mode Informer.
2. Choisissez **Surveillance → Rapports**.
3. Dans la liste, sélectionnez **Rapport sur les applications interdites en mode test** et cliquez dessus.

   Un rapport est généré.
4. Consultez les détails de rapport suivants :

   - Diagramme graphique qui affiche les dix applications avec le plus grand nombre de démarrages bloqués.
   - Tableau récapitulatif des interdictions d'applications spécifiant le nom du fichier exécutable, la raison, l'heure de l'interdiction et le nombre d'appareils où elle est survenue.
   - Tableau détaillé spécifiant des données sur l'appareil, sur le chemin du fichier et sur les critères d'interdiction.

Pour afficher un rapport sur les applications interdites en mode Actif :

1. Exécutez la tâche Contrôle du lancement des applications en mode Actif.
2. Choisissez **Surveillance → Rapports**.
3. Dans la liste, sélectionnez **Rapport sur les applications interdites** et cliquez dessus.

   Un rapport est généré.

Ce rapport comprend les mêmes données au sujet des blocs que le rapport sur les applications interdites en mode test.

Licence de l'application

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

À propos du Contrat de licence

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

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

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

- Lors de l'installation de Kaspersky Embedded Systems Security.
- Lors de l'installation de la console de Kaspersky Embedded Systems Security.
- En lisant le fichier license.txt inclus dans le kit de distribution.
- Sur le site de Kaspersky (https://www.kaspersky.fr/business/eula).

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

À propos de la licence

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

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

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

Vous pouvez activer l'application de deux manières :

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

Après l'expiration de la licence commerciale, seuls les tâches et les modules de l'application suivants restent disponibles sans mises à jour des bases de données :

- Protection des fichiers en temps réel
- Contrôle de l'intégrité du système
- Tâche d'analyse à la demande définie par l'utilisateur

Pour continuer à utiliser toutes les fonctionnalités de Kaspersky Embedded Systems Security, il faut renouveler votre licence commerciale. Il est recommandé de prolonger la période de validité de la licence avant sa date d'expiration pour assurer une protection maximale.

Si vous supprimez la clé de licence, l'application continue de fonctionner. Le module Contrôle de l'intégrité du système reste disponible, les autres modules, les tâches et les mises à jour des bases de données de Kaspersky Embedded Systems Security deviennent inaccessibles. Il en va de même si Kaspersky ajoute votre licence à la liste de refus.

À propos du certificat de licence

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

Il reprend les informations suivantes relatives à la licence octroyée :

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

À propos de la clé

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

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

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

Une clé peut être active ou de réserve.

La *clé active* est la clé actuellement utilisée pour faire fonctionner l'application. Une clé pour une licence commerciale peut être ajoutée en tant que clé active. L'application ne peut compter qu'une seule clé active.

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

À propos du fichier clé

Un *fichier clé* est un fichier portant l'extension key que Kaspersky vous fournit. Le fichier clé permet d'ajouter une clé de licence pour activer l'application.

Après l'achat de Kaspersky Embedded Systems Security, vous recevrez le fichier clé à l'adresse email indiquée.

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

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

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

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

À propos du code d'activation

Un *code d'activation* est une séquence unique de 20 caractères alphanumériques. Vous devez saisir un code d'activation pour ajouter une clé d'activation de Kaspersky Embedded Systems Security. Vous recevrez un code d'activation à l'adresse email que vous avez indiquée après l'achat de Kaspersky Embedded Systems Security.

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

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

Comparaison des fonctionnalités des applications en fonction du type de licence

L'ensemble des fonctionnalités de Kaspersky Embedded Systems Security dépend du type de licence (voir le tableau ci-dessous).

Comparaison des fonctions de Kaspersky Embedded Systems Security

Fonction	Kaspersky Embedded Systems Security	Kaspersky Embedded Systems Security Compliance Edition
Protection des fichiers en temps réel	✓	✓
Analyse à la demande	✓	✓
Contrôle du lancement des applications	✓	✓
Contrôle des appareils	✓	✓
Pare-feu	✓	✓
Contrôle de l'intégrité des fichiers	–	✓
Inspection des journaux	–	✓

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

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

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

1. Dans l'arborescence de la Console de l'application, développez le nœud **Licence**.
2. Dans le volet de résultats du nœud **Licence**, cliquez sur le lien **Ajouter une clé**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir**.
4. Sélectionnez un fichier clé portant l'extension .key.

   Vous pouvez aussi ajouter une clé en tant que clé de réserve. Pour ce faire, cochez la case **Utiliser comme clé supplémentaire**.

5. Cliquez sur **OK**.

Le fichier clé sélectionné sera appliqué. Dans ce cas :

- Si une clé active a déjà été ajoutée pour activer l'application et que vous ajoutez une autre clé comme clé active, la nouvelle clé remplace l'ancienne. La clé ajoutée antérieurement est supprimée.
- Si une clé de réserve a déjà été ajoutée pour activer l'application et que vous ajoutez une autre clé en tant que clé de réserve, la nouvelle clé remplace l'ancienne. La clé de réserve ajoutée antérieurement est supprimée.
- Si une clé active et une clé de réserve ont déjà été ajoutées pour activer l'application et que vous ajoutez une nouvelle clé comme clé active, la nouvelle clé remplace l'ancienne clé active ; la clé de réserve n'est pas supprimée.

Les informations sur la clé ajoutée s'affichent dans le nœud **Licence**.

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

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

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

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

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

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

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

1. Dans l'arborescence de la Console de l'application, développez le nœud **Licence**.
2. Dans le volet de résultats du nœud **Licence**, cliquez sur le lien **Ajouter un code d'activation**.
3. Dans la fenêtre qui s'ouvre, saisissez le code d'activation dans le champ **Code d'activation**.
   - Si vous souhaitez utiliser le code d'activation en tant que clé de réserve, sélectionnez la case **Utiliser comme clé supplémentaire**.
   - Pour consulter les informations sur une licence, cliquez sur le bouton **Afficher les informations sur la licence**. Les informations s'afficheront dans le bloc **Informations sur la licence**.

4. Cliquez sur **OK**.

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

Consultation des informations sur la licence active

Consultation de l'état de la licence

Les informations sur l'état de la licence active s'affichent dans le panneau de détails du nœud **Kaspersky Embedded Systems Security** de la Console de l'application. L'état de la licence peut prendre les valeurs suivantes :

- **Vérification de l'état de la clé** : Kaspersky Embedded Systems Security analyse le fichier de clé ajoutée et attend une réponse concernant l'état actuel.
- **Date d'expiration** : Kaspersky Embedded Systems Security est actif jusqu'à la date indiquée. L'état est mis en évidence en jaune dans les cas suivants :
  - La licence expirera dans 30 jours et aucune clé de réserve n'a été ajoutée.
  - La clé ajoutée est inscrite sur la liste de refus et va bientôt être bloquée.
- **L'application n'est pas activée** – Kaspersky Embedded Systems Security n'est pas activé car la clé n'a pas été ajoutée. L'état est mis en évidence en rouge.
- **La licence a expiré** : Kaspersky Embedded Systems Security n'est pas actif parce que la licence a expiré. L'état est mis en évidence en rouge.
- **Le Contrat de licence utilisateur final a été violé** : Kaspersky Embedded Systems Security n'est pas actif, car les conditions du Contrat de licence utilisateur final ont été violées. L'état est mis en évidence en rouge.
- **La clé figure sur la liste de refus** : la clé ajoutée a été bloquée et inscrite sur la liste de refus par les experts de Kaspersky, par exemple, en cas d'utilisation d'une clé par des tiers pour l'activation illicite d'une application. L'état est mis en évidence en rouge.

Consultation des informations sur la licence active

Pour consulter les informations sur la licence active,

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

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

Informations générales sur la licence dans le nœud Licence

Champ	Description
État du code d'activation ou de la clé	État du code d'activation ou état de la clé : *Clé active* ou *Réserve*.
Date d'expiration	Date et heure d'expiration de la licence associée à une clé active.
Type de licence	Type de licence : *Licence commerciale*.
État de l'activation	Les informations sur l'état d'activation peuvent prendre les valeurs suivantes : • **Appliqué** : si vous avez activé l'application à l'aide d'une clé. • **Activation de l'application** : si vous avez appliqué un code d'activation pour activer l'application et que le processus est toujours en cours. L'état devient **Appliqué** à la fin de l'activation de l'application et le contenu du panneau de détails du nœud est mis à jour. • **Erreur d'activation** : apparaît en cas d'échec de l'activation de l'application. Vous pouvez voir la cause de l'échec de l'activation dans le journal d'exécution de la tâche.
Clé	Le numéro de la clé utilisée pour activer l'application.

Pour consulter les informations détaillées relatives à la licence,

Dans le panneau de détails du nœud **Licence**, ouvrez le menu contextuel de la licence que vous souhaitez visualiser et sélectionnez **Propriétés**.

Des informations détaillées sur la licence dans la fenêtre <Numéro de clé> des propriétés

Champ	Description
Clé	Le numéro de la clé utilisée pour activer l'application.
Application	Le nom de l'application activée avec la clé ajoutée.
Type de licence	Type de licence : commerciale ou d'essai.
Durée de la licence	Le nombre de jours, à compter de la date d'activation de l'application, de validité de la licence.
Date d'activation	Date d'ajout de la clé dans l'application.
Date d'expiration	Date d'expiration de la licence associée à une clé active. Si vous activez l'application selon un abonnement illimité, la valeur du champ est *Illimité*. Si Kaspersky Embedded Systems Security ne parvient pas à déterminer la date d'expiration de la licence, la valeur du champ est définie sur *Inconnu*.
Expire dans (jours)	Nombre de jours restants avant l'expiration de la licence associée à la clé active.
Accès au Support technique	Des informations relatives au support technique fournit aux clients par Kaspersky ou ses partenaires conformément aux conditions du contrat de licence.
Informations sur le Support technique	Coordonnées de Kaspersky ou du partenaire qui fournit le Support Technique. Le champ peut être vide en l'absence de Support Technique.
Informations relatives au détenteur	Informations relatives au client de la licence : nom du client ou de l'organisation pour laquelle une licence a été achetée.
Informations sur la licence	Le numéro et type de licence actuelle.
Fonctionnalité(s)	Les fonctions de l'application accessibles sous la licence.

Renouvelement de l'autorisation

Par défaut, Kaspersky Embedded Systems Security vous avertit lorsqu'il reste 30 jours avant la date d'expiration de la licence.

Vous pouvez renouveler la licence avant sa date d'expiration avec une clé de réserve. Ainsi, la protection de l'appareil ne sera pas interrompue entre la fin de la validité de la licence active et l'activation de l'application à l'aide d'une nouvelle licence.

Pour renouveler une licence :

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

     L'application d'un code d'activation requiert une connexion à Internet.
4. Cliquez sur **OK**.

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

Suppression de la clé

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

Pour supprimer une clé ajoutée auparavant, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Licence**.
2. Dans le tableau contenant les informations relatives aux clés ajoutées qui figure dans le panneau des résultats du nœud **Licence**, sélectionnez la clé que vous souhaitez supprimer.

3. Dans le menu contextuel de la ligne contenant les informations sur la clé sélectionnée, choisissez l'option **Supprimer**.

4. Dans la fenêtre de confirmation, cliquez sur **Oui** afin de confirmer la suppression de la clé.

La clé sélectionnée sera supprimée.

Lancement et arrêt de Kaspersky Embedded Systems Security

Cette section contient des informations sur le démarrage et l'arrêt de Kaspersky Embedded Systems Security, ainsi que sur le démarrage de la Console de Kaspersky Embedded Systems Security et du plug-in d'administration pour la Console d'administration de Kaspersky Security Center.

Démarrage et arrêt de l'application

Une fois installé sur l'ordinateur de l'utilisateur, Kaspersky Embedded Systems Security se lance automatiquement. Par la suite, le lancement de Kaspersky Embedded Systems Security a lieu par défaut directement après celui du système d'exploitation. Il n'est pas possible de configurer le lancement automatique de l'application dans les paramètres du système d'exploitation.

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

Comment configurer le lancement automatique de l'application dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Paramètres de l'application** → **Sécurité et fiabilité** et cliquez sur **Paramètres**.
4. Sous l'onglet **Sécurité**, cochez ou décochez la case **Lancer l'application au démarrage de l'ordinateur (recommandé)** pour activer ou désactiver l'exécution automatique de l'application.
5. Enregistrez vos modifications.

Comment configurer le lancement automatique de l'application dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Paramètres de l'application** → **Sécurité et fiabilité**.

5. Cliquez sur **Configurer**.

   La fenêtre **Sécurité et fiabilité** s'ouvre.

6. Utilisez la case **Lancer l'application au démarrage de l'ordinateur (recommandé)** pour activer ou désactiver le lancement automatique de l'application.

7. Enregistrez vos modifications.

Comment configurer le lancement automatique de l'application dans la Console de l'application

1. Sélectionnez le nœud **Kaspersky Embedded Systems Security** dans l'arborescence de la Console de l'application.

2. Dans le menu contextuel du nœud, sélectionnez **Propriétés de l'application**.

3. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres de sécurité**.

4. Utilisez la case **Lancer l'application au démarrage de l'ordinateur (recommandé)** pour activer ou désactiver le lancement automatique de l'application.

5. Enregistrez vos modifications.

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

Comment lancer ou arrêter l'application dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.

2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.

3. Ouvrez les propriétés de l'ordinateur d'un double clic.

4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.

5. Dans la liste des applications Kaspersky installées sur l'ordinateur, sélectionnez **Kaspersky Embedded Systems Security for Windows (4.0.1)**.

6. Réalisez une des opérations suivantes :

   - Si vous souhaitez lancez l'application, cliquez sur le bouton à droite de la liste des applications Kaspersky.

   - Si vous souhaitez arrêter l'application, cliquez sur le bouton à droite de la liste des applications Kaspersky.

Comment lancer ou arrêter l'application dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez lancer ou arrêter Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de l'ordinateur s'ouvre.
3. Sélectionnez l'onglet **Applications**.
4. Cochez la case en face de **Kaspersky Embedded Systems Security for Windows (4.0.1)**.
5. Cliquez sur le bouton **Démarrer** ou **Arrêter**.

Comment démarrer ou arrêter l'application dans la Console de l'application

1. Pour arrêter Kaspersky Embedded Systems Security :
   a. Ouvrez la Console de l'application.

      Le compte utilisateur doit disposer des autorisations permettant d'accéder à la fonctionnalité **Fermer l'application**.

   b. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.
   c. Sélectionnez **Arrêter l'application**.
   d. Dans la fenêtre de confirmation, cliquez sur le bouton **Oui** pour confirmer l'arrêt de l'application.

      L'application sera arrêtée.
2. Pour lancer **Kaspersky Embedded Systems Security** :
   a. Exécutez le fichier avpui.exe situé dans le dossier d'installation de la Console de l'application sur l'appareil protégé. Par défaut, ce fichier se trouve dans le dossier C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security Console.

      La fenêtre **Sélectionner un appareil protégé** s'ouvre.
   b. Si Kaspersky Embedded Systems Security et la Console de l'application sont installés sur le même ordinateur, sélectionnez l'option **Ordinateur local (l'ordinateur sur lequel la Console de l'application est exécutée)**.
   c. Si Kaspersky Embedded Systems Security et la Console de l'application sont installés sur des ordinateurs différents :
      1. Sélectionnez **Autre appareil**.
      2. Cliquez sur **Parcourir** et indiquez le nom de l'ordinateur sur lequel l'application est installée.

3. Indiquez le port de connexion à l'ordinateur sur lequel l'application est installée :

   - **Utilisation des identifiants Windows**. Un port de connexion à l'aide des identifiants Windows. La valeur par défaut est 13032.

   - **Utilisation des identifiants d'utilisateurs créés manuellement**. Un port de connexion à l'aide des identifiants des utilisateurs créés manuellement. La valeur par défaut est 13031.

d. Si nécessaire, activez la fonctionnalité **Utiliser l'authentification** et saisissez les identifiants permettant de connecter la Console de l'application à l'ordinateur sur lequel l'application est installée. Le compte utilisateur indiqué doit disposer des autorisations permettant d'accéder aux fonctionnalités **Paramètres de lecture** et **Connexion à distance à l'application** sur l'ordinateur où l'application est installée.

e. Cliquez sur **Service d'administration des applications**.

f. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Démarrer**.

   L'application sera lancée.

La fenêtre **Sélectionner un appareil protégé** s'affiche également si la connexion à l'ordinateur sur lequel l'application est installée est perdue ou si le service KESS échoue. Vous pouvez restaurer le service KESS en cliquant sur le bouton **Lancer**.

Vous pouvez également lancer ou arrêter l'application via la ligne de commande.

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

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

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

- L'icône signale la suspension de la protection et du contrôle de l'ordinateur.

- L'icône indique que la protection et le contrôle de l'ordinateur sont activés.

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

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

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

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security**.

2. Sélectionnez **Suspendre la protection**.

3. Choisissez l'une des options suivantes :

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

   Kaspersky Embedded Systems Security suspend tous les modules de la protection et de contrôle qui ne sont pas accompagnés d'un cadenas dans la stratégie ( ).

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

1. Ouvrez le menu contextuel de l'icône de l'application, qui se trouve dans la zone de notification de la barre des tâches.
2. Sélectionnez **Rétablir la protection** dans le menu contextuel.

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

Interface de diagnostic compacte

Cette section décrit l'utilisation de l'Interface de diagnostic compacte.

À propos de l'interface de diagnostic compacte

Le module Interface de diagnostic compacte est installé et désinstallé avec le module Icône dans la barre d'état système indépendamment de la Console de l'application et peut être utilisé quand la Console de l'application n'est pas installée sur l'appareil protégé. L'interface de diagnostic compacte est lancée depuis l'icône de la barre d'état système ou via l'exécution du fichier avpui.exe à partir du dossier de l'application sur l'appareil protégé.

L'interface de diagnostic compacte permet de réaliser les opérations suivantes :

- Ouvrez la fenêtre **À propos** qui reprend la liste des mises à jour et des correctifs disponibles.
- Examiner les informations sur l'état général de l'application.
- Examiner les incidents de sécurité qui se sont produits.
- Examiner l'activité en cours sur l'appareil protégé.
- Lancer ou arrêter l'écriture des fichiers de vidage et de traçage.
- Ouvrez la Console de l'application.

L'interface de diagnostic compacte est disponible même si l'accès aux fonctions de Kaspersky Embedded Systems Security est protégé par un mot de passe. Aucun mot de passe requis.

L'interface de diagnostic compacte ne peut pas être configurée via Kaspersky Security Center.

Révision de l'état de Kaspersky Embedded Systems Security via l'interface de diagnostic compacte

Pour afficher l'état de l'application à l'aide de l'Interface de diagnostic compacte :

1. Ouvrez l'Interface de diagnostic compacte d'une des manières suivantes :
   - Exécutez le fichier avpui.exe situé dans le dossier d'installation de l'application sur l'appareil protégé. Par défaut, le fichier se trouve dans C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
   - Cliquez sur l'icône de l'application dans la zone de notification de la barre des tâches.

2. Consultez l'état actuel de la clé, des tâches Protection en temps réel de l'ordinateur et des tâches de mise à jour dans la section **État de la protection**. Différentes couleurs sont utilisées pour avertir l'utilisateur sur l'état de la protection (cf. tableau ci-dessous).

Indication de couleur dans la fenêtre de l'Interface de diagnostic compacte

Section	État
État de la protection en temps réel	Le panneau est *vert* si les conditions suivantes sont remplies : • Le module Protection des fichiers en temps réel est activé. • Le module Contrôle du lancement des applications est en cours d'exécution en mode **Bloquer**.
	Le panneau est *jaune* si une ou plusieurs des conditions suivantes sont remplies : • Le module Protection des fichiers en temps réel est désactivé. • Le module Contrôle du lancement des applications est en cours d'exécution en mode **Informer**.
	Le panneau est *rouge* si les deux conditions suivantes sont remplies : • Le module Protection des fichiers en temps réel est désactivé ou non installé. • Le module Contrôle du lancement des applications n'est pas installé ou est lancé en mode **Informer**.
Licence	Le panneau est *vert* si la licence en cours est valide.
	Un panneau *jaune* indique qu'un des événements suivants s'est produit : • *Vérification de l'état de la licence.* • *Il reste 14 jours avant l'expiration de la licence et aucune clé additionnelle ou code d'activation n'a été ajouté.* • *La clé ajoutée est inscrite sur la liste de refus et va bientôt être bloquée.*
	Un panneau *rouge* indique qu'un des événements suivants s'est produit : • *L'application n'est pas activée.* • *La licence a expiré.* • *Le Contrat de licence utilisateur final a été violé.* • *La clé figure sur la liste de refus.*
Mise à jour	Le panneau est *vert* lorsque les bases de l'application sont à jour.
	Le panneau est *jaune* lorsque les bases de l'application sont dépassées.
	Le panneau est *rouge* lorsque les bases de l'application sont fortement dépassées.

Révision des statistiques des événements de sécurité

La section **Statistiques** affiche tous les événements de sécurité. Les statistiques de chaque tâche de protection s'affichent dans un bloc séparé, spécifiant le nombre d'incidents, ainsi que la date et l'heure de survenue du dernier incident. Lorsqu'un incident est enregistré, le bloc devient rouge.

Pour consulter les statistiques, procédez comme suit :

1. Ouvrez l'Interface de diagnostic compacte d'une des manières suivantes :

   - Exécutez le fichier avpui.exe situé dans le dossier d'installation de l'application sur l'appareil protégé. Par défaut, le fichier se trouve dans C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.

   - Cliquez sur l'icône de l'application dans la zone de notification de la barre des tâches.

2. Passez à la section **Statistiques**.

3. Révisez les incidents de sécurité pour les tâches de protection.

Révision de l'activité en cours de l'application

Pour consulter l'activité en cours de l'application sur l'appareil protégé :

1. Ouvrez l'Interface de diagnostic compacte d'une des manières suivantes :
    - Exécutez le fichier avpui.exe situé dans le dossier d'installation de l'application sur l'appareil protégé. Par défaut, le fichier se trouve dans C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
    - Cliquez sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Passez à la section **Activité actuelle de l'application**.

Différentes couleurs sont utilisées pour indiquer l'état de l'activité de l'application :

- Dans la section **Tâches** :
    - *Vert*. Il n'y a aucune condition qui pourrait nécessité le jaune ou le rouge.
    - *Jaune*. Analyse rapide non réalisée depuis longtemps.
    - *Rouge*. Au moins une des conditions suivantes est remplie :
        - Aucune tâche n'est lancée et la planification du lancement n'est défini pour aucune des tâches.
        - Les erreurs de lancement de l'application sont consignées en tant qu'événements critiques.
- Dans la section **Kaspersky Security Network** :
    - *Vert*. La tâche **Utilisation de KSN** est lancée.
    - *Jaune*. La Déclaration de KSN est acceptée, mais la tâche n'est pas lancée.

Configuration du traçage de l'application et de l'enregistrement des vidages de la mémoire

Pour configurer le traçage de l'application et l'enregistrement du vidage de la mémoire, procédez comme suit :

1. Ouvrez l'Interface de diagnostic compacte d'une des manières suivantes :
    - Exécutez le fichier avpui.exe situé dans le dossier d'installation de l'application sur l'appareil protégé. Par défaut, le fichier se trouve dans C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
    - Cliquez sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Passez à la section **Diagnostic de dysfonctionnement**.

3. Utilisez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage.

   Si la protection des fichiers de vidage et des fichiers de traçage est activée, l'accès aux fichiers est réservé aux utilisateurs suivants :

   - Les fichiers dump sont accessibles aux administrateurs local et système ainsi qu'à l'utilisateur qui a activé l'enregistrement des fichiers dump et des fichiers de traçage.
   - Les fichiers de traçage sont accessibles uniquement aux administrateurs local et système.

4. Utilisez la case **Écrire les informations de débogage dans le fichier de traçage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   Par défaut, le traçage du fonctionnement de l'application est désactivé.

5. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour ce faire, cliquez sur le bouton **Parcourir** et sélectionnez le dossier requis.

   > Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

   Dans le dossier sélectionné, Kaspersky Embedded Systems Security crée un sous-dossier nommé « logs-Kaspersky Embedded Systems Security-<uid> » pour stocker les fichiers de traçage, où <uid> est un identifiant de journal unique à 8 caractères.

6. Sélectionnez le niveau de détail des informations de débogage :

   - **Normal** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application (option par défaut).
   - **Critique** signifie que le fichier de traçage enregistre uniquement les messages relatifs aux erreurs critiques.
   - **Diagnostic** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, ainsi que les avertissements.
   - **Important** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements et des informations complémentaires.
   - **Détaillé** signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.

   Un opérateur du Support Technique détermine le niveau de détails requis pour résoudre un éventuel problème.

7. Pour supprimer les anciens fichiers de traçage, activez la fonctionnalité **Supprimer les fichiers de traçage les plus anciens**.

   Si cette fonctionnalité est activée, configurez la taille maximale et le nombre de fichiers de traçage :

   a. Définissez le paramètre **Taille maximale d'un fichier de traçage (Mo)**.

      Valeurs disponibles : de 1 à 4 095 Mo. La valeur par défaut est 100 Mo.

   b. Définissez le paramètre **Nombre maximal de fichiers de traçage**.

      Valeurs disponibles : de 1 à 999. La valeur par défaut est 5.

8. Utilisez la case **Créer un fichier dump dans ce dossier en cas de dysfonctionnement** pour activer ou désactiver le traçage du fonctionnement de l'application.

   L'enregistrement du vidage de la mémoire est désactivé par défaut.

9. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour ce faire, cliquez sur le bouton **Parcourir** et sélectionnez le dossier requis.

   Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

10. Cliquez sur **Appliquer**.

Auto-défense de Kaspersky Embedded Systems Security

L'auto-défense empêche les autres applications d'exécuter des actions qui peuvent altérer le fonctionnement de Kaspersky Embedded Systems Security. L'application inclut des mécanismes d'auto-défense qui protègent l'application contre la modification ou la suppression de ses dossiers, des processus de mémoire et des entrées du registre du système. Kaspersky Embedded Systems Security prend en charge la technologie Antimalware Protected Process Light (AM-PPL) de Microsoft qui protège les processus des applications contre les actions malveillantes. De plus, l'application permet de gérer séparément les autorisations d'accès des utilisateurs aux fonctionnalités de l'application et aux services de l'application.

Activation et désactivation du mécanisme de l'autodéfense

Kaspersky Embedded Systems Security empêche la modification ou la suppression des fichiers d'application sur le disque dur, les processus de mémoire et les entrées dans le registre système.

Cette technologie bloque l'accès aux modules d'application suivants :

- Fichiers du dossier d'installation de Kaspersky Embedded Systems Security et autres fichiers de l'application ;
- Clés de registre avec des enregistrements appartenant à l'application ;
- Processus que l'application exécute.

> Les mécanismes d'autodéfense ne s'appliquent pas aux processus de Kaspersky Embedded Systems Security lancés par des processus parents non fiables.

Les mécanismes d'auto-défense de Kaspersky Embedded Systems Security sont activés par défaut.

Comment activer ou désactiver l'Autodéfense dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Paramètres de l'application**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Sécurité et fiabilité**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Sécurité**.
6. Dans le groupe **Autodéfense**, utilisez la case **Protéger les processus d'application contre les menaces externes** pour activer ou désactiver l'Autodéfense.

7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver l'Autodéfense dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et, dans le panneau des résultats, suivez le lien **Propriétés de l'application**.

2. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres de sécurité**.

3. Dans le groupe **Autodéfense**, utilisez la case **Protéger les processus d'application contre les menaces externes** pour activer ou désactiver l'Autodéfense.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver l'Autodéfense dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Paramètres de l'application**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Sécurité et fiabilité**.

   La fenêtre **Sécurité et fiabilité** s'ouvre.

6. Dans le groupe **Autodéfense**, utilisez la case **Protéger les processus de l'application contre les menaces externes** pour activer ou désactiver l'Autodéfense.

7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Prise en charge de la technologie AM-PPL

Kaspersky Embedded Systems Security prend en charge la technologie Antimalware Protected Process Light (ci-après « AM-PPL ») de Microsoft. La technologie AM-PPL protège les processus de Kaspersky Embedded Systems Security contre les actions malveillantes (par exemple, l'arrêt d'une application). La technologie AM-PPL autorise uniquement l'exécution de processus de confiance. Les processus de Kaspersky Embedded Systems Security sont signés conformément aux exigences de sécurité de Windows et sont dès lors considérés comme des processus de confiance. Pour en savoir plus sur la technologie AM-PPL, consultez le site de Microsoft. La technologie est activée par défaut AM-PPL.

Kaspersky Embedded Systems Security intègre également des mécanismes de protection des processus de l'application. La prise en charge de la technologie AM-PPL permet de déléguer les fonctions de protection des processus au système d'exploitation. Ainsi, vous augmentez la rapidité de l'application et réduisez la consommation des ressources de l'ordinateur.

L'application enregistre les services Kaspersky Embedded Systems Security (AVP) et Kaspersky Seamless Update Service (AVPSUS). La technologie AM-PPL protège uniquement le service AVP.

Conservez la technologie AM-PPL toujours active. Le module AM-PPL est un module important de la protection du système d'exploitation. La désactivation de AM-PPL n'est possible que dans un environnement de test distinct, dans le but de dépanner l'application.

La technologie AM-PPL est disponible pour les systèmes d'exploitation Windows 10 version 1703 (RS2) et suivantes et Windows Server 2019.

Pour activer ou désactiver la prise en charge de la technologie AM-PPL, procédez comme suit :

1. Désactivez le mécanisme d'autodéfense de l'application.

   Le mécanisme d'autodéfense empêche la modification et la suppression de processus de l'application dans la mémoire de l'ordinateur, y compris la modification de l'état de la technologie AM-PPL.

2. Lancez l'interpréteur de ligne de commande (cmd) au nom de l'administrateur.
3. Accédez au dossier dans lequel se trouve le fichier exécutable de Kaspersky Embedded Systems Security.
4. Pour activer la prise en charge de la technologie AM-PPL, exécutez la commande suivante :

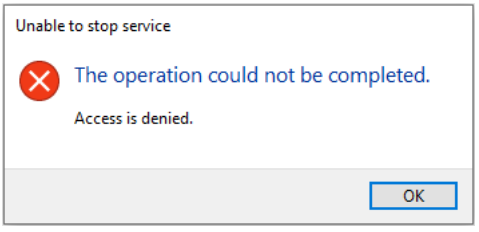
   ```
   klpsm.exe enable
   ```

5. Pour désactiver la prise en charge de la technologie AM-PPL, exécutez la commande suivante :

   ```
   klpsm.exe disable
   ```

6. Relancez Kaspersky Embedded Systems Security.
7. Restaurez le mécanisme d'autodéfense de l'application.

Par conséquent, lorsqu'un utilisateur tente d'arrêter le service AVP, une fenêtre système contenant un message d'erreur apparaît. L'utilisateur ne peut gérer les services d'application qu'à partir de l'interface de Kaspersky Embedded Systems Security.



Erreur d'accès aux services de l'application

Protection des services du système d'exploitation

Vous pouvez utiliser la fonctionnalité Protéger les services du système d'exploitation pour autoriser ou interdire les applications tierces à agir sur les services du système d'exploitation.

Comment activer ou désactiver la protection des services du système d'exploitation dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Paramètres de l'application**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Sécurité et fiabilité**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Sécurité**.
6. Utilisez la case **Protéger les services du système d'exploitation** pour activer ou désactiver la protection des services du système d'exploitation.

   Si la protection des services du système d'exploitation est activée, les applications tierces ne peuvent pas agir sur les processus du système d'exploitation.

   Si la protection des services du système d'exploitation est désactivée, des applications tierces peuvent agir sur les processus du système d'exploitation.

   Une fois que vous avez activé ou désactivé la fonction, il faut redémarrer l'ordinateur pour que les modifications soient appliquées.
7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.
8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver la protection des services du système d'exploitation dans la Console d'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et, dans le panneau des résultats, suivez le lien **Propriétés de l'application**.
2. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres de sécurité**.
3. Utilisez la case **Protéger les services du système d'exploitation** pour activer ou désactiver la protection des services du système d'exploitation.

   Si la protection des services du système d'exploitation est activée, les applications tierces ne peuvent pas agir sur les processus du système d'exploitation.

   Si la protection des services du système d'exploitation est désactivée, des applications tierces peuvent agir sur les processus du système d'exploitation.

   Une fois que vous avez activé ou désactivé la fonction, il faut redémarrer l'ordinateur pour que les modifications soient appliquées.
4. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver la protection des services du système d'exploitation dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Paramètres de l'application**.
5. Cliquez sur le bouton **Configurer** dans le groupe **Sécurité et fiabilité**.

   La fenêtre **Sécurité et fiabilité** s'ouvre.
6. Utilisez la case **Protéger les services du système d'exploitation** pour activer ou désactiver la protection des services du système d'exploitation.

   Si la protection des services du système d'exploitation est activée, les applications tierces ne peuvent pas agir sur les processus du système d'exploitation.

   Si la protection des services du système d'exploitation est désactivée, des applications tierces peuvent agir sur les processus du système d'exploitation.

   Une fois que vous avez activé ou désactivé la fonction, il faut redémarrer l'ordinateur pour que les modifications soient appliquées.
7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.
8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Configuration des autorisations utilisateurs pour administrer Kaspersky Embedded Systems Security

Par défaut, toutes les fonctionnalités de Kaspersky Embedded Systems Security sont accessibles aux membres du groupe Administrateurs sur l'appareil protégé et aux membres du groupe Administrateurs ESS créé sur l'appareil protégé lors de l'installation de Kaspersky Embedded Systems Security ainsi qu'au groupe SYSTEM.

Si l'utilisateur ne figure pas dans la liste des utilisateurs de Kaspersky Embedded Systems Security, il ne pourra pas ouvrir la Console de l'application.

Vous pouvez autoriser ou interdire l'accès à certaines fonctions de Kaspersky Embedded Systems Security à des utilisateurs individuels ou à des groupes d'utilisateurs.

À propos des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security

Autorisations d'accès	Description
Gérer les tâches	Lancement/arrêt/suspension/reprise d'une tâche de Kaspersky Embedded Systems Security.
Créer et supprimer les tâches	Création et suppression d'une tâche d'analyse à la demande.
Modifier les paramètres	Possibilités : • Importation des paramètres de Kaspersky Embedded Systems Security depuis un fichier de configuration. • Modifiez les paramètres de l'application.

Autorisations d'accès	Description
Paramètres de lecture	Possibilités : • Consultation des paramètres généraux de Kaspersky Embedded Systems Security et des paramètres des tâches. • Exportation des paramètres de Kaspersky Embedded Systems Security vers un fichier de configuration. • Consultation des paramètres des journaux d'exécution des tâches, du journal d'audit système et des notifications.
Gérer les 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.
Gérer les journaux	Suppression des journaux d'exécution des tâches et purge du journal d'audit système.
Lire les journaux	Possibilité de consulter les événements dans les journaux d'exécution des tâches et le journal d'audit système.
Récupérer les statistiques	Consultation des statistiques de chacune des tâches de Kaspersky Embedded Systems Security.
Gérer les licences de l'application	Fonction d'activation de Kaspersky Embedded Systems Security.
Désinstaller l'application	Fonction de désinstallation de Kaspersky Embedded Systems Security.
Lire les autorisations	Possibilité de consulter la liste des utilisateurs de Kaspersky Embedded Systems Security et des privilèges d'accès de ceux-ci.
Modifier les autorisations	Possibilités : • Modifier la liste des utilisateurs qui ont accès à l'administration de l'application ; • Modification des autorisations d'accès pour les fonctions de Kaspersky Embedded Systems Security.
Connexion à distance à l'application	Connexion à distance à l'application à l'aide de la Console de l'application. Pour pouvoir accéder à distance à l'application, l'utilisateur doit en outre disposer des droits d'accès à la fonctionnalité **Paramètres de lecture**.
Fermer l'application	Possibilité de quitter l'application à l'aide de la console d'application.
Désactiver la stratégie de Kaspersky Security Center	Possibilité de désactiver la stratégie de Kaspersky Security Center.
Exporter les paramètres	Possibilité d'exporter les paramètres de Kaspersky Embedded Systems Security.
Modifier le diagnostic de dysfonctionnement	Possibilité de configurer le traçage de l'application et l'enregistrement du vidage de la mémoire.

Comment configurer les autorisations des utilisateurs pour gérer Kaspersky Embedded Systems Security dans la Console d'administration de Kaspersky Security Center ?

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Complémentaire**.
4. Dans la section **Autorisations d'accès des utilisateurs pour la gestion des applications**, cliquez sur **Paramètres**.
5. Cette action ouvre une fenêtre ; dans cette fenêtre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement** et définissez un mot de passe pour le compte utilisateur KLAdmin. Le compte utilisateur est ajouté automatiquement à la liste des comptes utilisateurs.

6. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications. Pour ce faire, cliquez sur **Ajouter** dans le tableau des comptes utilisateurs.

   Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

7. Sélectionnez la méthode souhaitée pour ajouter des utilisateurs :

   - **Sélectionner un utilisateur/un groupe à partir d'Active Directory**. Vous pouvez accorder l'accès à Kaspersky Embedded Systems Security à des utilisateurs individuels ou à des groupes au sein du domaine Active Directory. Par exemple si le groupe "Tous" ne peut pas quitter l'application, vous pouvez octroyer l'autorisation **Fermer l'application** à un utilisateur en particulier.

   - **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**. Vous pouvez créer un compte utilisateur qui n'est pas présent dans Active Directory et lui attribuer des autorisations individuelles. Autrement dit, vous pouvez créer un *compte utilisateur de service* et l'utiliser à la place de KLAdmin. Vous n'avez donc pas besoin de partager votre mot de passe KLAdmin avec d'autres utilisateurs ni de créer différents comptes utilisateurs Active Directory. Vous pouvez définir n'importe quel nom d'utilisateur et n'importe quel mot de passe. Par exemple, vous pouvez accorder l'autorisation **Lire les journaux** au compte utilisateur de service. Par conséquent, si la consultation des rapports est interdite au groupe « Tous », vous pouvez ouvrir les rapports à l'aide du compte utilisateur de service ou du compte utilisateur KLAdmin.

     Pour ajouter un utilisateur ou un groupe d'utilisateurs manuellement, vous devez activer la protection par mot de passe.

8. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

9. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Configuration des autorisations des utilisateurs pour administrer Kaspersky Embedded Systems Security dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Autorisations d'accès des utilisateurs pour la gestion des applications** dans le menu contextuel du nœud.

2. Cette action ouvre une fenêtre ; dans cette fenêtre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement** et définissez un mot de passe pour le compte utilisateur KLAdmin. Le compte utilisateur est ajouté automatiquement à la liste des comptes utilisateurs.

3. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications. Pour ce faire, cliquez sur **Ajouter** dans le tableau des comptes utilisateurs.

   Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

4. Sélectionnez la méthode souhaitée pour ajouter des utilisateurs :

   - **Sélectionner un utilisateur/un groupe à partir d'Active Directory**. Vous pouvez accorder l'accès à Kaspersky Embedded Systems Security à des utilisateurs individuels ou à des groupes au sein du domaine Active Directory. Par exemple si le groupe "Tous" ne peut pas quitter l'application, vous pouvez octroyer l'autorisation **Fermer l'application** à un utilisateur en particulier.

   - **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**. Vous pouvez créer un compte utilisateur qui n'est pas présent dans Active Directory et lui attribuer des autorisations individuelles. Autrement dit, vous pouvez créer un *compte utilisateur de service* et l'utiliser à la place de KLAdmin. Vous n'avez donc pas besoin de partager votre mot de passe KLAdmin avec d'autres utilisateurs ni de créer différents comptes utilisateurs Active Directory. Vous pouvez définir n'importe quel nom d'utilisateur et n'importe quel mot de passe. Par exemple, vous pouvez accorder l'autorisation **Lire les journaux** au compte utilisateur de service. Par conséquent, si la consultation des rapports est interdite au groupe « Tous », vous pouvez ouvrir les rapports à l'aide du compte utilisateur de service ou du compte utilisateur KLAdmin.

     Pour ajouter un utilisateur ou un groupe d'utilisateurs manuellement, vous devez activer la protection par mot de passe.

5. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

6. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

7. Enregistrez vos modifications.

Comment configurer les droits d'accès des utilisateurs pour gérer Kaspersky Embedded Systems Security dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Complémentaire → Autorisations d'accès des utilisateurs pour la gestion des applications** et cliquez sur le bouton **Configurer**.

5. Cette action ouvre une fenêtre ; dans cette fenêtre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement** et définissez un mot de passe pour le compte utilisateur KLAdmin. Le compte utilisateur est ajouté automatiquement à la liste des comptes utilisateurs.

6. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications. Pour ce faire, cliquez sur **Ajouter** dans le tableau des comptes utilisateurs.

   Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

7. Sélectionnez la méthode souhaitée pour ajouter des utilisateurs :

   - **Sélectionner un utilisateur/un groupe à partir d'Active Directory**. Vous pouvez accorder l'accès à Kaspersky Embedded Systems Security à des utilisateurs individuels ou à des groupes au sein du domaine Active Directory. Par exemple si le groupe "Tous" ne peut pas quitter l'application, vous pouvez octroyer l'autorisation **Fermer l'application** à un utilisateur en particulier.

   - **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**. Vous pouvez créer un compte utilisateur qui n'est pas présent dans Active Directory et lui attribuer des autorisations individuelles. Autrement dit, vous pouvez créer un *compte utilisateur de service* et l'utiliser à la place de KLAdmin. Vous n'avez donc pas besoin de partager votre mot de passe KLAdmin avec d'autres utilisateurs ni de créer différents comptes utilisateurs Active Directory. Vous pouvez définir n'importe quel nom d'utilisateur et n'importe quel mot de passe. Par exemple, vous pouvez accorder l'autorisation **Lire les journaux** au compte utilisateur de service. Par conséquent, si la consultation des rapports est interdite au groupe « Tous », vous pouvez ouvrir les rapports à l'aide du compte utilisateur de service ou du compte utilisateur KLAdmin.

     Pour ajouter un utilisateur ou un groupe d'utilisateurs manuellement, vous devez activer la protection par mot de passe.

8. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

9. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Configuration des autorisations d'accès des utilisateurs pour gérer le service Kaspersky Embedded Systems Security

Lors de l'installation, Kaspersky Embedded Systems Security enregistre le service de l'application, *Kaspersky Embedded Systems Security Service*, sous Windows. Ainsi, l'application inclut des modules fonctionnels qui commencent au lancement du système d'exploitation. Pour réduire le risque d'accès par des tiers aux fonctionnalités de l'application et aux paramètres de sécurité de l'appareil protégé via le service de l'application, vous pouvez restreindre les autorisations de gestion du Kaspersky Embedded Systems Security Service.

Par défaut, le droit de gérer le Kaspersky Embedded Systems Security Service est accordé aux utilisateurs du groupe Administrateurs de l'appareil protégé. L'accès en lecture est octroyé aux groupes SERVICE et INTERACTIVE ; l'accès en lecture et en exécution est octroyé au groupe SYSTEM.

Il est impossible de supprimer le compte utilisateur SYSTEM ou de modifier les autorisations de ce compte. Si les autorisations du compte SYSTEM sont modifiées, les autorisations maximales sont rétablies pour ce compte lors de l'enregistrement des modifications.

Les utilisateurs qui disposent d'un accès aux fonctionnalités correspondant au niveau « Modifier les privilèges » peuvent accorder des autorisations de gestion du Kaspersky Embedded Systems Security Service à d'autres utilisateurs enregistrés sur l'appareil protégé ou appartenant au domaine.

Vous pouvez sélectionner l'un des niveaux prédéfinis suivants d'accès à l'administration du Kaspersky Embedded Systems Security Service pour un utilisateur ou un groupe de Kaspersky Embedded Systems Security :

- **Contrôle total** : possibilité de consulter et de modifier les paramètres généraux et les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service, ainsi que de démarrer et d'arrêter le Kaspersky Embedded Systems Security Service.
- **Lecture** : possibilité de consulter les paramètres généraux et les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.
- **Modifier** : possibilité de consulter et de modifier les paramètres généraux et les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.
- **Exécuter** : possibilité de démarrer et d'arrêter le Kaspersky Embedded Systems Security Service.

Vous pouvez également réaliser une configuration étendue des autorisations d'accès : autoriser ou interdire l'accès à des fonctions particulières de Kaspersky Embedded Systems Security (voir tableau ci-dessous).

Autorisations d'accès aux fonctionnalités du Kaspersky Embedded Systems Security Service

Fonction	Description
Lire les paramètres du service	Possibilité de consulter les paramètres généraux et les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.
Solliciter l'état du service auprès du Gestionnaire de contrôle des services	Possibilité de demander l'état d'exécution du Kaspersky Embedded Systems Security Service au Gestionnaire de contrôle des services Microsoft Windows.
Solliciter l'état du service	Possibilité d'interroger le Kaspersky Embedded Systems Security Service sur l'état d'exécution du service.
Lire la liste des services dépendants	Possibilité de consulter la liste des services dont dépend le Kaspersky Embedded Systems Security Service et de ceux qui dépendent du Kaspersky Embedded Systems Security Service.
Modifier les paramètres du service	Possibilité de consulter et de modifier les paramètres généraux et les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.
Démarrer le service	Possibilité de démarrer le Kaspersky Embedded Systems Security Service.
Arrêter le service	Possibilité d'arrêter le Kaspersky Embedded Systems Security Service.
Suspendre/Reprendre le service	Possibilité de suspendre et de reprendre le Kaspersky Embedded Systems Security Service.
Lire les autorisations	Possibilité de consulter la liste des utilisateurs du Kaspersky Embedded Systems Security Service et les privilèges d'accès de chacun d'entre eux.
Modifier les autorisations	Possibilités : • Ajouter ou supprimer des utilisateurs du Kaspersky Embedded Systems Security Service. • Modifier les autorisations d'accès des utilisateurs au Kaspersky Embedded Systems Security Service.
Supprimer le service	Possibilité d'annuler l'enregistrement du Kaspersky Embedded Systems Security Service dans le Gestionnaire de contrôle des services Microsoft Windows.
Requêtes de l'utilisateur au service	Possibilité de créer et d'envoyer des requêtes utilisateur au Kaspersky Embedded Systems Security Service.

Vous pouvez modifier la liste des utilisateurs et groupes d'utilisateurs autorisés à administrer le Kaspersky Embedded Systems Security Service, ainsi que les autorisations d'accès de ces utilisateurs et groupes d'utilisateurs.

Comment configurer les autorisations des utilisateurs pour gérer le Kaspersky Embedded Systems Security Service dans la Console d'administration de Kaspersky Security Center ?

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Complémentaire**.

4. Dans la section **Autorisations d'accès utilisateur pour l'administration du Service KESS**, cliquez sur **Paramètres**.

   Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

5. Ajoutez un utilisateur ou un groupe Active Directory pour lequel vous souhaitez configurer les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.

6. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

7. Configurez dans la liste des autorisations les autorisations des utilisateurs pour gérer le Kaspersky Embedded Systems Security Service.

8. Si nécessaire, configurez des autorisations spéciales pour les utilisateurs :

   a. Cliquez sur **Supplémentaire**.

   b. Une fenêtre s'ouvre. Dans cette fenêtre, sélectionnez un compte utilisateur.

   c. Double-cliquez pour ouvrir les propriétés du compte utilisateur.

   d. Une fenêtre s'ouvrira, dans cette fenêtre, cliquez sur le lien **Afficher les autorisations supplémentaires**.

   e. Une fenêtre s'ouvrira, dans cette fenêtre, configurez les autorisations spéciales pour l'utilisateur.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer les autorisations des utilisateurs pour gérer le Kaspersky Embedded Systems Security Service dans la Console de l'application ?

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Autorisations d'accès utilisateur pour l'administration du Service KESS** dans le menu contextuel du nœud.

2. Dans la fenêtre qui s'ouvre, dans le groupe **Autorisations**, cliquez sur le bouton **Ajouter**.

   Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

3. Ajoutez un utilisateur ou un groupe Active Directory pour lequel vous souhaitez configurer les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.

4. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

5. Configurez dans la liste des autorisations les autorisations des utilisateurs pour gérer le Kaspersky Embedded Systems Security Service.

6. Si nécessaire, configurez des autorisations spéciales pour les utilisateurs :

   a. Cliquez sur **Supplémentaire**.

   b. Une fenêtre s'ouvre. Dans cette fenêtre, sélectionnez un compte utilisateur.

   c. Double-cliquez pour ouvrir les propriétés du compte utilisateur.

d. Une fenêtre s'ouvrira, dans cette fenêtre, cliquez sur le lien **Afficher les autorisations supplémentaires**.

e. Une fenêtre s'ouvrira, dans cette fenêtre, configurez les autorisations spéciales pour l'utilisateur.

7. Enregistrez vos modifications.

Comment configurer les autorisations des utilisateurs pour gérer le Kaspersky Embedded Systems Security Service dans la Web Console de Kaspersky Security Center ?

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Complémentaire** → **Autorisations d'accès utilisateur pour l'administration du Service KESS** et cliquez sur le bouton **Configurer**.

   La fenêtre **Autorisations d'accès utilisateur pour l'administration du Service KESS** s'ouvre.
5. Ajoutez un utilisateur ou un groupe Active Directory pour lequel vous souhaitez configurer les autorisations des utilisateurs du Kaspersky Embedded Systems Security Service.
6. Sélectionnez un utilisateur ou un groupe d'utilisateurs à qui vous souhaitez accorder l'accès à la gestion de l'application.

   Vous ne pouvez pas configurer de autorisations spéciales pour administrer le service de l'application dans Web Console.
7. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Accès protégé par mot de passe aux fonctionnalités de Kaspersky Embedded Systems Security

La configuration des droits des utilisateurs permet de restreindre l'accès à l'[administration de l'application et aux services enregistrés à l'aide de la configuration des autorisations des utilisateurs]. Vous pouvez renforcer la protection des opérations critiques grâce à l'activation de la protection par mot de passe dans les paramètres de Kaspersky Embedded Systems Security.

Lorsqu'un utilisateur tente d'exécuter une action protégée par mot de passe, Kaspersky Embedded Systems Security l'invite à saisir le nom d'utilisateur et le mot de passe ou à utiliser un jeton pour l'authentification.

Nom d'utilisateur et mot de passe

La Protection par mot de passe fonctionne avec les comptes utilisateur suivants :

- **KLAdmin**. Un compte Administrateur avec accès illimité à Kaspersky Embedded Systems Security. Le compte utilisateur KLAdmin peut réaliser n'importe quelle action protégée par un mot de passe. Il est impossible de retirer l'autorisation pour le compte utilisateur KLAdmin. Kaspersky Embedded Systems Security exige la définition du mot de passe du compte utilisateur KLAdmin lors de l'activation de la Protection par mot de passe.

- **Compte ajouté manuellement**. Un compte en dehors du domaine Active Directory. Vous pouvez utiliser ce compte de service au lieu du compte KLAdmin si vous ne souhaitez pas partager le mot de passe de l'administrateur. Vous pouvez définir n'importe quel nom d'utilisateur et mot de passe et configurer des autorisations individuelles.

- **Groupe "Tous"**. Groupe standard de Windows qui reprend tous les utilisateurs du réseau de l'entreprise. Les utilisateurs du groupe "Tous" peuvent accéder à l'application avec certaines restrictions.

- **Utilisateurs ou groupes distincts**. Comptes utilisateurs pour lesquels vous pouvez configurer des autorisations particulières. Par exemple, si une action est interdite pour le groupe "Tous", vous pouvez l'autoriser pour un utilisateur ou un groupe en particulier.

L'interface de Kaspersky Embedded Systems Security masque le mot de passe désigné à l'écran. Kaspersky Embedded Systems Security conserve le mot de passe spécifié sous la forme d'une somme de contrôle calculée à la saisie du mot de passe.

Kaspersky Embedded Systems Security ne vérifie pas la sécurité du mot de passe et ne bloque pas la saisie du mot de passe après plusieurs tentatives infructueuses.

Lors de la création d'un mot de passe, il est recommandé de respecter les conditions suivantes :

- Le mot de passe ne contient pas le nom du compte ou le nom de l'ordinateur.
- Le mot de passe comporte au moins 8 caractères.
- Le mot de passe contient des caractères appartenant à au moins trois des catégories suivantes :
  - Lettres latines majuscules (A à Z)
  - Lettres latines minuscules (a à z)
  - Chiffres (0-9)
  - Point d'exclamation (!), signe dollar ($), signe dièse (#) et signe de pourcentage (%)

Jeton

Pour accéder aux fonctionnalités de Kaspersky Embedded Systems Security, vous devez sélectionner le certificat utilisateur approprié dans la liste des certificats stockés sur le jeton connecté et saisir votre code PIN. L'authentification par jeton est disponible uniquement pour les utilisateurs du domaine Active Directory. L'administrateur peut configurer les autorisations pour un utilisateur individuel ou un groupe. Pour que l'authentification par jeton fonctionne, vous devez déployer une infrastructure PKI de confiance et installer un logiciel dédié à la gestion du jeton.

Comment protéger par mot de passe l'accès aux fonctionnalités de Kaspersky Embedded Systems Security dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Complémentaire**.
4. Dans la section **Autorisations d'accès des utilisateurs pour la gestion des applications**, cliquez sur **Paramètres**.
5. Dans la fenêtre qui s'ouvre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement**.
6. Le cas échéant, décochez la case **Demander un mot de passe pour confirmer les actions critiques**.

   Si cette fonctionnalité est activée, l'application demande un nom d'utilisateur et un mot de passe lors de la suppression, de la modification ou de la récupération de l'application et lors de l'exécution d'actions sur la ligne de commande susceptibles de réduire le niveau de protection de l'appareil.

   Si cette fonctionnalité est désactivée et que l'utilisateur actuel dispose des droits nécessaires, Kaspersky Embedded Systems Security ne demande pas d'informations d'identification. Cette option est activée par défaut.

   > Si un mot de passe Windows vide est défini pour l'utilisateur actuel, vous devez entrer les informations d'identification d'un utilisateur qui possède les droits nécessaires et dispose d'un mot de passe non vide.

7. Spécifiez le mot de passe du compte utilisateur KLAdmin.
8. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications :

   a. Cliquez sur **Ajouter**.

      Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

   b. Dans la fenêtre qui s'ouvre, sélectionnez la méthode pour ajouter des utilisateurs : **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**.

c. Indiquez le nom d'utilisateur et le mot de passe.

d. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment protéger par mot de passe l'accès aux fonctionnalités de Kaspersky Embedded Systems Security dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Autorisations d'accès des utilisateurs pour la gestion des applications** dans le menu contextuel du nœud.

2. Dans la fenêtre qui s'ouvre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement**.

3. Le cas échéant, décochez la case **Demander un mot de passe pour confirmer les actions critiques**.

   Si cette fonctionnalité est activée, l'application demande un nom d'utilisateur et un mot de passe lors de la suppression, de la modification ou de la récupération de l'application et lors de l'exécution d'actions sur la ligne de commande susceptibles de réduire le niveau de protection de l'appareil.

   Si cette fonctionnalité est désactivée et que l'utilisateur actuel dispose des droits nécessaires, Kaspersky Embedded Systems Security ne demande pas d'informations d'identification. Cette option est activée par défaut.

   > Si un mot de passe Windows vide est défini pour l'utilisateur actuel, vous devez entrer les informations d'identification d'un utilisateur qui possède les droits nécessaires et dispose d'un mot de passe non vide.

4. Spécifiez le mot de passe du compte utilisateur KLAdmin.

5. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications :

   a. Cliquez sur **Ajouter**.

      Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

   b. Dans la fenêtre qui s'ouvre, sélectionnez la méthode pour ajouter des utilisateurs : **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**.

   c. Indiquez le nom d'utilisateur et le mot de passe.

   d. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

6. Enregistrez vos modifications.

Comment protéger par mot de passe l'accès aux fonctionnalités de Kaspersky Embedded Systems Security dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Complémentaire → Autorisations d'accès des utilisateurs pour la gestion des applications** et cliquez sur le bouton **Configurer**.

5. Dans la fenêtre qui s'ouvre, cochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement**.

6. Le cas échéant, décochez la case **Demander un mot de passe pour confirmer les actions critiques**.

   Si cette fonctionnalité est activée, l'application demande un nom d'utilisateur et un mot de passe lors de la suppression, de la modification ou de la récupération de l'application et lors de l'exécution d'actions sur la ligne de commande susceptibles de réduire le niveau de protection de l'appareil.

   Si cette fonctionnalité est désactivée et que l'utilisateur actuel dispose des droits nécessaires, Kaspersky Embedded Systems Security ne demande pas d'informations d'identification. Cette option est activée par défaut.

   > Si un mot de passe Windows vide est défini pour l'utilisateur actuel, vous devez entrer les informations d'identification d'un utilisateur qui possède les droits nécessaires et dispose d'un mot de passe non vide.

7. Spécifiez le mot de passe du compte utilisateur KLAdmin.

8. Si nécessaire, ajoutez des comptes utilisateurs auxquels vous souhaitez autoriser l'accès à la gestion des applications :

   a. Cliquez sur **Ajouter**.

      Le formulaire pour la configuration des autorisations d'accès des utilisateurs s'ouvre.

   b. Dans la fenêtre qui s'ouvre, sélectionnez la méthode pour ajouter des utilisateurs : **Ajouter un utilisateur/un groupe d'utilisateurs manuellement**.

   c. Indiquez le nom d'utilisateur et le mot de passe.

   d. Dans la liste **Autorisations**, configurez les autorisations d'accès des utilisateurs aux fonctionnalités de l'application.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

> Il est impossible de récupérer le mot de passe défini. Si vous oubliez votre mot de passe, vous ne pouvez plus contrôler l'application. En outre, vous ne pourrez pas supprimer l'application de l'appareil protégé.

Il est possible de réinitialiser le mot de passe à tout moment. Pour ce faire, décochez la case **Autoriser la confirmation d'actions avec l'application en utilisant les identifiants d'utilisateurs créés manuellement** et enregistrez les modifications. La protection par mot de passe est désactivée et la somme de contrôle de l'ancien mot de passe est supprimée. Répétez le processus de création du mot de passe avec un nouveau mot de passe.

Notifications du Bureau sécurisé

Kaspersky Embedded Systems Security prend en charge la fonctionnalité (Secure Desktop). Le but de cette fonctionnalité est de confirmer les actions susceptibles de réduire le niveau de sécurité de l'ordinateur. Cette fonctionnalité permet à une application d'afficher une boîte de dialogue de confirmation isolée des autres processus. Cette fonctionnalité utilise des droits élevés pour sécuriser la demande. De cette façon, seul l'utilisateur peut confirmer l'action et non le programme malveillant.

Kaspersky Embedded Systems Security affiche les notifications de la fonctionnalité Bureau sécurisé pour confirmer les actions suivantes :

- Traçage activé ou désactivé
- Paramètres de l'application exportés ou importés
- Protection interrompue
- Application fermée
- Clé active supprimée
- Kaspersky Embedded Systems Security est désinstallé
- Contrôle des appareils désactivé
- La Protection des fichiers en temps réel est désactivée
- Stratégie Kaspersky Security Center désactivée
- Rapports consultés
- Fichiers restaurés à partir d'une sauvegarde
- Paramètres de Kaspersky Embedded Systems Security modifiés
- Tâches d'application gérées autrement que par le démarrage

Comment activer ou désactiver les notifications du Bureau sécurisé dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Paramètres de l'application**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Sécurité et fiabilité**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Sécurité**.

6. Dans le groupe **Autodéfense**, cochez ou décochez la case **Activer les notifications de la fonctionnalité Bureau sécurisé** pour activer ou désactiver les notification du Bureau sécurisé.

   Si les mécanismes d'autodéfense sont désactivés, la case **Activer les notifications de la fonctionnalité Bureau sécurisé** n'est pas disponible.

7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver les notifications du Bureau sécurisé dans la Console d'administration

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et, dans le panneau des résultats, suivez le lien **Propriétés de l'application**.

2. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres de sécurité**.

3. Dans le groupe **Autodéfense**, cochez ou décochez la case **Activer les notifications de la fonctionnalité Bureau sécurisé** pour activer ou désactiver les notification du Bureau sécurisé.

   Si les mécanismes d'autodéfense sont désactivés, la case **Activer les notifications de la fonctionnalité Bureau sécurisé** n'est pas disponible.

4. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer ou désactiver les notifications du Bureau sécurisé dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Paramètres de l'application**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Sécurité et fiabilité**.

   La fenêtre **Sécurité et fiabilité** s'ouvre.

6. Dans le groupe **Autodéfense**, cochez ou décochez la case **Activer les notifications de la fonctionnalité Bureau sécurisé** pour activer ou désactiver les notification du Bureau sécurisé.

   Si les mécanismes d'autodéfense sont désactivés, la case **Activer les notifications de la fonctionnalité Bureau sécurisé** n'est pas disponible.

7. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Exclusions de l'analyse pour l'application

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Embedded Systems Security ne contrôle pas.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Embedded Systems Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger. Un administrateur peut également autoriser un utilisateur à créer sa propre zone de confiance locale pour un ordinateur particulier. De cette façon, les utilisateurs peuvent créer leurs propres listes locales d'exclusions et d'applications de confiance en plus de la zone de confiance générale proposée par une stratégie.

Les exclusions de l'analyse et les applications de confiance prédéfinies ont été ajoutées à la zone de confiance. Les exclusions d'analyse et les applications de confiance prédéfinies permettent de configurer rapidement Kaspersky Embedded Systems Security sans créer manuellement de zone de confiance.

Définition de l'exclusion de l'analyse

L'exclusion de l'analyse est un ensemble de conditions sous lesquelles Kaspersky Embedded Systems Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Les exclusions d'analyse peuvent être utilisées par les modules d'application et les tâches suivants :

- **Protection des fichiers en temps réel**
- **Analyse à la demande**
- **Détection comportementale**
- **Scanner AMSI**
- **Protection contre les menaces réseau**

Kaspersky Embedded Systems Security n'analyse pas l'objet si au lancement d'une des tâches d'analyse le disque dur ou le dossier d'emplacement de cet objet figure dans la zone d'analyse. Cependant, lors du lancement de la tâche d'analyse personnalisée, l'exclusion de l'analyse n'est pas appliquée à cet objet.

Kaspersky Embedded Systems Security ne prend pas en charge les listes d'exclusions contenant plus de 5 000 objets.

Comment créer une exclusion d'analyse dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Complémentaire → Zone de confiance** et cliquez sur **Paramètres**.

4. Sélectionnez l'onglet **Exclusions de l'analyse**.

5. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.

6. Cochez la case **Autoriser l'utilisation des exclusions locales** si vous souhaitez permettre à l'utilisateur de créer une liste locale d'exclusions. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

   Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. De plus, si la case est décochée, Kaspersky Embedded Systems Security masque la liste consolidée des exclusions d'analyse dans la Console de l'application.

7. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle exclusion d'analyse à une catégorie en particulier, sélectionnez une catégorie.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des exclusions à partir de la liste des exclusions d'analyse prédéfinies.

8. Pour exclure un fichier ou un dossier de l'analyse, cochez la case **Fichier ou dossier**. Cliquez sur le lien **sélectionner un fichier ou un dossier** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez un fichier ou un dossier en cliquant sur **Parcourir**.

   Vous pouvez également saisir le chemin manuellement. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

   - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

   - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

  Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

9. Pour exclure une zone prédéfinie de l'analyse, cochez la case **Zone prédéfinie**. Cliquez sur le lien **sélectionner une zone prédéfinie** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez l'une des zones standards sur l'appareil protégé.

10. Pour exclure certains objets de l'analyse, cochez la case **Type d'un objet détecté**. Cliquez sur le lien **saisir des noms d'objets**, cliquez sur le bouton **Ajouter**, puis dans la fenêtre qui s'ouvre, saisissez le nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, Kaspersky Embedded Systems Security exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.

11. Pour exclure un fichier en particulier de l'analyse, cochez la case **Hachage de l'objet**. Cliquez sur le lien **saisir le hachage de l'objet** pour ouvrir une fenêtre, puis dans cette fenêtre, saisissez un hachage de fichier.

    Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

12. Dans le groupe **Zone d'application de la règle**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

13. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

14. Enregistrez les modifications pour ajouter l'exclusion à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case à côté de l'objet.

Comment créer une exclusion d'analyse dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Complémentaire** → **Zone de confiance** et cliquez sur le bouton **Configurer**.

5. Sélectionnez l'onglet **Exclusions de l'analyse**.

6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'exclusions pour tous les ordinateurs de l'organisation. Les listes d'exclusions des stratégies parents et enfants sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les exclusions de la stratégie parente apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'exclusions de la stratégie parente n'est pas possible.

7. Cochez la case **Autoriser l'utilisation des exclusions locales** si vous souhaitez permettre à l'utilisateur de créer une liste locale d'exclusions. De cette façon, un utilisateur peut créer sa propre liste locale des exclusions en plus de la liste générale des exclusions créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

   Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des exclusions créée dans le cadre de la stratégie. De plus, si la case est décochée, Kaspersky Embedded Systems Security masque la liste consolidée des exclusions d'analyse dans la Console de l'application.

8. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des exclusions à partir de la liste des exclusions d'analyse prédéfinies.

9. Si vous souhaitez exclure un fichier ou un dossier de l'analyse, sélectionnez **Fichier ou dossier** et cochez la case dans le champ du même nom. Indiquez le chemin d'accès au fichier ou au dossier.

   Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

   - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

   - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

   - Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

     Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

10. Pour exclure une zone prédéfinie de l'analyse, sélectionnez **Zone prédéfinie**. Dans la liste déroulante, sélectionnez l'une des zones standards sur l'appareil protégé.

11. Si vous souhaitez exclure certains objets de l'analyse, cochez la case **Type d'un objet détecté** et saisissez le nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, Kaspersky Embedded Systems Security exclut les objets *Client-IRC*, *Client-P2P* et *Client-SMTP* des analyses.

12. Pour exclure un fichier en particulier de l'analyse, cochez la case **Hachage de l'objet** et ajoutez un hachage à partir d'un fichier ou d'une liste d'événements.

    Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

13. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

14. Dans le groupe **Modules de la protection**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

15. La nouvelle exclusion sera ajoutée à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case dans la colonne **État**.

16. Enregistrez vos modifications.

Création d'une exclusion d'analyse dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Dans la section **Exclusions**, cliquez sur le bouton **Paramètres** à côté du groupe **Exclusions de l'analyse**.

3. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle exclusion d'analyse à une catégorie en particulier, sélectionnez une catégorie.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des exclusions à partir de la liste des exclusions d'analyse prédéfinies.

4. Pour exclure un fichier ou un dossier de l'analyse, cochez la case **Fichier ou dossier**. Cliquez sur le lien **Sélectionnez un fichier ou un dossier** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez un fichier ou un dossier en cliquant sur **Parcourir**.

Vous pouvez également saisir le chemin manuellement. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

  Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

5. Pour exclure une zone prédéfinie de l'analyse, cochez la case **Zone prédéfinie**. Cliquez sur le lien **sélectionner une zone prédéfinie** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez l'une des zones standards sur l'appareil protégé.

6. Pour exclure certains objets de l'analyse, cochez la case **Type d'un objet détecté**. Cliquez sur le lien **saisir des noms d'objets**, cliquez sur le bouton **Ajouter**, puis dans la fenêtre qui s'ouvre, saisissez le nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, Kaspersky Embedded Systems Security exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.

7. Pour exclure un fichier en particulier de l'analyse, cochez la case **Hachage de l'objet**. Cliquez sur le lien **saisir le hachage de l'objet** pour ouvrir une fenêtre, puis dans cette fenêtre, saisissez un hachage de fichier.

   Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

8. Dans le groupe **Zone d'application de la règle**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

9. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

10. Enregistrez les modifications pour ajouter l'exclusion à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case à côté de l'objet.

Exemples de masque de chemin d'accès :
Chemins d'accès à des fichiers situés dans n'importe quel dossier :

- Le masque `*.exe` reprend tous les chemins d'accès aux fichiers portant l'extension exe.
- Le masque `example*` reprend tous les chemins d'accès aux fichiers dont le nom est EXAMPLE.

Chemins d'accès à des fichiers situés dans le dossier indiqué :

- Le masque `C:\dir\*.*` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir\*` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, y compris les sous-dossiers.
- Le masque `C:\dir\` reprend tous les chemins d'accès aux fichiers du dossier C:\dir\, y compris les sous-dossiers.
- Le masque `C:\dir\*.exe` inclut tous les chemins d'accès aux fichiers portant l'extension .EXE situés dans le dossier C:\dir\, mais pas dans les sous-dossiers de C:\dir\.
- Le masque `C:\dir\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\, mais pas dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir\*\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans le dossier C:\dir\ et dans les sous-dossiers du dossier C:\dir\.
- Le masque `C:\dir1\*\dir3\` inclura tous les chemins d'accès aux fichiers des sous-dossiers dir3 d'un niveau dans le dossier C:\dir1\.
- Le masque `C:\dir1\**\dirN\` inclura tous les chemins d'accès aux fichiers dans les sous-dossiers dirN du dossier C:\dir1\ à n'importe quel niveau.

Chemin d'accès aux fichiers situés dans tous les dossiers portant le nom indiqué :

- Le masque `dir\*.*` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir\*` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir\` reprend tous les chemins d'accès aux fichiers dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.
- Le masque `dir\*.exe` inclut tous les chemins d'accès aux fichiers portant l'extension .EXE situés dans les dossiers nommés "dir", mais pas dans les sous-dossiers de ces dossiers.
- Le masque `dir\test` reprend tous les chemins d'accès aux fichiers portant le nom test dans les dossiers portant le nom dir, mais pas dans leurs sous-dossiers.

Sélection des types d'objets à détecter

Pour sélectionner les types d'objets à identifier, procédez comme suit :

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et réalisez l'une des actions suivantes :
   - Dans le panneau des résultats du nœud, cliquez sur le lien **Configurer les paramètres de la zone de confiance**.
   - Dans le menu contextuel du nœud, sélectionnez **Zone de confiance**.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.
2. Dans la section **Types d'objets détectés**, cliquez sur **Paramètres**.

3. Dans la fenêtre qui s'ouvre, cochez les cases pour les types d'objets que Kaspersky Embedded Systems Security doit détecter :

- **Virus et vers**

  Sous-catégorie : virus et vers (Viruses_and_Worms)

  Niveau de danger : élevé

  Les virus et les vers classiques exécutent sur l'ordinateur des actions qui n'ont pas été autorisées par l'utilisateur. Ils peuvent créer leurs propres copies qui possèdent la capacité d'auto-reproduction.

  Virus classique

  Une fois que le virus classique s'est introduit dans un système, il infecte un fichier quelconque, s'y active, exécute son action malveillante, puis ajoute sa copie à d'autres fichiers.

  Le virus classique se multiplie uniquement sur les ressources locales de l'ordinateur et il est incapable de s'introduire lui-même dans un autre ordinateur. Il peut pénétrer dans d'autres systèmes uniquement s'il ajoute sa copie dans un fichier enregistré dans un dossier partagé, sur un cédérom d'installation ou si l'utilisateur envoie un email avec le fichier infecté en pièce jointe.

  Le code du virus classique peut s'introduire dans divers secteurs de l'ordinateur, du système d'exploitation ou de l'application. En fonction de l'environnement dans lequel ils évoluent, on parle de *virus de fichiers*, *virus de démarrage*, *virus de script* et *virus de macro*.

  Les virus peuvent infecter des fichiers de diverses manières. Les virus *écraseurs* (overwriting) remplacent le code du fichier infecté par leur propre code et suppriment ainsi le contenu du fichier. Le fichier infecté cesse de fonctionner et il ne peut être restauré. Les virus *parasites* (Parasitic) modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les *virus compagnons* (Companion) ne modifient pas les fichiers mais créent des copies. Lorsque le fichier infecté est exécuté, son double est lancé, à savoir le virus. Il existe également des *virus-liens* (Link), des virus *qui infectent les modules objets* (OBJ), des virus *qui infectent les bibliothèques de compilateur* (LIB), les virus *qui infectent les textes source des programmes* et d'autres.

  Ver

  Le code du ver, à l'instar de celui du virus classique, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Le ver doit son nom à sa capacité à "ramper" d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

  La principale caractéristique qui distingue les vers entre eux est leur mode de diffusion. Le tableau suivant reprend une description des différents types de vers en fonction du mode de diffusion.

  Mode de diffusion des vers

Type	Name	Description
Email-Worm	Email-Worm	Ils se diffusent via email. L'email infecté contient un fichier joint avec la copie du ver ou un lien vers ce fichier sur un site compromis ou créé spécialement à cette fin. Lorsque vous ouvrez le fichier joint, le ver est activé. Lorsque vous cliquez sur le lien, téléchargez le fichier, puis ouvrez celui-ci, le ver commence également à exécuter ses actions malveillantes. Ensuite, il continue à diffuser ses copies après avoir trouvé d'autres adresses email auxquelles il envoie des messages infectés.
IM-Worm	Vers de client IM	Ils se propagent via les clients IM. En règle générale, ce ver envoie aux contacts un message contenant un lien vers la copie du ver sur un site. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.

Type	Name	Description
IRC-Worm	Vers de chats	Ils se diffusent via les canaux IRC (Internet Relay Chats), ces systèmes qui permettent de discuter en temps réel avec d'autres personnes. Ce ver publie un fichier avec sa copie ou un lien vers celle-ci dans le chat. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.
Net-Worm	Vers de réseau (vers de réseaux informatiques)	Ils se diffusent via les réseaux informatiques. À la différence des autres types de vers, le ver de réseau se propage sans l'intervention de l'utilisateur. Il recherche une application vulnérable sur les ordinateurs du réseau local. Pour ce faire, il envoie un paquet réseau spécial (un exploit) qui contient le code du ver ou une partie de celui-ci. Si le réseau abrite un ordinateur "vulnérable", celui-ci acceptera le paquet. Une fois qu'il s'est complètement introduit dans cet ordinateur, le ver s'active.
P2P-Worm	Vers de réseau d'échange de fichiers	Ils se propagent via les réseaux d'échange de fichiers pair à pair. Afin d'infiltrer le réseau d'échange de fichiers, le ver se copie dans le dossier d'échange de fichiers qui se trouve normalement sur l'ordinateur de l'utilisateur. Le réseau d'échange de fichiers affiche les informations relatives à ce fichier et l'utilisateur peut "trouver" le fichier infecté comme n'importe quel autre fichier, le télécharger puis l'ouvrir. Les vers plus sophistiqués imitent le protocole d'un réseau d'échange de fichiers en particulier : ils répondent positivement aux recherches et proposent leur copie pour le téléchargement.
Ver	Autres vers	Parmi ces autres vers, citons : • Les vers qui diffusent leur copie via les ressources réseau. À l'aide des fonctions du système d'exploitation, ils consultent les répertoires réseau accessibles, se connectent aux ordinateurs du réseau mondial et tentent d'ouvrir leur disque en libre accès. À la différence des types de vers décrits ci-dessus, ces autres vers ne peuvent pas s'activer de manière autonome, mais uniquement lorsque l'utilisateur ouvre le fichier contenant la copie du ver. • Les vers qui n'adoptent aucun des modes de diffusion décrits dans ce tableau (par exemple, ceux qui se propagent via les téléphones portables).

- **Chevaux de Troie**

  Sous-catégories : chevaux de Troie (Trojan_programs)

  Niveau de danger : élevé

  À la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie. Ils s'infiltrent sur les ordinateurs via email ou via le navigateur lorsque l'internaute visite un site infecté. Les chevaux de Troie sont exécutés sur intervention de l'utilisateur. Ils entament leur action malveillante directement après l'exécution.

  Le comportement des chevaux de Troie sur l'ordinateur infecté varie. Parmi les fonctions principales des chevaux de Troie, citons le blocage, la modification ou la suppression d'informations ainsi que la perturbation du fonctionnement des ordinateurs ou des réseaux. De plus, les chevaux de Troie peuvent recevoir ou envoyer des fichiers, les exécuter, afficher des messages, contacter des pages Internet, télécharger des applications et les installer et redémarrer l'ordinateur.

  Les individus malintentionnés utilisent souvent des "sélections" composées de divers chevaux de Troie.

  Les types de comportement des chevaux de Troie sont décrits dans le tableau suivant.

  Types de comportement des chevaux de Troie sur l'ordinateur infecté

Type	Name	Description
Trojan-ArcBomb	Chevaux de Troie (bombes dans les archives)	Il s'agit d'archives qui, au moment de la décompression, atteignent un tel poids qu'elles perturbent le fonctionnement de l'ordinateur. Lorsque l'utilisateur tente de décompresser une archive de ce genre, l'ordinateur peut commencer à ralentir, voire à s'arrêter et le disque peut se remplir de données "vides". Ces "bombes" sont particulièrement dangereuses pour les serveurs de fichiers et de messagerie. Si le serveur utilise un système de traitement automatique des données entrantes, ce genre de "bombe d'archive" peut entraîner l'arrêt du serveur.
Backdoor	Chevaux de Troie pour l'administration à distance	Considérés comme les chevaux de Troie les plus dangereux. Leurs fonctions rappellent celles des programmes d'administration à distance installés sur les ordinateurs. Ces programmes s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu malintentionné d'administrer l'ordinateur à distance.
Trojan	Chevaux de Troie	Cette catégorie reprend les programmes malveillants suivants : • **Chevaux de Troie traditionnels**. Ils exécutent uniquement les fonctions fondamentales des chevaux de Troie : le blocage, la modification ou la suppression d'informations, la perturbation du fonctionnement des ordinateurs ou des réseaux. Ils ne possèdent pas les fonctions complémentaires caractéristiques d'autres chevaux de Troie décrits dans ce tableau. • **Chevaux de Troie "multicibles"**. Ils possèdent des fonctions complémentaires appartenant à divers types de chevaux de Troie.
Trojan-Ransom	Chevaux de Troie exigeant le versement d'une rançon	Ces programmes "prennent en otage" les données de l'ordinateur après les avoir modifiées ou bloquées ou perturbent le fonctionnement de l'ordinateur de telle manière que l'utilisateur n'est plus en mesure d'exploiter les données. L'individu malintentionné exige le versement d'une somme d'argent en échange de l'envoi d'un programme qui rétablira le fonctionnement de l'ordinateur et les données qu'il abrite.
Trojan-Clicker	Chevaux de Troie qui cliquent	Ils accèdent à des pages Internet depuis l'ordinateur de la victime : ils envoient des instructions au navigateur ou remplacent les adresses Internet conservées dans les fichiers système. Grâce à ces programmes malveillants, les individus malintentionnés organisent des attaques réseau ou augmentent le nombre de visites sur le site afin d'accroître le nombre d'affichages de bannières publicitaires.
Trojan-Downloader	Chevaux de Troie qui téléchargent	Ils accèdent à la page Internet de l'intrus, y téléchargent d'autres applications malveillantes et les installent sur l'ordinateur de l'utilisateur. Ils peuvent contenir le nom du fichier de l'application malveillante à télécharger ou le recevoir à partir de la page Internet consultée.
Trojan-Dropper	Chevaux de Troie qui procèdent à des installations	Ils enregistrent sur le disque, puis installent d'autres chevaux de Troie présents dans le corps de ces programmes. Les individus malintentionnés peuvent utiliser ce genre de chevaux de Troie pour : • Installer un programme malveillant à l'insu de l'utilisateur : ces chevaux de Troie n'affichent aucun message réel ou fictif (par exemple, messages relatifs à une erreur dans une archive ou à la version incorrecte du système d'exploitation) ; • Protéger un autre programme malveillant connu : tous les antivirus ne sont pas en mesure d'identifier un programme malveillant au sein d'un cheval de Troie qui réalise des installations.
Trojan-Notifier	Chevaux de Troie qui envoient des notifications	Ils signalent à l'individu malintentionné que la communication avec l'ordinateur infecté est établie et transmettent des informations relatives à l'ordinateur : adresse IP, numéro du port ouvert ou adresse email. Ils contactent l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens. Ces programmes sont souvent utilisés dans les sélections de différents chevaux de Troie. Ils indiquent à l'individu malintentionné que les autres chevaux de Troie ont bien été installés sur l'ordinateur de l'utilisateur.
Trojan-Proxy	Chevaux de Troie faisant office de proxy	Ils permettent à l'individu malintentionné de contacter anonymement des pages Internet via l'ordinateur de la victime ; le plus souvent, ils sont utilisés pour diffuser du spam.
Trojan-PSW	Chevaux de Troie qui volent des mots de passe	Il s'agit de chevaux de Troie qui volent des mots de passe (Password Stealing Ware) ; ils volent les données des comptes des utilisateurs, les données d'enregistrement d'un logiciel. Ils recherchent les données confidentielles dans les fichiers système et dans la base de registre et les transmettent à leur « attaquant » via email ou via FTP sur la page Internet de l'individu malintentionné ou par d'autres méthodes. Certains de ces programmes appartiennent à des groupes particuliers décrits dans ce tableau. Il s'agit des chevaux de Troie qui volent les comptes bancaires (Trojan-Banker), des chevaux de Troie qui volent les données des utilisateurs des clients IM (Trojan-IM) et des chevaux de Troie qui volent les données des adeptes de jeux en ligne (Trojan-GameThief).

Type	Name	Description
Trojan-Spy	Chevaux de Troie espions	Ils espionnent l'utilisateur et collectent des informations sur les actions qu'il effectue lorsqu'il travaille sur son ordinateur. Ils peuvent intercepter les données que l'utilisateur saisit au clavier, faire des captures d'écran ou collecter des listes d'applications actives. Une fois qu'ils ont obtenu ces informations, ils les transmettent à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Trojan-DDoS	Chevaux de Troie pour attaques réseau	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). Ces programmes infectent généralement plusieurs ordinateurs pour attaquer simultanément un serveur. Les programmes de type DoS lancent l'attaque depuis un ordinateur avec l'accord de l'utilisateur. Les programmes de type DDoS (Distributed DoS) lancent des attaques distribuées depuis plusieurs ordinateurs, à l'insu de l'utilisateur de l'ordinateur infecté.
Trojan-IM	Chevaux de Troie qui volent les données des utilisateurs de clients IM	Ils volent les numéros et les mots de passe des utilisateurs des clients IM. Ils transmettent ces informations à l'individu malintentionné par email ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Rootkit	Rootkits	Ils masquent d'autres applications malveillantes et leur activité, et prolongent ainsi la persistance de ces applications dans le système d'exploitation. Ils peuvent également dissimuler des fichiers, des processus dans la mémoire d'un ordinateur infecté ou des clés de registre qui exécutent des applications malveillantes. Les rootkits peuvent masquer l'échange de données entre les applications sur l'ordinateur de l'utilisateur et les autres ordinateurs du réseau.
Trojan-SMS	Chevaux de Troie qui envoient des messages SMS	Ils infectent des téléphones mobiles et les utilisent pour envoyer des messages SMS vers des numéros payants.
Trojan-GameThief	Chevaux de Troie qui volent les données des adeptes de jeux en ligne	Ils volent les comptes des adeptes de jeux en ligne ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens.
Trojan-Banker	Chevaux de Troie qui volent les données de comptes bancaires.	Ils volent les données des comptes bancaires ou les données des comptes de système de porte-monnaie électronique ; ils transmettent les données à l'individu malveillant par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens.
Trojan-Mailfinder	Chevaux de Troie qui récoltent des adresses email	Ils recueillent les adresses email sur l'ordinateur et les envoient à l'individu malintentionné par email, via FTP (sur le site de l'individu malintentionné) ou via d'autres moyens. Les individus malintentionnés utilisent ensuite ces adresses pour diffuser du spam.

- **Outils malveillants**

  Sous-catégories : outils malveillants (Malicious_tools)

  Niveau de danger : Moyen

  Contrairement aux autres types de logiciels malveillants, les outils malveillants n'exécutent pas leurs actions immédiatement après leur démarrage. Elles peuvent être stockées et lancées en toute sécurité sur l'ordinateur de l'utilisateur. Les individus malintentionnés utilisent les fonctions de ces programmes pour développer des virus, des vers et des chevaux de Troie, organiser des attaques réseau contre des serveurs distants, s'introduire dans des ordinateurs ou exécuter d'autres actions malveillantes.

  Les différentes fonctionnalités des outils malveillants sont regroupées en types présentés dans le tableau suivant.

  Fonctionnalités des outils malveillants

Type	Name	Description
Constructor	Constructeurs	Ils permettent de créer de nouveaux virus, vers ou chevaux de Troie. Certains constructeurs sont dotés d'une interface standard à base de fenêtres qui permet, à l'aide de menus, de sélectionner le type de programme malveillant à créer, son mode de résistance face aux débogueurs ainsi que d'autres propriétés.
Dos	Attaques réseau	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service).

Type	Name	Description
Exploit	Exploits	L'*exploit* est un ensemble de données ou de code qui exploite une vulnérabilité de l'application dans laquelle il est exécuté afin de réaliser une action malveillante quelconque sur l'ordinateur. Par exemple, un exploit peut écrire ou lire des fichiers ou contacter des pages Internet "infectées". Divers exploits exploitent les vulnérabilités de diverses applications et services réseau. L'exploit sous la forme d'un paquet réseau se transmet via le réseau vers de nombreux ordinateurs à la recherche d'ordinateurs possédant des services réseau vulnérables. L'exploit d'un fichier DOC utilise la vulnérabilité de l'éditeur de test. Il peut commencer à exécuter les fonctions intégrées par l'individu malintentionné lorsque l'utilisateur ouvre le fichier infecté. L'exploit intégré à un email recherche les vulnérabilités dans un client de messagerie quelconque. Il peut commencer à exécuter l'action malveillante dès que l'utilisateur ouvre le message infecté dans le client de messagerie. Les vers de réseau (Net-Worm) se diffusent grâce aux exploits. Les exploites de type Nuker sont des paquets réseau qui mettent l'ordinateur hors service.
FileCryptor	Encodeurs	Ils encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus.
Flooder	Programmes de "pollution" du réseau	Ils envoient une multitude de messages via les canaux réseau. Les programmes utilisés pour polluer les canaux IRC (Internet Relay Chats) appartiennent à cette catégorie. La catégorie Flooder ne reprend pas les applications qui "polluent" l'email, les clients IM et les systèmes mobiles. Ces programmes sont regroupés dans des catégories distinctes décrites dans ce tableau (Email-Flooder, IM-Flooder et SMS-Flooder).
HackTool	Outils de piratage	Ils permettent de s'emparer de l'ordinateur sur lequel ils sont installés ou d'attaquer un autre ordinateur (par exemple, ajout d'autres utilisateurs au système sans l'autorisation de la victime ; purge des journaux du système afin de dissimuler les traces de leur présence dans le système). Il s'agit de quelques sniffers qui possèdent des fonctions malveillantes telles que l'interception des mots de passe. Les sniffers sont des programmes qui permettent de consulter le trafic réseau.
Hoax	Canulars	Ils effraient l'utilisateur à l'aide de messages semblables à ceux que pourrait produire un virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu.
Spoofer	Utilitaires d'imitation	Ils envoient des messages et des requêtes réseau au départ d'adresses fictives. Les individus malintentionnés les utilisent pour se faire passer pour l'expéditeur.
VirTool	Instruments pour la modification des programmes malveillants	Ils permettent de modifier d'autres programmes malveillants afin de les rendre invisibles pour les logiciels antivirus.
Email-Flooder	Programmes qui "inondent" l'email.	Ils envoient de nombreux messages aux adresses email du carnet d'adresses ("pollution du courrier"). Ce flux important de messages empêche l'utilisateur de lire le courrier utile.
IM-Flooder	Programmes de "pollution" des clients IM	Ils envoient de nombreux messages aux utilisateurs de clients IM. Ce flux important de messages empêche l'utilisateur de lire les messages utiles.
SMS-Flooder	Programmes de "pollution" des messages SMS	Ils envoient de nombreux messages SMS vers les téléphones portables.

- **Logiciel publicitaire**

  Sous-catégorie : Logiciels publicitaires (Adware)

  Niveau de danger : Moyen

  Les logiciels publicitaires montrent des publicités à l'utilisateur. Elles affichent des bannières publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. Certains d'entre elles recueillent également des informations marketing sur l'utilisateur qu'elles renvoient à l'auteur : par exemple, catégorie de sites Internet visités, mots clés utilisés dans les recherches. À la différence des chevaux de Troie espions, elles transmettent ces informations avec l'autorisation de l'utilisateur.

- **Numéroteurs automatiques**

  Sous-catégorie : numéroteurs automatiques.

  Niveau de danger : Moyen

Les numéroteurs automatiques peuvent établir subrepticement des connexions téléphoniques à l'aide d'un modem.

- **Programme légitime qui peut être utilisé par des intrus pour nuire à votre ordinateur ou à vos données personnelles**

  Sous-catégorie : Programmes légitimes pouvant être exploités par un individu malintentionné afin de nuire à l'ordinateur ou à vos données.

  Niveau de danger : Moyen

  La majorité de ces applications est utile et bon nombre d'utilisateurs les emploient. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

  Toutefois, si les individus malintentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

  Ces programmes se distinguent par leurs fonctions dont les types sont décrits dans le tableau ci-dessous :

Type	Name	Description
Client-IRC	Clients de chats	Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus malintentionnés les utilisent pour diffuser des programmes malveillants.
Downloader	Programmes de téléchargement	Ils peuvent télécharger des fichiers depuis des pages Internet en mode caché.
Monitor	Programmes de surveillance	Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications exécutées et les échangent de données avec les applications sur d'autres ordinateurs).
PSWTool	Récupérateur de mots de passe	Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus malintentionnés les installent à l'insu des utilisateurs.
RemoteAdmin	Programmes d'administration à distance	Ils sont largement utilisés par les administrateurs de système. Ces programmes permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus malintentionnés les installent dans ce même but à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer. Les applications légitimes d'administration à distance se distinguent des backdoors. Les chevaux de Troie possèdent des fonctions qui leur permettent de s'introduire dans un système et de s'y installer. Les applications légitimes ne possèdent pas de telles fonctions.
Server-FTP	Serveurs FTP	Ils remplissent les fonctions d'un serveur FTP. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP.
Server-Proxy	Serveurs proxy	Ils remplissent les fonctions d'un serveur proxy. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.
Server-Telnet	Serveurs Telnet	Ils remplissent les fonctions d'un serveur Telnet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet.
Server-Web	Serveurs Internet	Ils remplissent les fonctions d'un serveur Internet. Les individus malintentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP.
RiskTool	Outils utilisés sur l'ordinateur local	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille sur son propre ordinateur. Ces outils permettent à l'utilisateur de masquer des fichiers ou des fenêtres d'applications actives et de mettre fin à des processus actifs.
NetTool	Outils réseau	Ils offrent à l'utilisateur des options supplémentaires lorsqu'il travaille avec d'autres ordinateurs sur le réseau. Ces outils permettent à l'utilisateur de les redémarrer, de détecter les ports ouverts et de lancer des applications installées sur les ordinateurs.
Client-P2P	Clients de réseaux d'échange de fichiers	Ils permettent d'utiliser les réseaux P2P. Les individus malintentionnés peuvent les utiliser pour diffuser des programmes malveillants.
Client-SMTP	Clients SMTP	Envoient les emails en mode caché. Les individus malintentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du spam en leur nom.

Type	Name	Description
WebToolbar	Barre d'outils Internet	Ils ajoutent une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche.
FraudTool	Pseudo-programmes	Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-programmes antivirus qui affichent des messages signalant la détection de logiciels malveillants. Or, en réalité, ils ne trouvent ni ne désinfectent rien.

- **Objets compactés pouvant dissimuler un programme malveillant**

  Sous-catégorie : fichiers compressés susceptibles de causer des dommages.

  Niveau de danger : Moyen.

  Le fichier est compressé à l'aide d'un outil de compression spécial utilisé pour contenir des programmes malveillants : virus, vers, chevaux de Troie. Kaspersky Embedded Systems Security analyse le module de décompression dans les archives autoextractibles SFX.

  Pour dissimuler les programmes malveillants afin qu'ils ne soient pas détectés par un antivirus, les pirates informatiques les compressent à l'aide d'empaqueteurs spéciaux. Les experts de Kaspersky ont identifié les outils de compression que les individus malintentionnés utilisent le plus souvent.

- **Objets compactés à plusieurs reprises**

  Sous-catégorie : fichiers compressés à plusieurs reprises.

  Niveau de danger : Moyen.

  Le fichier est emballé par un ou plusieurs empaqueteurs trois fois ou plus.

  Pour dissimuler un programme malveillant afin qu'il ne soit pas détecté par un antivirus, les pirates informatiques peuvent compresser un fichier plusieurs fois. Kaspersky Embedded Systems Security analyse les fichiers compressés.

4. Enregistrez vos modifications.

Composition de la liste des applications de confiance

La *Liste des applications de confiance* est une liste des applications pour lesquelles Kaspersky Embedded Systems Security ne contrôle pas l'activité de fichier et réseau (y compris l'activité malveillante), ni les requêtes qu'elles adressent à la base de registre. Par défaut Kaspersky Embedded Systems Security surveille les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Après l'ajout d'une application à la liste des applications de confiance, Kaspersky Embedded Systems Security cesse de surveiller l'activité de l'application.

La différence entre les exclusions d'analyse et les applications de confiance est que pour les exclusions, Kaspersky Embedded Systems Security n'analyse pas les fichiers, tandis que pour les applications de confiance, il ne contrôle pas les processus lancés. Si une application de confiance crée un fichier malveillant dans un dossier qui n'est pas inclus dans les exclusions d'analyse, Kaspersky Embedded Systems Security détectera le fichier et éliminera la menace. Si le dossier est ajouté aux exclusions, Kaspersky Embedded Systems Security ignorera ce fichier.

Par exemple, si vous estimez que les objets utilisés par l'application standard Bloc-notes de Microsoft Windows ne posent aucun danger (vous faites confiance à cette application), il faut ajouter l'application Bloc-notes de Microsoft Windows à la liste des applications de confiance afin que les objets utilisés par cette application ne soient pas surveillés. Cela augmentera les performances de l'ordinateur, ce qui est particulièrement important lors de l'utilisation d'applications serveur.

De plus, certaines actions que Kaspersky Embedded Systems Security considère comme suspectes peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Les applications de confiance permettent d'éviter les problèmes de compatibilité entre Kaspersky Embedded Systems Security et d'autres applications (par exemple, le problème de la double analyse du trafic réseau d'un ordinateur tiers par Kaspersky Embedded Systems Security et par une autre application antivirus).

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre programmes présentant une menace. Pour exclure entièrement l'application de l'analyse Kaspersky Embedded Systems Security, il est nécessaire d'utiliser les exclusions de l'analyse.

Kaspersky Embedded Systems Security ne prend pas en charge les listes d'applications de confiance contenant plus de 5 000 objets.

Comment ajouter une application à la liste de confiance dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Complémentaire**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Zone de confiance**.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications de confiance**.

   Une fenêtre reprenant la liste des applications de confiance s'ouvre.
6. Cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers** si vous souhaiter ignorer l'analyse des opérations de lecture des fichiers si ces opérations sont réalisées par des outils de copie de sauvegarde installés sur l'appareil protégé.
7. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'applications de confiance pour tous les ordinateurs de l'organisation. Les listes des applications de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les applications de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'applications de confiance de stratégie parent n'est pas possible

8. Cochez la case **Autoriser la modification des applications locales de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale d'applications de confiance en plus de la liste générale d'applications de confiance créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

   Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des applications de confiance créée dans le cadre de la stratégie. De plus, si la case est décochée, Kaspersky Embedded Systems Security masque la liste consolidée des applications de confiance dans la Console de l'application.

9. Cochez la case **Ne pas vérifier l'activité des fichiers des processus spécifiés** pour ignorer l'analyse des opérations sur les fichiers pour les processus de confiance.

10. Cliquez sur **Ajouter** et sélectionnez une action :

    - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.
    - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle application de confiance à la racine de la liste.
    - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle application de confiance à une catégorie en particulier, sélectionnez une catégorie.
    - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des applications à partir de la liste des applications de confiance prédéfinies.

11. Dans la fenêtre qui s'ouvre, cochez la case **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme fiable** et saisissez le chemin d'accès au fichier pour déterminer si le processus est fiable.

    Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

    > Kaspersky Embedded Systems Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'applications de confiance dans la console Kaspersky Security Center. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère * (par exemple, `C:\Users\*\Documents\File.exe`). Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

12. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).

13. Cliquez sur **OK**.

    La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case à côté de l'objet.

14. Enregistrez vos modifications.

Comment ajouter une application à la liste de confiance dans Kaspersky Security Center Web Console

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

4. Sélectionnez l'onglet **Paramètres de l'application**.

5. Rendez-vous dans **Complémentaire** → **Zone de confiance** et cliquez sur le bouton **Configurer**.

6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications de confiance**.

7. Cochez la case **Ne pas vérifier les opérations de sauvegarde de fichiers** si vous souhaiter ignorer l'analyse des opérations de lecture des fichiers si ces opérations sont réalisées par des outils de copie de sauvegarde installés sur l'appareil protégé.

8. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'applications de confiance pour tous les ordinateurs de l'organisation. Les listes des applications de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les applications de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultées. La modification ou la suppression d'applications de confiance de stratégie parent n'est pas possible

9. Cochez la case **Autoriser la modification des applications locales de confiance** si vous souhaitez autoriser l'utilisateur à créer une liste locale d'applications de confiance. De cette façon, un utilisateur peut créer sa propre liste locale d'applications de confiance en plus de la liste générale d'applications de confiance créée dans le cadre de la stratégie. Un administrateur peut utiliser Kaspersky Security Center pour afficher, ajouter, modifier ou supprimer des éléments de la liste dans les propriétés de l'ordinateur.

   Si la case est décochée, l'utilisateur ne peut accéder qu'à la liste générale des applications de confiance créée dans le cadre de la stratégie. De plus, si la case est décochée, Kaspersky Embedded Systems Security masque la liste consolidée des applications de confiance dans la Console de l'application.

10. Cochez la case **Ne pas vérifier l'activité des fichiers des processus spécifiés** pour ignorer l'analyse des opérations sur les fichiers pour les processus de confiance.

11. Cliquez sur **Ajouter** et sélectionnez une action :

    - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.

    - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle application de confiance à la racine de la liste.

    - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle application de confiance à une catégorie en particulier, sélectionnez une catégorie.

    - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des applications à partir de la liste des applications de confiance prédéfinies.

12. Dans la fenêtre qui s'ouvre, cochez la case **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme fiable** et saisissez le chemin d'accès au fichier pour déterminer si le processus est fiable.

    Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

Kaspersky Embedded Systems Security ne prend pas en charge la variable d'environnement `%userprofile%` lors de la génération d'une liste d'applications de confiance dans la console Kaspersky Security Center. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère * (par exemple, `C:\Users\*\Documents\File.exe`). Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

13. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).

14. Cliquez sur **OK**.

    La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case dans la colonne **Action**.

15. Enregistrez vos modifications.

Comment ajouter une application à la liste des applications de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Dans la section **Exclusions**, cliquez sur le bouton **Paramètres** à côté du groupe **Applications de confiance**.

3. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.
   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle application de confiance à la racine de la liste.
   - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle application de confiance à une catégorie en particulier, sélectionnez une catégorie.
   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des applications à partir de la liste des applications de confiance prédéfinies.

4. Sélectionnez un fichier dans la liste ou saisissez le chemin d'accès au fichier exécutable de l'application de confiance.

   Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

Kaspersky Embedded Systems Security prend en charge les variables d'environnement. Parallèlement, Kaspersky Embedded Systems Security convertit le chemin d'accès dans l'interface locale de l'application. Autrement dit, si vous saisissez le chemin d'accès au fichier `%userprofile%\Documents\File.exe`, une entrée `C:\Users\Fred123\Documents\File.exe` est ajoutéedans l'interface locale de l'application pour l'utilisateur Fred123. Par conséquent, Kaspersky Embedded Systems Security ignore le programme de confiance `File.exe` pour les autres utilisateurs. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère `*` (par exemple, `C:\Users\*\Documents\File.exe`).

Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

5. Configurez les paramètres avancés de l'application de confiance (cf. tableau ci-après).

6. Cliquez sur **OK**.

   La nouvelle application de confiance sera ajoutée à la liste. Vous pouvez exclure une application de la zone de confiance à tout moment en utilisant la case à côté du nom de l'objet.

7. Enregistrez vos modifications.

Paramètres des applications de confiance

Paramètre	Description
Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme de confiance	Kaspersky Embedded Systems Security détermine l'état de confiance du processus sur la base du chemin d'accès complet au dossier.
Utiliser le hachage du fichier du processus pour le considérer comme fiable	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 pour définir l'état de confiance du processus.
Utilisation des règles	Vous pouvez configurer une liste de modules de Kaspersky Embedded Systems Security qui ne surveilleront pas l'activité d'une application de confiance : • **Protection des fichiers en temps réel**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security exclut de l'analyse tous les fichiers ouverts à l'aide d'une application de confiance. Cette option est activée par défaut. • **Surveillance de l'accès au registre**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas les modifications apportées par une application de confiance aux clés de registre comprises dans la zone de surveillance du module Contrôle de l'intégrité du système. Par défaut, la fonctionnalité est désactivée. • **Détection comportementale et Protection contre les Exploits**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas l'activité des fichiers et l'activité réseau d'une application de confiance dans le système d'exploitation à l'aide des modules Détection comportementale et Protection contre les Exploits. Par défaut, la fonctionnalité est désactivée. • **Interaction avec le module Scanner AMSI**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas les requêtes adressées par une application de confiance au module Scanner AMSI. Par défaut, la fonctionnalité est désactivée. • **Contrôle de l'intégrité des fichiers**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas les modifications apportées par une application de confiance aux fichiers compris dans la zone de surveillance du module Contrôle de l'intégrité du système. Par défaut, la fonctionnalité est désactivée. • **Contrôle du lancement des applications**. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas le lancement d'une application de confiance par l'intermédiaire du module Contrôle du lancement des applications. Par défaut, la fonctionnalité est désactivée. Pour les applications de confiance prédéfinies, toutes les fonctionnalités sont activées par défaut, à l'exception de **Contrôle du lancement des applications**.
Autoriser l'interaction avec l'interface de l'application	Kaspersky Embedded Systems Security bloque toute tentative de gestion des services d'application à partir d'un ordinateur distant. Si la case est cochée, l'application d'accès à distance à l'ordinateur peut gérer les paramètres de Kaspersky Embedded Systems Security via l'interface de Kaspersky Embedded Systems Security.
Ne pas surveiller l'activité des applications enfants	Kaspersky Embedded Systems Security ne surveille pas l'activité des fichiers ni du réseau des applications qui sont lancées par cette application. Vous pouvez appliquer l'exclusion de manière récursive. Dans ce cas, l'application ne surveille pas l'activité de toute la chaîne d'applications enfants.
Ne pas hériter les restrictions du processus parent (application)	Les restrictions configurées pour le processus parent ne seront pas appliquées par Kaspersky Embedded Systems Security à un processus enfant. Le processus parent est lancé par une application pour laquelle des droits d'application et des règles réseau d'application sont configurés.
Ne pas analyser la mémoire du processus	Kaspersky Embedded Systems Security n'analyse pas la mémoire du processus.

Création d'une zone de confiance locale

L'utilisateur peut désormais créer sa propre zone de confiance locale pour un ordinateur spécifique. De cette façon, l'utilisateur peut créer ses propres listes locales d'exclusions d'analyse et d'applications de confiance en plus de la zone de confiance générale proposée par une stratégie. Un administrateur peut autoriser ou interdire l'utilisation d'exclusions locales ou d'applications locales de confiance dans les paramètres de stratégie. Pour ce faire, utilisez les cases **Autoriser l'utilisation des exclusions locales** et **Autoriser la modification des applications locales de confiance** sous les onglets **Exclusions de l'analyse** et **Applications de confiance** dans la section **Zone de confiance** de la stratégie.

Si la création d'une zone de confiance locale est autorisée par un administrateur, l'utilisateur peut ajouter ses propres exclusions d'analyse et applications de confiance dans la Console de l'application. Dans le même temps, l'utilisateur ne dispose pas des autorisations nécessaires pour modifier ou supprimer des objets de la zone de confiance configurée dans la stratégie. L'administrateur peut également afficher, ajouter, modifier ou supprimer des éléments de liste dans la console Kaspersky Security Center si des exclusions doivent être ajoutées pour un ordinateur individuel.

Kaspersky Embedded Systems Security masque les listes des exclusions d'analyse et des applications de confiance dans la Console de l'application si la configuration de la zone de confiance est bloquée par l'administrateur dans la console (symbole « cadenas fermé »), et si les exclusions d'analyse et les applications de confiance locales sont interdites.

Comment ajouter un objet à la zone de confiance locale dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Dans la fenêtre des propriétés de l'ordinateur, choisissez la section **Applications**.
5. Dans la liste des applications de Kaspersky installées sur l'ordinateur, choisissez **Kaspersky Embedded Systems Security**, puis ouvrez les propriétés de l'application d'un double-clic.
6. Dans la fenêtre des paramètres de l'application, sélectionnez **Complémentaire → Zone de confiance** et cliquez sur **Paramètres**.
7. Sous l'onglet **Exclusions de l'analyse**, dressez une liste des exclusions de l'analyse locale.

   Les règles de création d'exclusions d'analyse locale sont les mêmes que pour les exclusions générales. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

8. Sous l'onglet **Applications de confiance**, dressez une liste des applications locales de confiance. Une fenêtre reprenant la liste des applications locales de confiance s'ouvre.

   Les règles d'ajout d'applications à la liste des applications locales de confiance sont les mêmes que les règles d'ajout à la liste générale. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

9. Enregistrez vos modifications.

Comment ajouter un objet à la zone de confiance locale dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous voulez permettre à un utilisateur d'effectuer une action bloquée.
3. Sélectionnez l'onglet **Applications**.
4. Cliquez sur **Kaspersky Embedded Systems Security**.

   La fenêtre des paramètres locaux de l'application s'ouvre.

5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Dans la fenêtre des paramètres de l'application, sélectionnez **Complémentaire** → **Zone de confiance** et cliquez sur **Configurer**.

   La fenêtre **Exclusions et types d'objets détectés** s'ouvre.

7. Sous l'onglet **Exclusions de l'analyse**, dressez une liste des exclusions de l'analyse locale.

   Les règles de création d'exclusions locales sont les mêmes que les règles de création d'exclusions générales. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

8. Sous l'onglet **Applications de confiance**, dressez une liste des applications locales de confiance.

   Les règles d'ajout d'applications à la liste des applications locales de confiance sont les mêmes que les règles d'ajout à la liste générale. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

9. Enregistrez vos modifications.

Comment créer une exclusion d'analyse locale dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Dans la section **Exclusions de l'analyse et applications de confiance**, cliquez sur le bouton **Paramètres** à côté du groupe **Exclusions de l'analyse locale**.

   Kaspersky Embedded Systems Security masque la liste des exclusions d'analyse dans la Console de l'application si la configuration des exclusions d'analyse est bloquée par l'administrateur dans la Console d'administration de Kaspersky Security Center (symbole « cadenas fermé ») et si les exclusions d'analyse locales sont interdites (la case **Autoriser l'utilisation des exclusions locales** est décochée).

3. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les exclusions de l'analyse dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une exclusion de l'analyse à cette catégorie.

   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle exclusion d'analyse à la racine de la liste.

   - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle exclusion d'analyse à une catégorie en particulier, sélectionnez une catégorie.

   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des exclusions à partir de la liste des exclusions d'analyse prédéfinies.

4. Sélectionner **Nouvelle exclusion** ouvre la fenêtre **Exclusion de l'analyse**.

5. Pour exclure un fichier ou un dossier de l'analyse, cochez la case **Fichier ou dossier**. Cliquez sur le lien **Sélectionnez un fichier ou un dossier** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez un fichier ou un dossier en cliquant sur **Parcourir**.

   Vous pouvez également saisir le chemin manuellement. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

   - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

   - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

   - Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

     Vous pouvez utiliser des masques au début, au milieu ou à la fin du chemin du fichier. Par exemple, si vous souhaitez ajouter un dossier pour tous les utilisateurs aux exclusions, saisissez le masque `?:\Users\*\Folder\`.

6. Pour exclure une zone prédéfinie de l'analyse, cochez la case **Zone prédéfinie**. Cliquez sur le lien **sélectionner une zone prédéfinie** pour ouvrir une fenêtre, puis dans cette fenêtre, sélectionnez l'une des zones standards sur l'appareil protégé.

7. Pour exclure certains objets de l'analyse, cochez la case **Type d'un objet détecté**. Cliquez sur le lien **saisir des noms d'objets**, cliquez sur le bouton **Ajouter**, puis dans la fenêtre qui s'ouvre, saisissez le nom du type d'objet selon la classification de l'Encyclopédie Kaspersky (par exemple, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Vous pouvez utiliser des masques avec le caractère `?` (remplace n'importe quel caractère unique) et le caractère `*` (remplace n'importe quel nombre de caractères). Par exemple, si le masque `Client*` est spécifié, Kaspersky Embedded Systems Security exclut les objets `Client-IRC`, `Client-P2P` et `Client-SMTP` des analyses.

8. Pour exclure un fichier en particulier de l'analyse, cochez la case **Hachage de l'objet**. Cliquez sur le lien **saisir le hachage de l'objet** pour ouvrir une fenêtre, puis dans cette fenêtre, saisissez un hachage de fichier.

   Si le fichier est modifié, l'hachage du fichier sera également modifié. Dans ce cas, le fichier modifié ne sera pas ajouté aux exclusions.

9. Dans le groupe **Zone d'application de la règle**, sélectionnez les modules auxquels vous souhaitez que l'exclusion d'analyse s'applique.

10. Le cas échéant, saisissez un bref commentaire pour l'exclusion de l'analyse à créer dans le champ **Commentaires**.

11. Enregistrez les modifications pour ajouter l'exclusion à la liste. Vous pouvez désactiver l'exclusion à tout moment en cochant la case à côté de l'objet.

Comment ajouter une application à la liste des applications locales de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Dans la section **Exclusions**, cliquez sur le bouton **Paramètres** à côté du groupe **Applications de confiance locales**.

   Kaspersky Embedded Systems Security masque la liste consolidée des applications de confiance dans la Console de l'application si la configuration des applications de confiance est bloquée par l'administrateur dans la Console d'administration de Kaspersky Security Center (symbole « cadenas fermé ») et si les applications de confiance locales sont interdites (la case **Autoriser la modification des applications locales de confiance** est décochée).

3. Cliquez sur **Ajouter** et sélectionnez une action :

   - **Catégorie**. Vous pouvez regrouper les applications de confiance dans des catégories distinctes. Pour créer une nouvelle catégorie, saisissez le nom de la catégorie et ajoutez au moins une application de confiance à cette catégorie.
   - **Nouvelle exclusion**. Kaspersky Embedded Systems Security ajoute une nouvelle application de confiance à la racine de la liste.
   - **Nouvelle exclusion de la catégorie sélectionnée**. Pour ajouter une nouvelle application de confiance à une catégorie en particulier, sélectionnez une catégorie.
   - **Sélectionner une exclusion dans la liste**. Pour configurer rapidement Kaspersky Embedded Systems Security, vous pouvez ajouter des applications à partir de la liste des applications de confiance prédéfinies.

4. Sélectionner **Nouvelle exclusion** ouvre la fenêtre **Exclusion de l'analyse**.

5. Cochez la case **Utiliser le chemin d'accès complet du processus sur le disque pour le considérer comme fiable** et saisissez le chemin d'accès au fichier exécutable de l'application de confiance.

   Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque :

Kaspersky Embedded Systems Security prend en charge les variables d'environnement. Parallèlement, Kaspersky Embedded Systems Security convertit le chemin d'accès dans l'interface locale de l'application. Autrement dit, si vous saisissez le chemin d'accès au fichier `%userprofile%\Documents\File.exe`, une entrée `C:\Users\Fred123\Documents\File.exe` est ajoutéedans l'interface locale de l'application pour l'utilisateur Fred123. Par conséquent, Kaspersky Embedded Systems Security ignore le programme de confiance `File.exe` pour les autres utilisateurs. Pour appliquer l'entrée à tous les comptes utilisateur, vous pouvez utiliser le caractère `*` (par exemple, `C:\Users\*\Documents\File.exe`).

Chaque fois que vous ajoutez une nouvelle variable d'environnement, vous devez redémarrer l'application.

6. Dans la fenêtre des propriétés de l'application de confiance, configurez les paramètres avancés.
7. Enregistrez les modifications pour ajouter l'exclusion à la liste.

Exportation et importation de la zone de confiance

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Embedded Systems Security ne contrôle pas. La zone de confiance est constituée des listes suivantes : *exclusions d'analyse* et *applications de confiance*. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'exclusions du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions et la liste des applications de confiance ou pour procéder à la migration de la liste vers un autre serveur.

L'application utilise le format XML pour exporter et importer la *liste des exclusions* et des applications de confiance.

Kaspersky Embedded Systems Security ne prend pas en charge les listes d'exclusions ni les listes d'applications de confiance contenant plus de 5 000 objets.

Comment exporter et importer la zone de confiance dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Complémentaire** → **Zone de confiance** et cliquez sur **Paramètres**.
4. Pour exporter la liste des règles, procédez comme suit :
   a. Sélectionnez l'onglet **Exclusions de l'analyse**.
   b. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

c. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

d. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

Kaspersky Embedded Systems Security exporte la liste dans un fichier XML.

5. Pour exporter la liste des applications de confiance :

a. Sélectionnez l'onglet **Applications de confiance**.

b. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

c. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

d. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

Kaspersky Embedded Systems Security exporte la liste dans un fichier XML.

6. Pour importer la liste des exclusions, procédez comme suit :

a. Sélectionnez l'onglet **Exclusions de l'analyse**.

Une fenêtre reprenant la liste des exclusions s'ouvre.

b. Cliquez sur l'icône du dossier et sélectionnez **Importer** dans la liste déroulante.

c. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

d. Ouvrez le fichier.

Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

7. Pour importer une liste d'applications de confiance :

a. Sélectionnez l'onglet **Applications de confiance**.

Une fenêtre reprenant la liste des applications de confiance s'ouvre.

b. Cliquez sur **Importer**.

c. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications de confiance.

d. Ouvrez le fichier.

Si l'ordinateur dispose déjà d'une liste d'applications de confiance, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

8. Enregistrez vos modifications.

Comment exporter et importer la zone de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Complémentaire → Zone de confiance** et cliquez sur le bouton **Configurer**.
5. Pour exporter la liste des règles, procédez comme suit :

a. Sous l'onglet **Exclusions de l'analyse et applications de confiance**, sélectionnez les exclusions que vous souhaitez exporter.

b. Cliquez sur les trois points et sélectionnez **Exporter**.

c. Confirmez que vous souhaitez exporter uniquement les exclusions sélectionnées ou exporter la liste complète des exclusions.

Kaspersky Embedded Systems Security exporte la liste dans un fichier XML.

6. Pour exporter la liste des applications de confiance :

a. Sous l'onglet **Exclusions de l'analyse et applications de confiance**, sélectionnez les applications que vous souhaitez exporter.

b. Cliquez sur les trois points et sélectionnez **Exporter**.

c. Confirmez que vous souhaitez exporter uniquement les applications sélectionnées ou exporter la liste entière.

Kaspersky Embedded Systems Security exporte la liste dans un fichier XML.

7. Pour importer la liste des exclusions, procédez comme suit :

a. Sous l'onglet **Exclusions de l'analyse et applications de confiance**, cliquez sur **Importer depuis la version antérieure** si vous souhaitez importer la liste des exclusions à partir d'un fichier XML créé dans la version 3.4 ou une version antérieure de l'application.

Si vous importez des règles depuis un fichier XML créé dans la version 4.0 ou une version ultérieure, cliquez sur **Importer**.

b. Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

c. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

d. Cliquez sur **Importer**.

8. Pour importer une liste d'applications de confiance :

    a. Sous l'onglet **Exclusions de l'analyse et applications de confiance**, cliquez sur **Importer depuis la version antérieure** si vous souhaitez importer la liste des applications de confiance à partir d'un fichier XML créé dans la version 3.4 ou une version antérieure de l'application.

    Si vous importez des applications de confiance depuis un fichier XML créé dans la version 4.0 ou une version ultérieure, cliquez sur **Importer**.

    b. Si l'ordinateur dispose déjà d'une liste d'applications de confiance, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

    c. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des applications de confiance.

    d. Cliquez sur **Importer**.

9. Enregistrez vos modifications.

Comment exporter ou importer la zone de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

    La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Pour exporter la liste des exclusions et des applications de confiance :

    a. Dans la section **Exclusions**, cliquez sur le bouton **Paramètres** à côté des groupes **Exclusions de l'analyse** ou **Applications de confiance**.

    Une fenêtre contenant une liste d'exclusions d'analyse ou une liste d'applications de confiance s'ouvre.

    b. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

    c. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

        1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

        2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

    d. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

    Kaspersky Embedded Systems Security exporte la liste dans un fichier XML.

3. Pour importer une liste d'exclusions et d'applications de confiance :

    a. Dans la section **Exclusions**, cliquez sur le bouton **Paramètres** à côté des groupes **Exclusions de l'analyse** ou **Applications de confiance**.

    b. Sélectionnez les exclusions des applications de confiance que vous souhaitez importer.

    c. Cliquez sur l'icône du dossier et sélectionnez **Importer**.

    d. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des excluions ou des applications de confiance.

e. Ouvrez le fichier.

Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

4. Enregistrez vos modifications.

Utilisation du stockage système sécurisé des certificats

L'utilisation du stockage système sécurisé des certificats permet d'exclure de l'analyse antivirus les applications signées par une signature numérique de confiance. Kaspersky Embedded Systems Security attribue automatiquement ces applications au groupe *De confiance*

Comment configurer l'utilisation d'un stockage des certificats du système de confiance dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Complémentaire → Zone de confiance** et cliquez sur **Paramètres**.
4. Sélectionnez l'onglet **Boutique des certificats système de confiance**.
5. Cochez la case **Utiliser la boutique des certificats système de confiance**, et dans la liste déroulante, sélectionnez la boutique système que Kaspersky Embedded Systems Security doit considérer comme étant de confiance.
6. Enregistrez vos modifications.

Comment configurer l'utilisation d'un stockage des certificats du système de confiance dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Complémentaire → Zone de confiance** et cliquez sur le bouton **Configurer**.
5. Sélectionnez l'onglet **Boutique des certificats système de confiance**.
6. Cochez la case **Utiliser la boutique des certificats système de confiance**, et dans la liste déroulante, sélectionnez la boutique système que Kaspersky Embedded Systems Security doit considérer comme étant de confiance.
7. Enregistrez vos modifications.

Comment configurer l'utilisation d'un stockage des certificats du système de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et sélectionnez **Zone de confiance** dans le menu contextuel du nœud.

   La fenêtre **Configurer les paramètres de la zone de confiance** s'ouvre.

2. Sous **Boutique des certificats système de confiance**, cochez la case **Utiliser la boutique des certificats système de confiance**, et dans la liste déroulante, sélectionnez la boutique système que Kaspersky Embedded Systems Security doit considérer comme étant de confiance.

3. Enregistrez vos modifications.

Exclusions d'analyse prédéfinies et applications de confiance

Les exclusions d'analyse et les applications de confiance prédéfinies permettent d'ajouter rapidement à la zone de confiance les processus et fichiers des logiciels suivants :

- Serveur Microsoft Exchange
- Microsoft SQL Server
- Microsoft Hyper-V
- Le processus de déduplication des données dans Microsoft Windows Server
- Microsoft System Center Configuration Manager

Vous pouvez sélectionner des exclusions prédéfinies et des applications de confiance comme suit :

- Installation de l'application.
  - Installation locale de l'application à l'aide de l'Assistant
  - Propriétés du paquet d'installation
- Configuration de la stratégie.
  - Assistant de création d'une stratégie
  - Propriétés de la stratégie : exclusions de l'analyse et applications de confiance.
  - Sur la ligne de commande.

Protection des fichiers en temps réel

Le module Protection des fichiers en temps réel de Kaspersky Embedded Systems Security analyse les objets de l'appareil protégé suivants lorsqu'ils sont sollicités :

- Fichiers
- Flux de données alternatifs NTFS.
- Les enregistrements de démarrage principaux et les secteurs d'amorçage des disques durs locaux ou des appareils externes.
- Fichiers des conteneurs Windows Server 2016 et Windows Server 2019.

Lorsqu'une application quelconque enregistre un fichier sur l'appareil protégé ou le lit, Kaspersky Embedded Systems Security intercepte le fichier, y recherche la présence éventuelle de menaces et, s'il identifie une menace, exécute une action par défaut ou une action que vous avez définie : tenter de le désinfecter, le placer en quarantaine ou le supprimer. Avant la désinfection ou la suppression, Kaspersky Embedded Systems Security enregistre une copie chiffrée du fichier source dans le dossier Sauvegarde.

Kaspersky Embedded Systems Security intercepte les opérations sur les fichiers exécutées dans les conteneurs Windows Server 2016 et Windows Server 2019.

Un *conteneur* est un environnement isolé qui permet aux applications de fonctionner sans interaction directe avec le système d'exploitation. Si un conteneur se trouve dans la zone de protection du module, Kaspersky Embedded Systems Security analyse les fichiers du conteneur auxquels les utilisateurs accèdent à la recherche de menaces pour l'ordinateur. En cas de détection d'une menace, l'application tente de désinfecter le conteneur. Si la désinfection réussit, le conteneur continue de fonctionner. Si la désinfection échoue, le conteneur est désactivé.

Kaspersky Embedded Systems Security détecte également les applications malveillantes pour les processus exécutés dans le sous-système Windows pour Linux®. Pour ces processus, le module Protection des fichiers en temps réel applique l'action définie par la configuration actuelle.

À propos de la zone de protection de la tâche et des paramètres de sécurité

Par défaut, le module Protection des fichiers en temps réel protège tous les objets du système de fichiers de l'appareil. Si la sécurité n'exige pas de protéger tous les objets du système de fichiers ou vous voulez exclure expressément certains objets de la zone d'action de la tâche de protection en temps réel, vous pouvez limiter la zone de protection.

Dans la Console de l'application, la zone de protection se présente sous la forme d'une liste de ressources fichiers de l'appareil que Kaspersky Embedded Systems Security peut surveiller.

Paramètres de sécurité

Les paramètres de sécurité de la tâche peuvent être configurés globalement pour l'ensemble des nœuds ou des éléments repris dans la zone de protection ou individuellement pour chaque nœud ou élément dans la liste des ressources de fichier de l'appareil.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Vous pouvez configurer les paramètres de la zone de protection sélectionnée de l'une des manières suivantes :

- Sélection d'un des niveaux de sécurité prédéfinis.
- Configuration manuelle des paramètres de sécurité pour les nœuds ou les éléments sélectionnés dans la liste des ressources de fichier (le niveau de sécurité devient **Personnalisé**).

Zones de protection prédéfinies

La liste des ressources fichiers affiche les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security couvre les zones de protection définies suivantes :

- **Disques durs locaux**. Kaspersky Embedded Systems Security protège les fichiers sur les disques durs de l'appareil.
- **Disques amovibles**. Kaspersky Embedded Systems Security protège les fichiers sur les appareils externes tels que les disques compacts ou amovibles. Vous pouvez inclure ou exclure de la zone de protection tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.
- **Réseau**. Kaspersky Embedded Systems Security protège les fichiers qui sont enregistrés dans les dossiers réseau ou qui y sont lus par les applications exécutées sur l'appareil. Kaspersky Embedded Systems Security ne protège pas les fichiers lorsqu'ils sont sollicités par des applications à partir d'autres appareils protégés.

Par défaut, vous pouvez afficher et configurer des zones de protection prédéfinies dans la liste de zones ; vous pouvez également ajouter des zones prédéfinies à la liste au moment de sa création dans les paramètres de la zone de protection.

Les disques réseau connectés ne sont pas non plus affichés dans la liste des ressources fichier de l'appareil protégé. Pour inclure les objets d'un disque réseau dans la zone de protection, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

À propos des niveaux de sécurité prédéfinis

Pour les entrées sélectionnées dans l'arborescence ou la liste des ressources de fichiers de l'appareil protégé, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé**, **Protection maximale** et **Informer**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si votre réseau a adopté des mesures de sécurité pour l'appareil protégé additionnelles comme des pare-feux ou des stratégies de sécurité existantes, en plus de l'installation de Kaspersky Embedded Systems Security sur les appareils protégés et les postes de travail.

Recommandé

Le niveau de sécurité **Recommandé** offre le meilleur équilibre entre la protection et l'impact sur les performances des appareils protégés. Les experts de Kaspersky recommandent ce niveau pour protéger les appareils sur la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité élevé pour les appareils.

Informer

Le niveau de sécurité **Informer** est recommandé si le réseau de votre organisation comporte un grand nombre d'ordinateurs potentiellement infectés et si leur blocage est susceptible de perturber considérablement le fonctionnement de votre organisation.

Niveaux de sécurité prédéfinis et valeurs des paramètres correspondantes

Options	Niveau de sécurité			
	Performance maximale	Recommandé	Protection maximale	Informer
Protection des objets	Objets analysés en fonction de la liste d'extensions indiquée dans les bases antivirus	Objets analysés en fonction du format	Objets analysés en fonction du format	Objets analysés en fonction du format
Scan only new and modified files	Activée	Activée	Désactivée	Activée

Options	Niveau de sécurité			
	Performance maximale	Recommandé	Protection maximale	Informer
Scan of compound files	Désactivée	Analyser les fichiers aux formats Microsoft Office	Analyser les fichiers aux formats Microsoft Office	Analyser les fichiers aux formats Microsoft Office
Actions à exécuter sur les objets infectés et autres	Interdire l'accès et désinfecter. Supprimer si la désinfection échoue	Interdire l'accès et exécuter l'action recommandée par les experts de Kaspersky	Interdire l'accès et désinfecter. Supprimer si la désinfection échoue	Informer
Appliquer l'action aux types d'objets sélectionnés	Désactivée	Désactivée	Désactivée	Désactivée
Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré	Désactivée	Désactivée	Activée	Désactivée
Les objets système critiques sont les fichiers nécessaires au fonctionnement du système d'exploitation et de Kaspersky Embedded Systems Security. Vous ne pouvez pas supprimer ces fichiers. Il est impossible d'arrêter les processus associés à ces objets.				
Unpack in the background compound files larger than (MB)				
Stop scanning if it takes longer than (sec)	60 s	60 s	60 s	60 s
Do not scan compound objects larger than (MB)	8 Mo	8 Mo	Non configuré	8 Mo
Utiliser la technologie iSwift	Activée	Activée	Activée	Activée
Utiliser la technologie iChecker	Activée	Activée	Activée	Activée

Extensions de fichiers analysés par défaut par le module 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?*

Configuration du module Protection des fichiers en temps réel

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

Paramètres par défaut du module Protection des fichiers en temps réel

Paramètre	Valeur par défaut	Description
Zone de protection	L'ensemble de l'appareil protégé, à l'exception des disques virtuels.	Utilisez cette option pour modifier la zone de protection.
Paramètres de sécurité	Identique pour toute la zone de protection ; correspond au niveau de sécurité **Recommandé**.	Pour les nœuds sélectionnés dans l'arborescence ou dans la liste des ressources de fichiers de l'appareil protégé, vous pouvez exécuter les actions suivantes : • Sélectionner un autre niveau de sécurité prédéfini ; • Modifier manuellement les paramètres de sécurité. Vous pouvez enregistrer la configuration de paramètres de sécurité du nœud sélectionné dans un modèle en vue de l'appliquer par la suite à un autre nœud.
Mode de protection des objets	**Mode intelligent**.	Cette option permet de sélectionner le mode de protection, c'est-à-dire de définir le type de tentative d'accès pour lesquels Kaspersky Embedded Systems Security va analyser les objets.
Analyse heuristique	Le niveau de sécurité **Moyen** est appliqué.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Block access to network shared resources for the sessions that show malicious activity	Pas appliqué.	Choisissez cette option pour bloquer la session en cours et pour ajouter l'adresse IP de l'hôte ou le LUID de l'hôte pour lequel une activité malveillante a été détectée dans la section Stockage des ordinateurs bloqués.
Lancer une analyse des zones critiques en cas de détection d'une infection active	Appliquée.	Kaspersky Embedded Systems Security crée et lance une tâche d'analyse rapide quand une infection active est détectée.
Arrêter le conteneur en cas d'échec de la désinfection	Appliquée.	Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.
Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows	Appliquée.	Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.

Comment activer l'analyse antivirus des fichiers dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Paramètres de la protection des fichiers en temps réel**, cliquez sur **Paramètres**.
5. Cochez la case **Protection des fichiers en temps réel**.

6. Dans le groupe **Mode de protection des objets**, sous l'onglet **Général**, sélectionnez le mode de fonctionnement Protection des fichiers en temps réel :

   - **Mode intelligent**. Kaspersky Embedded Systems Security sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si le processus accède à l'objet plusieurs fois et le modifie, Kaspersky Embedded Systems Security analyse l'objet uniquement après son dernier enregistrement par le processus.

   - **À l'ouverture et en cas de modification**. Kaspersky Embedded Systems Security analyse un objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié. Cette option est sélectionnée par défaut.

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

   - **Lors de l'exécution**. Kaspersky Embedded Systems Security analyse le fichier uniquement en cas d'ouverture pour exécution.

7. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

8. Cochez ou décochez la case **Block access to network shared resources for the sessions that show malicious activity**.

9. Cochez ou décochez la case **Launch critical areas scan when active infection is detected**.

   Si la case est cochée, lorsqu'une infection active est détectée, Kaspersky Embedded Systems Security exécute la tâche prédéfinie *Analyse des zones critiques*. Cette case est cochée par défaut.

10. Spécifiez les paramètres d'analyse des opérations sur les fichiers exécutées dans les conteneurs Windows.

11. Enregistrez vos modifications.

Comment activer l'analyse antivirus des fichiers dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Protection des fichiers en temps réel** et cliquez sur le bouton **Configurer**.

5. Cochez la case **Activer la Protection des fichiers en temps réel**.

6. Dans le groupe **Mode de protection des objets**, sous l'onglet **Général**, sélectionnez le mode de fonctionnement Protection des fichiers en temps réel :

   - **Mode intelligent**. Kaspersky Embedded Systems Security sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si le processus accède à l'objet plusieurs fois et le modifie, Kaspersky Embedded Systems Security analyse l'objet uniquement après son dernier enregistrement par le processus.

   - **À l'ouverture et en cas de modification**. Kaspersky Embedded Systems Security analyse un objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié. Cette option est sélectionnée par défaut.

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

- **Lors de l'exécution**. Kaspersky Embedded Systems Security analyse le fichier uniquement en cas d'ouverture pour exécution.

7. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

8. Cochez ou décochez la case **Bloquer l'accès aux ressources partagées du réseau pour les sessions réseau présentant une activité malveillante**.

9. Cochez ou décochez la case **Lancer une analyse des zones critiques en cas de détection d'une infection active**.

   Si la case est cochée, lorsqu'une infection active est détectée, Kaspersky Embedded Systems Security exécute la tâche prédéfinie *Analyse des zones critiques*. Cette case est cochée par défaut.

10. Spécifiez les paramètres d'analyse des opérations sur les fichiers exécutées dans les conteneurs Windows.

11. Enregistrez vos modifications.

Comment activer l'analyse antivirus des fichiers dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Protection des fichiers en temps réel**.

2. Dans le panneau des résultats du nœud **Protection des fichiers en temps réel**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.

3. Cochez la case **Protection des fichiers en temps réel**.

4. Dans le groupe **Mode de protection des objets**, sous l'onglet **Général**, sélectionnez le mode de fonctionnement Protection des fichiers en temps réel :

   - **Mode intelligent**. Kaspersky Embedded Systems Security sélectionne lui-même les objets à analyser. Un objet est analysé lors de son ouverture, puis une deuxième fois lors de son enregistrement s'il a été modifié. Si le processus accède à l'objet plusieurs fois et le modifie, Kaspersky Embedded Systems Security analyse l'objet uniquement après son dernier enregistrement par le processus.

   - **À l'ouverture et en cas de modification**. Kaspersky Embedded Systems Security analyse un objet à l'ouverture et l'analyse à nouveau lors de son enregistrement, s'il a été modifié. Cette option est sélectionnée par défaut.

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

   - **Lors de l'exécution**. Kaspersky Embedded Systems Security analyse le fichier uniquement en cas d'ouverture pour exécution.

5. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

6. Cochez ou décochez la case **Block access to network shared resources for the sessions that show malicious activity**.

7. Cochez ou décochez la case **Launch critical areas scan when active infection is detected**.

   Si la case est cochée, lorsqu'une infection active est détectée, Kaspersky Embedded Systems Security exécute la tâche prédéfinie *Analyse des zones critiques*. Cette case est cochée par défaut.

8. Spécifiez les paramètres d'analyse des opérations sur les fichiers exécutées dans les conteneurs Windows.

9. Enregistrez vos modifications.

Configuration de la zone de protection pour le module Protection des fichiers en temps réel

Par défaut, le module Protection des fichiers en temps réel applique les mêmes paramètres de sécurité à toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Les valeurs par défaut des paramètres de sécurité peuvent être modifiées en les configurant comme paramètres communs pour l'ensemble de la zone de protection ou comme paramètres différents pour des éléments individuels dans la liste des ressources de fichiers de l'appareil.

Si le même objet est inclus dans plusieurs entrées de la zone de protection et si ces entrées ont des niveaux de sécurité différents, la dernière règle de la liste a la priorité. Prenons l'exemple d'une zone de protection qui inclut deux entrées : **Tous les disques durs** (niveau de sécurité **Inform**) et `*\Users\*\Downloads\*` (niveau de sécurité **Custom**). L'application analyse les disques durs conformément au niveau Informer, à l'exception du dossier `Downloads`. L'application analyse le dossier `Downloads` selon les paramètres définis manuellement, car cette entrée est la dernière de la liste de la zone de protection.

Comment configurer la zone de protection pour la Protection des fichiers en temps réel dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.

4. Dans la section **Protection des fichiers en temps réel**, cliquez sur **Paramètres**.

5. Sélectionnez l'onglet **Zone de protection**.

6. Dans la liste des ressources de fichiers de l'appareil protégé, sélectionnez les éléments pour lesquels vous souhaitez définir un niveau de sécurité prédéfini.

7. Si le partage de fichiers ne figure pas dans la liste, ajoutez-le manuellement :

   a. Cliquez sur **Ajouter**.

   b. Indiquez le chemin d'accès à l'objet à l'aide de l'arborescence des dossiers ou saisissez le chemin dans le champ **Objet**.

Le cas échéant, saisissez le masque du chemin d'accès à l'aide de caractères spéciaux :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

L'objet **Cet ordinateur** dans la liste des ressources de fichiers de l'ordinateur contient les objets suivants : **Tous les disques durs**, **Tous les disques réseau** et **Tous les disques amovibles**.

c. Cliquez sur **OK**.

8. Assurez-vous que la ressource de fichier sélectionnée est incluse dans la zone de protection.

9. Spécifiez un niveau de sécurité prédéfini de la zone de protection sélectionnée en cliquant sur **Configurer**. Par défaut, les mêmes paramètres de sécurité sont appliqués à l'ensemble de la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**. Vous pouvez également modifier les paramètres de sécurité par défaut.

10. Enregistrez vos modifications.

Comment configurer la zone de protection pour la Protection des fichiers en temps réel dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Protection des fichiers en temps réel** et cliquez sur le bouton **Configurer**.

5. Sélectionnez l'onglet **Zone de protection**.

6. Dans la liste des ressources de fichiers de l'appareil protégé, sélectionnez les éléments pour lesquels vous souhaitez définir un niveau de sécurité prédéfini.

7. Si le partage de fichiers ne figure pas dans la liste, ajoutez-le manuellement :

   a. Cliquez sur **Ajouter**.

   b. Dans la liste **Type d'objet**, sélectionnez une option :

Pour l'option **Masque**, utilisez des caractères spéciaux pour saisir le masque du chemin de l'objet :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

L'objet **Cet ordinateur** dans la liste des ressources de fichiers de l'ordinateur contient les objets suivants : **Tous les disques durs**, **Tous les disques réseau** et **Tous les disques amovibles**.

c. Cliquez sur **OK**.

8. Assurez-vous que la ressource de fichier sélectionnée est incluse dans la zone de protection à l'aide du commutateur à bascule en regard de l'élément de la liste.

9. Spécifiez un niveau de sécurité prédéfini de la zone de protection sélectionnée en cliquant sur **Modifier**. Par défaut, les mêmes paramètres de sécurité sont appliqués à l'ensemble de la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**. Vous pouvez également modifier les paramètres de sécurité par défaut.

10. Enregistrez vos modifications.

Comment configurer la zone de protection pour la Protection des fichiers en temps réel dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur** → **Protection des fichiers en temps réel**.

2. Dans le panneau des résultats du nœud **Protection des fichiers en temps réel**, cliquez sur **Configurer la zone de protection**.

   La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.

3. Dans la liste des ressources de fichiers de l'appareil protégé, sélectionnez les éléments pour lesquels vous souhaitez définir un niveau de sécurité prédéfini.

4. Si le partage de fichiers ne figure pas dans la liste, ajoutez-le manuellement :

   a. Cliquez sur **Ajouter**.

   b. Indiquez le chemin d'accès à l'objet à l'aide de l'arborescence des dossiers ou saisissez le chemin dans le champ **Objet**.

Le cas échéant, saisissez le masque du chemin d'accès à l'aide de caractères spéciaux :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

L'objet **Cet ordinateur** dans la liste des ressources de fichiers de l'ordinateur contient les objets suivants : **Tous les disques durs**, **Tous les disques réseau** et **Tous les disques amovibles**.

c. Cliquez sur **OK**.

5. Assurez-vous que la ressource de fichier sélectionnée est incluse dans la zone de protection.

6. Spécifiez un niveau de sécurité prédéfini de la zone de protection sélectionnée en cliquant sur **Configurer**. Par défaut, les mêmes paramètres de sécurité sont appliqués à l'ensemble de la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**. Vous pouvez également modifier les paramètres de sécurité par défaut.

7. Enregistrez vos modifications.

Configuration manuelle des paramètres de sécurité

Par défaut, les tâches de protection en temps réel de l'ordinateur appliquent les mêmes paramètres de sécurité pour toute la zone de protection. Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone de protection ou avec des variations pour des éléments individuels dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil.

Lorsque vous utilisez l'arborescence des ressources du fichier de l'appareil protégés, les paramètres de sécurité configurés pour le nœud parent sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Comment configurer les paramètres de sécurité manuellement dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.

4. Dans la section **Protection des fichiers en temps réel**, cliquez sur **Paramètres**.
5. Dans la fenêtre **Protection des fichiers en temps réel**, rendez-vous dans l'onglet **Zone de protection**.
6. Sélectionnez la ressource dont vous souhaitez configurer les paramètres de sécurité.
7. Cliquez sur **Configurer**.
8. Dans la fenêtre qui s'ouvre, sélectionnez le niveau de sécurité requis et cliquez sur **Paramètres**.
9. Sous l'onglet **Général**, spécifiez les paramètres suivants :
   - Objets qui doivent être inclus dans 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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.
   - Dans le groupe **Optimisation**, cochez ou décochez la case **Scan only new and modified files**.
   - Dans la section **Analyse des fichiers composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
     - **Analyser les archives**
     - **Analyser les paquets de distribution**
     - **Analyser les fichiers aux formats Microsoft Office**
     - **Analyser les fichiers au format de messagerie**
10. Sous l'onglet **Actions**, spécifiez les paramètres suivants :
    - Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
      - **Informer**
      - **Bloquer**
      - **Exécuter une action supplémentaire**

Sélectionnez l'action dans la liste déroulante.

- **Désinfecter**
- **Disinfect. Delete if disinfection fails**
- **Supprimer**
- **Recommandé**

- Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

  a. Cochez ou décochez la case **Appliquer l'action aux types d'objets sélectionnés**.

  b. Cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.

- Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case **Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré**.

11. Sous l'onglet **Optimisation**, spécifiez les paramètres suivants :

- **Unpack in the background compound files larger than (MB)**
- **Arrêter l'analyse si elle dure plus de (s.)**
- **Ne pas analyser les objets composés de plus de (Mo)**
- **Utiliser la technologie iSwift**
- **Utiliser la technologie iChecker**

12. Enregistrez les nouveaux paramètres de sécurité.

Comment configurer manuellement les paramètres de sécurité dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Protection des fichiers en temps réel** et cliquez sur le bouton **Configurer**.
5. Sélectionnez l'onglet **Zone de protection**.
6. Réalisez une des opérations suivantes :

- Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle règle et spécifier les paramètres de sécurité associés.
- Sélectionnez une règle existante et cliquez sur le bouton **Modifier**.

La fenêtre **Modifier la zone** s'ouvre.

7. Réglez le commutateur à bascule sur **Actif**.
8. Sélectionnez un niveau de sécurité et définissez les paramètres de sécurité nécessaires.
9. Dans la section **Mode de protection des objets**, sélectionnez le type d'objet que vous souhaitez inclure dans la zone de protection :
   - Objets qui doivent être inclus dans 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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.
10. Dans la section **Optimisation**, cochez ou décochez la case **Protéger uniquement les nouveaux fichiers et les fichiers modifiés**.
11. Dans la section **Protection des objets composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
    - **Analyser les archives**
    - **Analyser les paquets de distribution**
    - **Analyser les fichiers aux formats Microsoft Office**
    - **Analyser les fichiers au format de messagerie**
12. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
    - **Informer**
    - **Bloquer**
    - **Exécuter une action supplémentaire**

      Sélectionnez l'action dans la liste déroulante.
      - **Désinfecter**
      - **Désinfecter ; supprimer si la désinfection est impossible**

- Supprimer
- Recommandé

13. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

    a. Cochez ou décochez la case Appliquer l'action aux types d'objets sélectionnés.

    b. Si la case est cochée, cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.

14. Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré.

15. Configurez les paramètres suivants dans la section **Optimisation** :

    - Décompresser les fichiers composés en arrière-plan
    - Arrêter l'analyse si elle dure plus de (s.)
    - Ne pas analyser les objets composés de plus de (Mo)
    - Utiliser la technologie iSwift
    - Utiliser la technologie iChecker

16. Enregistrez les nouveaux paramètres de sécurité.

Comment configurer manuellement les paramètres de sécurité dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur** → **Protection des fichiers en temps réel**.

2. Dans le panneau des résultats du nœud **Protection des fichiers en temps réel**, cliquez sur **Configurer la zone de protection**.

   La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.

3. Sélectionnez la ressource dont vous souhaitez configurer les paramètres de sécurité.

4. Cliquez sur **Configurer**.

5. Dans la fenêtre qui s'ouvre, sélectionnez le niveau de sécurité requis et cliquez sur **Paramètres**.

6. Sous l'onglet **Général**, spécifiez les paramètres suivants :

    - Objets qui doivent être inclus dans 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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.

- **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.

- **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.

- Dans le groupe **Optimisation**, cochez ou décochez la case **Protéger uniquement les nouveaux fichiers et les fichiers modifiés**.

- Dans la section **Analyse des fichiers composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :

  - **Analyser les archives**. Analyse des formats d'archives ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE et autres. L'application analyse les archives non seulement par extension, mais aussi par format. Lors de la vérification des archives, l'application effectue une décompression récursive. Il est ainsi possible de détecter les menaces à l'intérieur d'archives à plusieurs niveaux (une archive dans une archive).

  - **Analyser les paquets de distribution**. La case active/désactive l'analyse des paquets de distribution des logiciels tiers.

  - **Analyser les fichiers aux formats Microsoft Office**. Analyse les fichiers Microsoft Office (DOC, DOCX, XLS, PPT et autres extensions Microsoft). Les fichiers au format Office incluent également des objets OLE. Kaspersky Embedded Systems Security analyse les fichiers au format Office dont la taille est inférieure à 1 Mo, que la case soit cochée ou non.

  - **Analyser les fichiers au format de messagerie**.

7. Sous l'onglet **Actions**, spécifiez les paramètres suivants :

- Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

  - **Informer**

  - **Bloquer**

  - **Exécuter une action supplémentaire**.

    Sélectionnez l'action dans la liste déroulante.

    - **Désinfecter**

    - **Disinfect. Delete if disinfection fails**

    - **Supprimer**

    - **Recommandé**

- Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

  a. Cochez ou décochez la case **Appliquer l'action aux types d'objets sélectionnés**.

  b. Cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.

- Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case **Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré**.

8. Sous l'onglet **Optimisation**, spécifiez les paramètres suivants :

   - **Unpack in the background compound files larger than (MB)**
   - **Arrêter l'analyse si elle dure plus de (s.)**
   - **Ne pas analyser les objets composés de plus de (Mo)**
   - **Utiliser la technologie iSwift**
   - **Utiliser la technologie iChecker**

9. Enregistrez les nouveaux paramètres de sécurité.

Analyser les conteneurs.

Un *conteneur* est un environnement isolé dans lequel une application peut s'exécuter sans interagir directement avec le système d'exploitation. L'utilisation de conteneurs comporte les risques suivants :

- Les pirates peuvent être en mesure d'exploiter les vulnérabilités de la conteneurisation pour compromettre les applications à l'intérieur du conteneur.
- Les pirates informatiques peuvent exploiter une configuration non sécurisée de l'environnement du conteneur pour obtenir un accès non autorisé aux données de l'ordinateur ou pour compromettre l'intégrité du système.
- Une attaque réussie sur un conteneur peut permettre à un pirate d'accéder aux données de l'ordinateur.
- Les pirates informatiques sont susceptibles d'exploiter les vulnérabilités du réseau pour en intercepter le trafic.

Kaspersky Embedded Systems Security est un outil externe permettant de détecter les outils malveillants à l'intérieur des conteneurs. Cela permet de maintenir les performances des conteneurs et d'éviter les conflits avec d'autres applications à l'intérieur des conteneurs. L'installation de Kaspersky Embedded Systems Security à l'intérieur du conteneur n'est pas prise en charge.

En plus d'assurer la sécurité des conteneurs, Kaspersky Embedded Systems Security permet de gérer les applications à l'intérieur des conteneurs à l'aide du module Contrôle du lancement des applications. Le module Contrôle du lancement des applications est configuré pour les conteneurs de la même manière que pour les applications installées sur l'ordinateur. Le module Contrôle de l'intégrité du système prend également en charge les conteneurs.

Exigences relatives au conteneur

- Le conteneur doit être un conteneur Docker. Les autres outils de conteneurisation ne sont pas pris en charge.
- Le conteneur doit fonctionner en mode d'isolation du processus. Le mode d'isolation de Hyper-V n'est pas pris en charge.
- Le conteneur doit être placé sur un serveur Windows Serveur 2016, 2019 ou 2022 (Docker Host).
- Le conteneur doit inclure une image système Windows (Docker Image). Windows 10 et 11 ne sont pas pris en charge. Les images Linux ne sont pas prises en charge.
- Analyse des conteneurs s'exécutant dans WSL2 : Windows Subsystem for Linux v2 Le mode (Docker Wine) n'est pas pris en charge.

Action en cas de détection d'une menace

Si une menace est détectée à l'intérieur d'un conteneur, l'application applique l'action sélectionnée pour le module Protection des fichiers en temps réel. L'analyse des conteneurs présente des paramètres complémentaires (voir les instructions ci-dessous). Si une menace est détectée, l'application bloque l'activité malveillante et exécute l'action sélectionnée (par exemple, tente de désinfecter l'objet). Kaspersky Embedded Systems Security peut arrêter le conteneur s'il ne parvient pas à désinfecter l'objet détecté. Par défaut, l'arrêt des conteneurs est activé.

Comment configurer l'analyse des conteneurs dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Protection des fichiers en temps réel**, cliquez sur **Paramètres**.
5. Dans le groupe **Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows**, configurez les paramètres d'analyse du conteneur :
   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.
   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.
6. Enregistrez les nouveaux paramètres de sécurité.

Comment configurer l'analyse des conteneurs dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Protection des fichiers en temps réel** et cliquez sur le bouton **Configurer**.
5. Dans le groupe **Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows**, configurez les paramètres d'analyse du conteneur :

   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.

   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.
6. Enregistrez les nouveaux paramètres de sécurité.

Comment configurer l'analyse des conteneurs dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Protection des fichiers en temps réel**.
2. Dans le panneau des résultats du nœud **Protection des fichiers en temps réel**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Protection des fichiers en temps réel** s'ouvre.
3. Dans le groupe **Analyse des opérations sur les fichiers exécutées dans des conteneurs Windows**, configurez les paramètres d'analyse du conteneur :

   - **Arrêter le conteneur en cas d'échec de la désinfection**. Il se peut que l'application ne dispose pas des droits de lecture et d'écriture suffisants pour l'objet détecté. Dans ce cas, la désinfection ou la suppression de l'objet détecté est impossible. Si cette case est cochée, l'application bloque l'objet détecté et arrête le conteneur. Si cette case est décochée, l'application bloque uniquement l'objet détecté.

   - **Ne pas analyser les opérations sur les fichiers exécutées dans des conteneurs Windows**. Si la case est cochée, l'application analyse le conteneur uniquement lors de son démarrage. Si cette case est décochée, l'application analyse le conteneur en permanence et en temps réel.
4. Enregistrez vos modifications.

Utilisation du KSN

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Embedded Systems Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau Kaspersky Security Network permet de récupérer ces données.

La fonctionnalité KSN peut ne pas être disponible dans le logiciel aux États-Unis.

Kaspersky Security Network (KSN) est un ensemble de services cloud qui permet d'accéder à la banque de solutions de Kaspersky sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Embedded Systems Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite. Si vous participez à Kaspersky Security Network, Kaspersky Embedded Systems Security reçoit des informations des services KSN sur la réputation des adresses Internet analysées, ainsi que des informations sur la catégorie et la réputation des fichiers analysés. Pour en savoir plus sur la configuration de l'accès à KSN, consultez l'aide de Kaspersky Security Center.

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

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

L'infrastructure des bases de données de réputation de Kaspersky

Kaspersky Embedded Systems Security prend en charge les solutions d'infrastructure suivantes pour utiliser les bases de données de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques.

- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Embedded Systems Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KPSN a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :

  - absence de connexion des postes de travail locaux à Internet ;

  - interdiction législative ou restriction imposée par la sécurité de l'entreprise sur l'envoi de données hors du pays ou hors du réseau local de l'organisation.

Activation de l'utilisation de Kaspersky Security Network

Comment activer l'utilisation de Kaspersky Security Network.dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Network, sélectionnez le dossier **Stratégies**.
2. Sélectionnez la stratégie requise de Kaspersky Embedded Systems Security et ouvrez les propriétés de la stratégie d'un double-clic.
3. Une fenêtre s'ouvre ; dans cette fenêtre, dans la liste des sections, sélectionnez **Protection en temps réel de l'ordinateur → Utilisation de KSN**.
4. Cliquez sur **Paramètres**.
5. Cochez la case **Kaspersky Security Network** pour activer le module.

   Si vous avez activé l'utilisation de KSN, Kaspersky Embedded Systems Security affichera la déclaration de Kaspersky Security Network. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.

   Par défaut, Kaspersky Embedded Systems Security utilise le mode Étendu de Kaspersky Security Network. Le mode étendu de Kaspersky Security Network est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Embedded Systems Security envoie des données supplémentaires à Kaspersky.
6. Le cas échéant, décochez la case **Activer le mode étendu de KSN**.
7. Enregistrez vos modifications.

Si l'utilisation de Kaspersky Security Network est activée, Kaspersky Embedded Systems Security utilise les informations sur la réputation des fichiers, des ressources Internet et des applications reçues de Kaspersky Security Network.

Activation de l'utilisation de Kaspersky Security Network dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Kaspersky Security Network**.
3. Dans la fenêtre principale de l'application, cliquez sur **Propriétés**.
4. Cochez la case **Kaspersky Security Network** pour activer le module.

   Si vous avez activé l'utilisation de KSN, Kaspersky Embedded Systems Security affichera la déclaration de Kaspersky Security Network. Veuillez lire et accepter les conditions d'utilisation de la Déclaration de Kaspersky Security Network (KSN) si vous les acceptez.

   Par défaut, Kaspersky Embedded Systems Security utilise le mode Étendu de Kaspersky Security Network. Le mode étendu de Kaspersky Security Network est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Embedded Systems Security envoie des données supplémentaires à Kaspersky.

5. Le cas échéant, décochez la case **Activer le mode étendu de KSN**.

6. Enregistrez vos modifications.

Si l'utilisation de Kaspersky Security Network est activée, Kaspersky Embedded Systems Security utilise les informations sur la réputation des fichiers, des ressources Internet et des applications reçues de Kaspersky Security Network.

Activation de l'utilisation de Kaspersky Security Network dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans la section **Protection en temps réel de l'ordinateur → Utilisation de KSN** et cliquez sur le bouton **Configurer**.

5. Dans la fenêtre qui s'ouvre, cochez la case **Activer Kaspersky Security Network** pour activer le module.

   Si vous avez activé l'utilisation de KSN, Kaspersky Embedded Systems Security affichera la déclaration de Kaspersky Security Network. Si vous êtes d'accord, vous acceptez les conditions d'utilisation de Kaspersky Security Network.

   Par défaut, Kaspersky Embedded Systems Security utilise le mode Étendu de Kaspersky Security Network. Le mode étendu de Kaspersky Security Network est un mode de fonctionnement de l'application dans le cadre duquel Kaspersky Embedded Systems Security envoie des données supplémentaires à Kaspersky.

6. Le cas échéant, décochez la case **Activer le mode étendu de KSN**.

7. Enregistrez vos modifications.

Par conséquent, si l'utilisation de Kaspersky Security Network est activée, Kaspersky Embedded Systems Security utilise les informations sur la réputation des fichiers, des ressources Internet et des applications reçues de Kaspersky Security Network.

Statistiques d'utilisation de Kaspersky Security Network

Pendant l'exécution de la tâche *Utilisation de KSN*, vous pouvez consulter les informations relatives au nombre d'objets traités par Kaspersky Embedded Systems Security depuis le démarrage de la tâche jusqu'à présent.

Pour consulter les statistiques d'utilisation de KSN, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Protection en temps réel de l'ordinateur**.

2. Sélectionnez le nœud enfant **Kaspersky Security Network**.

   Dans le panneau des résultats, dans la section **Statistiques**, les statistiques de la tâche s'affichent (cf. le tableau ci-dessous).

Statistiques de KSN

Champ	Description
Requêtes fichier envoyées	Nombre de requêtes sur la réputation des objets envoyées par Kaspersky Embedded Systems Security à KSN.
Fichiers douteux dans KSN	Nombre d'objets auxquels KSN a attribué une réputation non fiable.
Erreurs d'envoi des requêtes	Nombre de requêtes KSN traitées avec une erreur.
Statistiques collectées	Nombre de paquets de statistiques générés envoyés à KSN.
Objets supprimés	Nombre d'objets supprimés avec succès 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.
Placé dans la Sauvegarde	Nombre d'objets copiés avec succès dans la sauvegarde par Kaspersky Embedded Systems Security.
Objets non déplacés dans la Sauvegarde	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu copier dans la sauvegarde, par exemple en raison d'un espace disque insuffisant. L'application ne désinfecte pas et ne supprime pas les fichiers qui n'ont pas pu être placés dans la sauvegarde.
Mode limité	L'état indique si l'application envoie des requêtes sur la réputation des fichiers en mode limité. En mode limité, Kaspersky Embedded Systems Security n'envoie qu'une partie des demandes de réputation de fichiers selon les recommandations des experts de Kaspersky.

Les valeurs des champs **Objets supprimés**, **Objets non supprimés**, **Placé dans la Sauvegarde**, **Objets non déplacés dans la Sauvegarde** sont générés à partir des statistiques du module Protection des fichiers en temps réel.

Limitations de Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Embedded Systems Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Kaspersky Private Security Network vous permet d'utiliser votre propre base de données de réputation locale pour vérifier la réputation des objets (fichiers ou adresses Internet). La réputation d'un objet ajouté à la base de données de réputation locale a une priorité plus élevée que celle d'un objet ajouté à KSN/KPSN. Par exemple, imaginez que Kaspersky Embedded Systems Security analyse un ordinateur et demande la réputation d'un fichier dans KSN/KPSN. Si le fichier a une réputation *Douteuses* dans la base de données de réputation locale, mais a une réputation *De confiance* dans KSN/KPSN, Kaspersky Embedded Systems Security détectera le fichier comme *Douteuses* et prendra les mesures définies concernant les menaces détectées.

Cependant, dans certains cas, il se peut que Kaspersky Embedded Systems Security ne demande pas la réputation d'un objet dans KSN/KPSN. Si tel est le cas, Kaspersky Embedded Systems Security ne recevra pas les données de la base de données de réputation locale de KPSN. Il se peut que Kaspersky Embedded Systems Security ne demande pas la réputation d'un objet dans KSN/KPSN pour les raisons suivantes :

- Les applications de Kaspersky utilisent des bases de données de réputation hors ligne. Les bases de données de réputation hors ligne sont conçues pour optimiser les ressources pendant le fonctionnement des applications Kaspersky et pour protéger les objets d'importance critique sur l'ordinateur. Les bases de données de réputation hors ligne sont créées par les experts de Kaspersky à partir des données de Kaspersky Security Network. Les applications Kaspersky mettent à jour les bases de données de réputation hors ligne avec les bases antivirus de l'application en question. Si les bases de données de réputation hors ligne contiennent des informations sur un objet en cours d'analyse, l'application ne demande pas la réputation de cet objet à KSN/KPSN.

- Les exclusions d'analyse (zone de confiance) sont configurées dans les paramètres de l'application. Si tel est le cas, l'application ne tient pas compte de la réputation de l'objet dans la base de données de réputation locale.

- L'application utilise des technologies d'optimisation de l'analyse, comme iSwift ou iChecker, ou met en cache les demandes de réputation à KSN/KPSN. Si tel est le cas, il se peut que l'application ne demande pas la réputation des objets précédemment analysés.

- Pour optimiser sa charge de travail, l'application analyse les fichiers d'un certain format et d'une certaine taille. La liste des formats et des limites de taille pertinents est déterminée par les experts de Kaspersky. Cette liste est mise à jour avec les bases antivirus de l'application.

Paramètres du proxy KSN

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

Le service KSN Proxy offre les possibilités suivantes :

- L'ordinateur de l'utilisateur peut interroger KSN et transmettre à KSN des informations, même s'il n'a pas d'accès direct à Internet.

- Le service KSN Proxy met en cache les données traitées, ce qui réduit la charge sur le canal de communication avec le réseau externe et accélère la réception des informations sollicitées sur l'ordinateur de l'utilisateur.

Par défaut, une fois que KSN est activé et que la Déclaration KSN est acceptée, l'application utilise un serveur proxy pour se connecter à Kaspersky Security Network. Le serveur proxy utilisé par l'application est le Serveur d'administration de Kaspersky Security Center via le port TCP 13111. Ainsi, si le proxy KSN n'est pas disponible, vous devez vérifier le fonctionnement de l'appareil en tant que serveur proxy KSN. Vous devez vérifier les points suivants :

- Le service *ksnproxy* est exécuté sur le Serveur d'administration.

- Le Pare-feu de l'ordinateur ne bloque pas le port 13111.

Vous pouvez configurer l'utilisation du proxy KSN comme suit : activer ou désactiver le proxy KSN, et configurer le port pour la connexion. Pour ce faire, vous devez ouvrir les propriétés du Serveur d'administration. Pour en savoir plus à propos de la configuration du proxy KSN, veuillez consulter l'aide de Kaspersky Security Center. Vous pouvez également activer ou désactiver le proxy KSN pour des ordinateurs individuels dans la stratégie de Kaspersky Embedded Systems Security.

Comment activer le proxy KSN dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise de Kaspersky Embedded Systems Security et ouvrez les propriétés de la stratégie d'un double-clic.
3. Une fenêtre s'ouvre ; dans cette fenêtre, dans la liste des sections, sélectionnez **Protection en temps réel de l'ordinateur → Utilisation de KSN**.
4. Cliquez sur **Paramètres**.
5. Dans le groupe **Paramètres de KSN Proxy**, utilisez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver KSN Proxy.
6. Le cas échéant, cochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Si la case est cochée, Kaspersky Embedded Systems Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).
7. Enregistrez vos modifications.

Comment activer le proxy KSN dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Kaspersky Security Network**.
3. Dans la fenêtre principale de l'application, cliquez sur **Propriétés**.
4. Dans le groupe **Paramètres de KSN Proxy**, utilisez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver KSN Proxy.
5. Le cas échéant, cochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Si la case est cochée, Kaspersky Embedded Systems Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).
6. Enregistrez vos modifications.

Comment activer le proxy KSN dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Utilisation de KSN** et cliquez sur le bouton **Configurer**.

5. Cochez et décochez la case **Utiliser le Serveur d'administration comme serveur proxy KSN** pour activer ou désactiver le proxy KSN.

6. Le cas échéant, cochez la case **Utiliser les serveurs de Kaspersky Security Network si le serveur proxy KSN n'est pas disponible**.

   Si la case est cochée, Kaspersky Embedded Systems Security utilise les serveurs KSN quand le service KSN Proxy est inaccessible. Les serveurs KSN peuvent être situés à la fois du côté de Kaspersky et du côté de tiers (lorsque Kaspersky Private Security Network est utilisé).

7. Enregistrez vos modifications.

L'adresse du proxy KSN correspond à l'adresse du Serveur d'administration. Lorsque le nom de domaine du Serveur d'administration est modifié, vous devez mettre à jour manuellement l'adresse du proxy KSN.

Protection contre les Exploits

Kaspersky Embedded Systems Security permet de protéger la mémoire du processus contre les exploits. Cette fonctionnalité est mise en œuvre par le module Protection contre les Exploits, que vous pouvez utiliser pour modifier l'état d'activité du module et configurer la protection des processus contre les exploits.

Le module Protection contre les Exploits surveille le code qui exploite les vulnérabilités d'un ordinateur pour obtenir des privilèges d'administrateur ou effectuer des actions malveillantes de la part de l'exploit. Les exploits, par exemple, utilisent l'attaque par débordement de tampon. Dans ce cas, l'exploit envoie un gros volume de données à l'application vulnérable. Lors du traitement de ces données, l'application vulnérable exécute un code malveillant. Suite à cette attaque, un exploit pourrait lancer l'installation non autorisée d'une application malveillante. S'il s'avère que la tentative d'exécution d'un fichier exécutable depuis une application vulnérable n'est pas due à l'utilisateur, Kaspersky Embedded Systems Security bloque le lancement de ce fichier ou le signale à l'utilisateur. Le module protège la mémoire du processus contre les Exploits à l'aide de l'Agent de protection des processus externe dans le processus protégé.

L'*Agent de protection de processus* (ci-après également appelé *Agent*) est un module de Kaspersky Embedded Systems Security chargé dynamiquement qui s'intègre aux processus protégés en vue de contrôler leur intégrité et de réduire l'impact de l'exploitation des vulnérabilités.

Le fonctionnement de l'Agent à l'intérieur du processus protégé dépend des itérations de lancement et d'arrêt de ce processus : le chargement primaire de l'Agent dans le processus ajouté à la liste des processus protégés est possible seulement au relancement du processus. Le déchargement de l'Agent de processus une fois supprimé de la liste est possible seulement après le relancement du processus.

Il convient d'arrêter l'Agent avant de le décharger des processus protégés : lors de la suppression du module Protection contre les Exploits, l'application gèle l'environnement et force le déchargement de l'Agent des processus protégés. Si, au cours de la désinstallation du module, l'agent est inséré dans un des processus protégés, vous devez arrêter le processus affecté. Un redémarrage de l'appareil protégé peut être nécessaire (par exemple, si le processus système est protégé).

En cas de détection de signes d'une attaque de l'Exploit sur le processus protégé, Kaspersky Embedded Systems Security exécute une des actions suivantes :

- termine le processus lors de la tentative d'exploitation de la vulnérabilité ;
- informe que le processus a été compromis.

Vous pouvez arrêter la protection des processus d'une des manières suivantes :

- supprimer le module ;
- supprimer le processus de la liste des processus protégés et le relancer.

Mode de protection contre les exploits

Vous pouvez configurer les actions de réduction de l'impact de l'exploitation des vulnérabilités dans les processus protégés, en sélectionnant un de deux modes :

- **Bloquer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security termine un processus protégé en cas de détection d'une tentative d'exploit si une technique de réduction de l'impact active a été appliquée au processus.

  En cas de détection d'une tentative d'exploitation d'une vulnérabilité dans un processus du système d'exploitation critique protégé, Kaspersky Embedded Systems Security ne termine pas ce processus quel que soit le mode indiqué dans les paramètres du module Protection contre les Exploits.

- **Informer** (lorsque vous travaillez dans Kaspersky Security Center Web Console – **Informer**). Appliquez ce mode pour recevoir des informations sur les instances d'exploits dans les processus protégés à l'aide des événements dans les journaux de sécurité. Le processus exploité continue d'être exécuté.

  Si ce mode est sélectionné, Kaspersky Embedded Systems Security crée des événements pour consigner toutes les tentatives d'exploit de vulnérabilités. Sélectionné par défaut.

Activation et désactivation de la Protection contre les Exploits

Kaspersky Embedded Systems Security permet de surveiller les fichiers exécutables exécutés par les applications vulnérables. Si Kaspersky Embedded Systems Security détecte qu'un fichier exécutable d'une application vulnérable n'a pas été lancé par l'utilisateur, il exécute l'action sélectionnée (par exemple, il interdit l'opération).

Comment activer ou désactiver la Protection contre les Exploits dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise de Kaspersky Embedded Systems Security et ouvrez les propriétés de la stratégie d'un double-clic.
3. Une fenêtre s'ouvre ; dans cette fenêtre, dans la liste des sections, sélectionnez **Protection en temps réel de l'ordinateur → Protection contre les Exploits**.
4. Cliquez sur **Paramètres**.
5. Cochez la case **Protection contre les Exploits** pour activer le module.
6. Sous l'onglet **Général**, sélectionnez un mode de protection contre les exploits : **Bloquer** ou **Informer**.
7. Si nécessaire, décochez la case **Protection contre les Exploits** pour désactiver le module.
8. Enregistrez vos modifications.

Comment activer ou désactiver la Protection contre les Exploits dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les Exploits**.
3. Dans la fenêtre principale de l'application, cliquez sur **Propriétés**.
4. Cochez la case **Protection contre les Exploits** pour activer le module.
5. Sous l'onglet **Général**, sélectionnez un mode de protection contre les exploits : **Bloquer** ou **Informer**.
6. Si nécessaire, décochez la case **Protection contre les Exploits** pour désactiver le module.
7. Enregistrez vos modifications.

Comment activer ou désactiver la Protection contre les Exploits dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Protection contre les Exploits** et cliquez sur le bouton **Configurer**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sous **Mode de Protection contre les Exploits**, cochez la case **Empêcher l'exploit des processus vulnérables** pour activer le module.
6. Sélectionnez un mode de protection contre les exploits : **Bloquer** ou **Informer**.
7. Si nécessaire, décochez la case **Empêcher l'exploit des processus vulnérables** pour désactiver le module.
8. Enregistrez vos modifications.

Activation et désactivation de la protection de la mémoire

Kaspersky Embedded Systems Security bloque les processus externes qui tentent d'accéder aux processus du système. La protection de la mémoire des processus système est activée par défaut.

Comment activer ou désactiver la protection de la mémoire dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise de Kaspersky Embedded Systems Security et ouvrez les propriétés de la stratégie d'un double-clic.
3. Une fenêtre s'ouvre ; dans cette fenêtre, dans la liste des sections, sélectionnez **Protection en temps réel de l'ordinateur → Protection contre les Exploits**.
4. Cliquez sur **Paramètres**.
5. Sous l'onglet **Général**, cochez la case **Activer la protection de la mémoire des processus système**.
6. Le cas échéant, décochez la case **Activer la protection de la mémoire des processus système**.
7. Enregistrez vos modifications.

Comment activer ou désactiver la protection de la mémoire dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les Exploits**.
3. Dans la fenêtre principale de l'application, cliquez sur **Propriétés**.
4. Sous l'onglet **Général**, cochez la case **Activer la protection de la mémoire des processus système**.
5. Le cas échéant, décochez la case **Activer la protection de la mémoire des processus système**.
6. Enregistrez vos modifications.

Comment activer ou désactiver la protection de la mémoire dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Protection contre les Exploits** et cliquez sur le bouton **Configurer**.
5. Dans la fenêtre qui s'ouvre, dans le groupe **Protection de la mémoire des processus système**, cochez la case **Protection de la mémoire des processus système**.
6. Si nécessaire, décochez la case **Protection de la mémoire des processus système** pour désactiver la protection de la mémoire du processus système.
7. Enregistrez vos modifications.

Création de la liste des processus protégés

Par défaut, le module Protection contre les Exploits protège plusieurs processus. L'application peut générer automatiquement la liste des processus protégés. Vous pouvez également ajouter ou supprimer des processus manuellement.

Comment gérer la liste des processus protégés dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise de Kaspersky Embedded Systems Security et ouvrez les propriétés de la stratégie d'un double-clic.
3. Une fenêtre s'ouvre ; dans cette fenêtre, dans la liste des sections, sélectionnez **Protection en temps réel de l'ordinateur → Protection contre les Exploits**.
4. Cliquez sur **Paramètres**.
5. Sous l'onglet **Processus protégés**, sélectionnez l'une des options suivantes pour protéger les processus contre l'injection de code malveillant :
   - **Détecter automatiquement les processus protégés**. Si vous sélectionnez cette option, l'application crée automatiquement une liste de processus protégés.
   - **Protéger uniquement les processus de la liste ci-dessous**. Si vous sélectionnez cette option, vous pouvez sélectionner les processus que vous souhaitez protéger.
6. Si vous avez sélectionné **Protéger uniquement les processus de la liste ci-dessous**, vous pouvez modifier la liste des processus protégés de l'une des manières suivantes :
   - Si nécessaire, cliquez sur **Ajouter** et sélectionnez le processus que vous souhaitez ajouter à la liste des processus protégés.
   - Pour supprimer un processus de la liste des processus protégés créée, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

     Le bouton **Supprimer** devient accessible dès que vous avez sélectionné au moins un processus dans la liste.
7. Enregistrez vos modifications.

Comment gérer la liste des processus protégés à l'aide de la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, développez le nœud **Protection en temps réel de l'ordinateur**.
2. Sélectionnez le nœud enfant **Protection contre les Exploits**.
3. Dans la fenêtre principale de l'application, cliquez sur **Propriétés**.

4. Sous l'onglet **Processus protégés**, sélectionnez l'une des options suivantes pour protéger les processus contre l'injection de code malveillant :

   - **Détecter automatiquement les processus protégés**. Si vous sélectionnez cette option, l'application crée automatiquement une liste de processus protégés.

   - **Protéger uniquement les processus de la liste ci-dessous**. Si vous sélectionnez cette option, vous pouvez sélectionner les processus que vous souhaitez protéger.

5. Si vous avez sélectionné **Protéger uniquement les processus de la liste ci-dessous**, vous pouvez modifier la liste des processus protégés de l'une des manières suivantes :

   - Si nécessaire, cliquez sur **Ajouter** et sélectionnez le processus que vous souhaitez ajouter à la liste des processus protégés.

   - Pour supprimer un processus de la liste des processus protégés créée, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

     Le bouton **Supprimer** devient accessible dès que vous avez sélectionné au moins un processus dans la liste.

6. Enregistrez vos modifications.

Comment gérer la liste des processus protégés dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans la section **Protection en temps réel de l'ordinateur** → **Protection contre les Exploits** et cliquez sur le bouton **Configurer**.

5. Sous **Liste des processus protégés**, choisissez l'une des options suivantes pour protéger les processus contre l'injection de code malveillant :

   - **Détecter automatiquement les processus protégés**. Si vous sélectionnez cette option, l'application crée automatiquement une liste de processus protégés.

   - **Protéger uniquement les processus de la liste ci-dessous**. Si vous sélectionnez cette option, vous pouvez ajouter, modifier et supprimer les processus que vous souhaitez protéger.

6. Si vous avez sélectionné **Protéger uniquement les processus de la liste ci-dessous**, effectuez l'une des actions suivantes :

   - Cliquez sur **Ajouter** pour ouvrir la fenêtre **Processus protégé**, et dans cette fenêtre :

     a. Cochez la case **Processus protégé**.

     b. Dans le champ **Nom du processus**, saisissez le nom du processus.

     c. Enregistrez vos modifications.

- Si nécessaire, modifiez les paramètres du processus dans la liste des processus protégés. Pour ce faire, procédez comme suit :

  a. Sélectionnez un processus dans la liste des processus protégés.

  b. Cliquez sur **Modifier**. Le bouton **Modifier** devient accessible dès que vous avez sélectionné au moins un processus dans la liste.

  c. Dans la fenêtre **Processus protégé**, cochez ou décochez la case **Processus protégé**.

  d. Si nécessaire, modifiez le nom du processus dans le champ **Nom du processus**.

  e. Enregistrez vos modifications.

- Si nécessaire, vous pouvez supprimer un processus de la liste des processus protégés. Pour ce faire, procédez comme suit :

  a. Sélectionnez au moins un processus dans la liste des processus protégés.

  b. Cliquez sur **Supprimer**. Le bouton **Supprimer** devient accessible dès que vous avez sélectionné au moins un processus dans la liste.

7. Enregistrez vos modifications.

Réparation des actions malicieuses

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

Lors de la restauration des actions du programme malveillant dans le système d'exploitation, Kaspersky Embedded Systems Security effectue les actions suivantes :

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

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

  Kaspersky Embedded Systems Security ne restaure pas des sections et des clés de registre modifiées ou supprimées par l'application malveillante.
- **Activité système**
  - arrêt des processus lancés par l'application malveillante ;
  - arrêt des processus dans lesquels l'application malveillante s'est introduite ;

Kaspersky Embedded Systems Security ne restaure pas des processus arrêtés par l'application malveillante.

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

Une annulation des actions d'une application malveillante peut être déclenchée par le module Protection des fichiers en temps réel ou lors d'une Analyse à la demande.

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

Comment activer ou désactiver le module Réparation des actions malicieuses dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Protection en temps réel de l'ordinateur**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Réparation des actions malicieuses**.
5. La fenêtre **Réparation des actions malicieuses** s'ouvre sous l'onglet **Général**.
6. Réalisez une des opérations suivantes :
   - Cochez la case **Réparation des actions malicieuses** si vous souhaitez activer le module Réparation des actions malicieuses.
   - Décochez la case **Réparation des actions malicieuses** si vous souhaitez désactiver le module Réparation des actions malicieuses.
7. Cliquez sur le bouton **OK** dans la fenêtre **Réparation des actions malicieuses**.
8. Dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur le bouton **OK**.

Comment activer ou désactiver le module Réparation des actions malicieuses dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Réparation des actions malicieuses**.

6. La fenêtre **Réparation des actions malicieuses** s'ouvre.

7. Réalisez une des opérations suivantes :

   - Cochez la case **Réparation des actions malicieuses** si vous souhaitez activer le module Réparation des actions malicieuses.

   - Décochez la case **Réparation des actions malicieuses** si vous souhaitez désactiver le module Réparation des actions malicieuses.

8. Cliquez sur le bouton **OK** dans la fenêtre **Réparation des actions malicieuses**.

9. Dans la fenêtre **<Nom de la stratégie>**, cliquez sur le bouton **Enregistrer**.

Procédure d'activation ou de désactivation du module Réparation des actions malicieuses dans Kaspersky Embedded Systems Security Console

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Protection en temps réel de l'ordinateur → Réparation des actions malicieuses**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Réparation des actions malicieuses** s'ouvre sous l'onglet **Général**.

3. Réalisez une des opérations suivantes :

   - Cochez la case **Réparation des actions malicieuses** si vous souhaitez activer le module Réparation des actions malicieuses.

   - Décochez la case **Réparation des actions malicieuses** si vous souhaitez désactiver le module Réparation des actions malicieuses.

4. Cliquez sur le bouton **OK** dans la fenêtre **Réparation des actions malicieuses**.

Détection comportementale

Le module Détection comportementale récupère des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent intervenir avec plus d'efficacité. Le module Détection comportementale utilise des modèles de comportement d'applications dangereux. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Embedded Systems Security exécute la réaction choisie. La fonction de Kaspersky Embedded Systems Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

Activation et désactivation de la protection par chiffrement des dossiers locaux

Comment activer ou désactiver le module Détection comportementale dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
5. Cochez ou décochez la case **Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Général**.
7. Utilisez la case **Activer la protection des dossiers locaux contre le chiffrement externe** pour activer ou désactiver l'option. Si cette case est cochée, Kaspersky Embedded Systems Security répond aux activités malveillantes par l'action indiquée ci-dessous.
8. Sélectionnez l'action appropriée dans le groupe **Action exécutée lors de la détection d'une activité malveillante** :
   - **Supprimer**. Si cet élément est sélectionné, Kaspersky Embedded Systems Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application.
   - **Bloquer**. Si cet élément est sélectionné, Kaspersky Embedded Systems Security arrête l'application en cas de détection d'une activité malveillante de l'application.
   - **Informer**. Si vous avez choisi cette option, Kaspersky Embedded Systems Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.
9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer ou désactiver le module Détection comportementale dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Détection comportementale** et cliquez sur le bouton **Configurer**.

   La fenêtre **Détection comportementale** s'ouvre.
5. Utilisez la case **Activer la Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Général**.
7. Utilisez la case **Activer la protection des dossiers locaux contre le chiffrement externe** pour activer ou désactiver l'option. Si cette case est cochée, Kaspersky Embedded Systems Security répond aux activités malveillantes par l'action indiquée ci-dessous.
8. Sélectionnez l'action appropriée dans le groupe **Lors de la détection du chiffrement externe de dossiers partagés** :

   - **Supprimer**. Si cet élément est sélectionné, Kaspersky Embedded Systems Security supprime le fichier exécutable du programme malveillant et crée une copie de sauvegarde du fichier dans la sauvegarde, après avoir détecté une activité malveillante de l'application.
   - **Bloquer**. Si cet élément est sélectionné, Kaspersky Embedded Systems Security arrête l'application en cas de détection d'une activité malveillante de l'application.
   - **Informer**. Si vous avez choisi cette option, Kaspersky Embedded Systems Security, après avoir détecté l'activité malveillante de l'application ajoute les informations relatives à l'activité malveillante de cette application dans la liste des menaces actives.
9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer ou désactiver le module Détection comportementale dans la Console d'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Détection comportementale**.
2. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Behavior Detection** s'ouvre.
3. Cochez la case **Détection comportementale**.
4. Rendez-vous dans l'onglet **Général**.
5. Utilisez la case **Activer la protection des dossiers locaux contre le chiffrement externe** pour activer ou désactiver l'option. Si cette case est cochée, Kaspersky Embedded Systems Security répond aux activités malveillantes par l'action indiquée ci-dessous.

6. Sélectionnez l'action appropriée dans le groupe **Lors de la détection du chiffrement externe de dossiers partagés** :

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

   - **Bloquer**. Si cet élément est sélectionné, Kaspersky Embedded Systems Security arrête l'application en cas de détection d'une activité malveillante de l'application.

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

7. Enregistrez vos modifications.

Protection des dossiers partagés contre le chiffrement externe

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

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

En cas de détection d'une tentative de modification de fichiers dans des dossiers partagés, Kaspersky Embedded Systems Security effectue les actions suivantes :

- Bloque l'accès à la modification de fichiers pour la session à l'origine de l'activité malveillante (le fichier sera en lecture seule) ;

- Crée des copies de sauvegarde des fichiers modifiés ;

- Ajoute une entrée aux rapports de l'interface de l'application locale et envoie des informations sur l'activité malveillante détectée à Kaspersky Security Center ;

- Si le module Réparation des actions malicieuses est activé, l'application restaure les fichiers modifiés au départ des copies de sauvegarde.

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

Par défaut, la protection des dossiers partagés contre le chiffrement externe est activée et fonctionne conformément aux recommandations des experts de Kaspersky. Pour configurer cette fonctionnalité, vous pouvez créer une zone de protection et configurer des exclusions, si nécessaire. Par défaut, l'application identifie automatiquement les dossiers partagés et surveille l'activité des fichiers dans tous les dossiers. En cas de détection d'une tentative de chiffrement externe des fichiers dans les dossiers partagés, Kaspersky Embedded Systems Security bloque la session de l'utilisateur distant pendant une heure (par défaut).

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

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
5. Cochez ou décochez la case **Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
7. Utilisez la case **Protéger les dossiers partagés** pour activer ou désactiver l'option.
8. Sélectionnez l'action appropriée dans le groupe **Protection des dossiers partagés contre le chiffrement externe** :

   - **Bloquer la connexion pendant N min**. Si cette option est sélectionnée, lorsque Kaspersky Embedded Systems Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers (en lecture seule) pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, si une tentative de modification de fichiers dans les dossiers partagés est détectée, Kaspersky Embedded Systems Security ajoute des informations sur cette tentative de modification de fichiers dans les dossiers partagés à la liste des menaces actives, ajoute un enregistrement aux rapports de l'interface locale de l'application, et envoie à Kaspersky Security Center des informations relatives à la détection d'activités malveillantes.

9. Si nécessaire, créez une zone de protection et configurez les exclusions.

10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Détection comportementale** et cliquez sur le bouton **Configurer**.

   La fenêtre **Détection comportementale** s'ouvre.

5. Utilisez la case **Activer la Détection comportementale** pour activer ou désactiver le module.

6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

7. Utilisez la case **Activer la protection des dossiers partagés contre le chiffrement externe** pour activer ou désactiver l'option.

8. Sélectionnez l'action appropriée dans le groupe **Détection d'un chiffrement externe** :

   - **Bloquer la connexion**. Si cette option est sélectionnée, lorsque Kaspersky Embedded Systems Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers (en lecture seule) pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, si une tentative de modification de fichiers dans les dossiers partagés est détectée, Kaspersky Embedded Systems Security ajoute des informations sur cette tentative de modification de fichiers dans les dossiers partagés à la liste des menaces actives, ajoute un enregistrement aux rapports de l'interface locale de l'application, et envoie à Kaspersky Security Center des informations relatives à la détection d'activités malveillantes.

9. Si nécessaire, créez une zone de protection et configurez les exclusions.

10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer ou désactiver la protection des dossiers partagés contre le chiffrement externe dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur** → **Détection comportementale**.

2. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Behavior Detection** s'ouvre.

3. Cochez la case **Détection comportementale**.

4. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

5. Utilisez la case **Protéger les dossiers partagés** pour activer ou désactiver l'option.

6. Sélectionnez l'action appropriée dans le groupe **Protection des dossiers partagés contre le chiffrement externe** :

   - **Bloquer la connexion pendant N min**. Si cette option est sélectionnée, lorsque Kaspersky Embedded Systems Security détecte une tentative de modification des fichiers dans les dossiers partagés, il bloque l'accès à la modification des fichiers (en lecture seule) pour la session qui a initié l'activité malveillante et crée des copies de sauvegarde des fichiers modifiés.

     Si le module Réparation des actions malicieuses a été activé et que l'option **Bloquer la connexion pendant X minutes** a été sélectionné, les fichiers modifiés sont restaurés au départ des copies de sauvegarde.

   - **Informer**. Si cette option est sélectionnée, si une tentative de modification de fichiers dans les dossiers partagés est détectée, Kaspersky Embedded Systems Security ajoute des informations sur cette tentative de modification de fichiers dans les dossiers partagés à la liste des menaces actives, ajoute un enregistrement aux rapports de l'interface locale de l'application, et envoie à Kaspersky Security Center des informations relatives à la détection d'activités malveillantes.

7. Si nécessaire, créez une zone de protection et configurez les exclusions.

8. Enregistrez vos modifications.

Modification de la zone de protection

Une *zone de protection* est une liste de chemins d'accès aux dossiers partagés dans lesquels Kaspersky Embedded Systems Security contrôle l'activité des fichiers. Kaspersky Embedded Systems Security prend en charge les variables d'environnement et les caractères `*` et `?` lors de la saisie d'un masque : par défaut, l'application identifie automatiquement les dossiers partagés et suit l'activité des fichiers dans tous les dossiers.

L'exclusion d'un dossier de la zone de protection peut réduire le nombre de faux positifs si votre entreprise utilise le chiffrement des données lors de l'échange de fichiers à l'aide de dossiers partagés. Par exemple, le module Détection comportementale peut générer des faux positifs lorsque l'utilisateur traite des fichiers portant l'extension ENC dans un dossier partagé. Une telle activité correspond à un modèle comportemental typique de chiffrement externe. Si vous avez chiffré des fichiers dans un dossier partagé pour protéger des données, ajoutez ce dossier aux exclusions.

Vous pouvez également exclure des ordinateurs si vous souhaitez que les tentatives de chiffrement externe de la part de ces derniers soient ignorées.

Comment configurer la zone de protection dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
5. Cochez ou décochez la case **Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
7. Cliquez sur le bouton **Configurer** dans le groupe **Zone de protection**.
8. Dans la fenêtre qui s'ouvre, sélectionnez le mode **Seuls les dossiers partagés indiqués**.
9. Cliquez sur **Ajouter**.
10. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

    Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.

11. Cliquez sur **OK**.
12. Si nécessaire, définissez les exclusions de la zone de protection :

    a. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions**.

    b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

    c. Dans la fenêtre qui s'affiche, saisissez le chemin d'accès au dossier ou au fichier.

    Utilisez des masques :

    - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

    - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

    - Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

    Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

13. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer la zone de protection dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Détection comportementale** et cliquez sur le bouton **Configurer**.

   La fenêtre **Détection comportementale** s'ouvre.
5. Utilisez la case **Activer la Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
7. Sous les **Zone de protection**, sélectionnez le mode **Uniquement les dossiers partagés indiqués**.
8. Cliquez sur **Ajouter**.
9. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

   > Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.
10. Cliquez sur **OK**.
11. Si nécessaire, définissez les exclusions de la zone de protection :

    a. Cliquez sur le bouton **Ajouter** dans le groupe **Objet à exclure**.

    b. Dans la fenêtre qui s'affiche, saisissez le chemin d'accès au dossier ou au fichier.

    Utilisez des masques :

    - Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.
    - Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.
    - Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

12. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment configurer la zone de protection dans la Console de l'application

1. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
2. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
3. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Détection comportementale**.
4. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Behavior Detection** s'ouvre.
5. Cochez ou décochez la case **Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
7. Cliquez sur le bouton **Configurer** dans le groupe **Zone de protection**.
8. Dans la fenêtre qui s'ouvre, sélectionnez le mode **Seuls les dossiers partagés indiqués**.
9. Cliquez sur le bouton **Ajouter** dans le groupe **Zone de protection**.
10. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au dossier partagé que vous souhaitez inclure dans la zone de protection (par exemple, `C:\Share`).

    > Pour ajouter un dossier partagé à la zone de protection, utilisez un chemin d'accès local.

11. Cliquez sur **OK**.
12. Si nécessaire, définissez les exclusions de la zone de protection :

    a. Cliquez sur le bouton **Paramètres** dans le groupe **Exclusions**.

    b. Cliquez sur le bouton **Ajouter** dans la fenêtre **Exclusions selon un masque** qui s'affiche.

    c. Dans la fenêtre qui s'affiche, saisissez le chemin d'accès au dossier ou au fichier.

Utilisez des masques :

- Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers.

- Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide.

- Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.

Dans la zone de protection, vous pouvez exclure un objet de l'analyse sans le supprimer de la liste des objets. Pour ce faire, décochez la case à côté de l'objet.

13. Enregistrez vos modifications.

Ajout d'ordinateurs de confiance pour le chiffrement externe des données

Si votre organisation utilise le chiffrement externe des données dans son flux de travail d'échange de fichiers, vous devez créer une liste d'ordinateurs de confiance. Kaspersky Embedded Systems Security ne contrôle pas le chiffrement des données provenant des ordinateurs de confiance.

Sur les appareils protégés exécutant Windows XP ou Windows Server 2003, Kaspersky Embedded Systems Security surveillera les tentatives de chiffrement des dossiers partagés, même si vous ajoutez un ordinateur distant à la liste des ordinateurs de confiance.

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

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

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
5. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
6. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions d'adresses IP**.
7. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
8. Saisissez l'adresse IP ou le nom de l'ordinateur pour lequel les tentatives de chiffrement externe ne doivent pas être traitées.
9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Détection comportementale** et cliquez sur le bouton **Configurer**.

   La fenêtre **Détection comportementale** s'ouvre.
5. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
6. Cliquez sur le bouton **Ajouter** dans le groupe **Exclusions**.
7. Saisissez l'adresse IP ou le nom de l'ordinateur pour lequel les tentatives de chiffrement externe ne doivent pas être traitées.
8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment ajouter un ordinateur de confiance pour le chiffrement externe des données dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Détection comportementale**.
2. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Behavior Detection** s'ouvre.
3. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

4. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions d'adresses IP**.
5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
6. Saisissez l'adresse IP ou le nom de l'ordinateur pour lequel les tentatives de chiffrement externe ne doivent pas être traitées.
7. Enregistrez vos modifications.

Configuration de la période de blocage d'un ordinateur non fiable

Un *ordinateur non fiable* est un ordinateur distant qui mène des activités malveillantes ou qui chiffre des données. Par défaut, Kaspersky Embedded Systems Security bloque la session de l'utilisateur distant pendant une heure. À l'expiration de la période de blocage, Kaspersky Embedded Systems Security supprime l'ordinateur de la liste de blocage et rétablit l'accès au dossier partagé.

Comment configurer la période de blocage de l'ordinateur douteux dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.
4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.
5. Cochez ou décochez la case **Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.
7. Sous **Lors de la détection du chiffrement externe de dossiers partagés**, configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.
8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer la période de blocage d'un ordinateur douteux dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Détection comportementale** et cliquez sur le bouton **Configurer**.

   La fenêtre **Détection comportementale** s'ouvre.
5. Utilisez la case **Activer la Détection comportementale** pour activer ou désactiver le module.
6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

7. Sous **Détection d'un chiffrement externe**, configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.

8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer la période de blocage d'un ordinateur douteux dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Détection comportementale**.

2. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Behavior Detection** s'ouvre.

3. Cochez la case **Détection comportementale**.

4. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

5. Sous **Protection des dossiers partagés contre le chiffrement externe**, configurez la période de blocage d'un ordinateur non fiable menant des activités malveillantes ou chiffrant des données.

6. Enregistrez vos modifications.

Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe

Vous pouvez exporter la liste des exclusions dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions ou pour procéder à la migration de la liste vers un autre serveur.

Comment exporter et importer une liste d'exclusions dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur**.

4. Dans la section **Détection comportementale**, cliquez sur **Paramètres**.

5. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

6. Cliquez sur le bouton **Configurer** dans le groupe **Exclusions d'adresses IP**.

7. Pour exporter la liste des règles, procédez comme suit :

   a. Si nécessaire, sélectionnez les exclusions que vous souhaitez exporter.

   b. Cliquez sur le bouton , puis sélectionnez le mode d'exportation : exportez toute la liste des exclusions, ou uniquement une sélection d'exclusions.

c. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier au format XML dans lequel vous voulez exporter la liste des exclusions et choisissez le dossier dans lequel vous souhaitez enregistrer ce fichier.

d. Enregistrez le fichier.

Kaspersky Embedded Systems Security exporte la liste des exclusions dans un fichier XML.

8. Pour importer la liste des exclusions, procédez comme suit :

a. Appuyez sur le bouton → **Importer**.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

b. Ouvrez le fichier.

Kaspersky Embedded Systems Security importe les exclusions.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment exporter et importer une liste d'exclusions dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Protection en temps réel de l'ordinateur** → **Détection comportementale** et cliquez sur le bouton **Configurer**.

La fenêtre **Détection comportementale** s'ouvre.

5. Utilisez la case **Activer la Détection comportementale** pour activer ou désactiver le module.

6. Rendez-vous dans l'onglet **Protection des dossiers partagés**.

7. Pour exporter la liste des exclusions dans le groupe **Exclusions**, procédez comme suit :

a. Si nécessaire, sélectionnez les exclusions que vous souhaitez exporter.

b. Cliquez sur le bouton **Exporter**, puis sélectionnez le mode d'exportation : exportez toute la liste des exclusions, ou uniquement une sélection d'exclusions.

c. Enregistrez le fichier.

Kaspersky Embedded Systems Security exporte la liste des exclusions dans un fichier XML.

8. Pour importer la liste d'exclusions dans le groupe **Exclusions**, procédez comme suit :

a. Cliquez sur le bouton **Importer** et sélectionnez le mode d'importation : ajouter ou remplacer.

b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

c. Ouvrez le fichier.

Kaspersky Embedded Systems Security importe les exclusions selon le mode sélectionné.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Protection contre les menaces réseau

Le module Protection contre les menaces réseau analyse le trafic réseau entrant à la recherche d'activités typiques des attaques réseau. En cas de détection d'une tentative d'attaque réseau ciblant votre ordinateur, Kaspersky Embedded Systems Security bloque l'activité réseau de l'ordinateur attaquant. Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de l'application. La liste des attaques réseau que le module Protection contre les menaces réseau détecte est enrichie lors de la mise à jour des bases et des modules de l'application.

Par défaut, la tâche *Protection contre les menaces réseau* s'exécute en mode **Bloquer**. Dans ce mode, Kaspersky Embedded Systems Security bloque la connexion aux ordinateurs qui affichent une activité typique des attaques réseau et, dans certains cas, ajoute les adresses IP de ces ordinateurs à la liste des sessions réseau bloquées.

Vous pouvez afficher la liste des ordinateurs douteux dans le Stockage des ordinateurs bloqués.

Kaspersky Embedded Systems Security efface la liste du groupe lorsque l'application est redémarrée et lorsque les paramètres de la Protection contre les menaces réseau sont modifiés.

Vous pouvez restaurer l'accès aux hôtes bloqués et spécifier le nombre de jours, d'heures et de minutes au terme desquels ces hôtes peuvent à nouveau accéder aux ressources de fichier réseau après leur blocage en configurant les paramètres de stockage des hôtes bloqués.

Les adresses IP des hôtes affichant une activité typique des attaques réseau sont supprimées de la liste des ordinateurs douteux dans les cas suivants :

- Kaspersky Embedded Systems Security est désinstallé.
- L'adresse IP a été supprimée manuellement de la liste des hôtes douteux.
- Le délai de blocage des hôtes a expiré.
- Le mode **Bloquer** a été désactivé.

Activation et configuration de la Protection contre les menaces réseau

Comment activer et configurer la Protection contre les menaces réseau dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité réseau**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection contre les menaces réseau**.
5. Dans la fenêtre qui s'ouvre, cochez la case **Protection contre les menaces réseau**.

6. Sélectionnez le mode de tâche dans la section **Operating mode** :

   - **Bloquer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, bloque la connexion aux ordinateurs qui affichent une telle activité et, dans certains cas, ajoute les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre également dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

   - **Inform**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, mais ne bloque pas la connexion aux ordinateurs qui affichent une telle activité et n'ajoute pas les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

7. Utilisez la case **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection des attaques correspondantes.

8. Le cas échéant, cochez la case **Block attacking devices for N min**.

9. Dans le groupe **MAC spoofing protection**, cochez ou décochez la case **Enable protection against MAC spoofing attacks**.

10. Si nécessaire, vous pouvez ajouter des exclusions au blocage.

11. Enregistrez vos modifications.

Comment activer et configurer la Protection contre les menaces réseau dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Choisissez **Contrôle de l'activité réseau** → **Protection contre les menaces réseau**.

5. Sous l'onglet **Général**, cochez la case **Activer la Protection contre les menaces réseau**.

6. Sélectionnez le mode de fonctionnement de la tâche :

   - **Bloquer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, bloque la connexion aux ordinateurs qui affichent une telle activité et, dans certains cas, ajoute les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre également dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

   - **Informer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, mais ne bloque pas la connexion aux ordinateurs qui affichent une telle activité et n'ajoute pas les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

7. Utilisez la case **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection des attaques correspondantes.

8. Le cas échéant, cochez la case **Bloquer les appareils attaquants pendant N min**.

9. Cochez ou décochez la case **Activer la protection contre les attaques MAC spoofing**.

10. Si nécessaire, vous pouvez ajouter des exclusions au blocage.

11. Enregistrez vos modifications.

Comment activer et configurer la Protection contre les menaces réseau dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Protection en temps réel de l'ordinateur → Protection contre les menaces réseau**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Propriétés : Protection contre les menaces réseau** s'ouvre.

3. Cochez la case **Protection contre les menaces réseau**.

4. Sélectionnez le mode de tâche dans la section **Mode de fonctionnement** :

   - **Bloquer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, bloque la connexion aux ordinateurs qui affichent une telle activité et, dans certains cas, ajoute les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre également dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

   - **Informer**. Si ce mode est sélectionné, Kaspersky Embedded Systems Security analyse le trafic réseau entrant à la recherche d'une activité typique des attaques réseau, mais ne bloque pas la connexion aux ordinateurs qui affichent une telle activité et n'ajoute pas les adresses IP des ordinateurs à la liste des sessions réseau bloquées. L'application enregistre dans le journal du module les événements relatifs à l'activité détectée typique d'attaques réseau.

5. Utilisez la case **Traiter l'analyse des ports et l'inondation des réseaux comme des attaques** pour activer ou désactiver la détection des attaques correspondantes.

6. Le cas échéant, cochez la case **Bloquer les appareils attaquants pendant N min**.

7. Dans le groupe **MAC spoofing protection**, cochez ou décochez la case **Activer la protection contre les attaques MAC spoofing**.

8. Si nécessaire, vous pouvez ajouter des exclusions au blocage.

9. Enregistrez vos modifications.

Création d'une exclusion du blocage

Kaspersky Embedded Systems Security peut reconnaitre une attaque réseau et bloquer une connexion réseau non sécurisée qui transmet un grand nombre de paquets (par exemple, provenant de caméras de surveillance). Pour travailler avec des appareils de confiance, vous pouvez ajouter les adresses IP de ces appareils à la liste des exclusions. Vous pouvez également sélectionner le protocole et le port utilisés pour la communication et autoriser des activités réseau spécifiques.

La possibilité de sélectionner des protocoles et des ports pour les exclusions a été ajoutée dans Kaspersky Embedded Systems Security 4.0. Assurez-vous que l'application et le plug-in d'administration sont mis à jour vers la version 4.0 ou ultérieure. Si vous utilisez une version antérieure de l'application ou du plug-in d'administration, Kaspersky Embedded Systems Security peut autoriser les activités réseau uniquement par adresse IP.

Comment créer une exclusion du blocage dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité réseau**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection contre les menaces réseau**.
   La fenêtre **Protection contre les menaces réseau** s'ouvre.
5. Rendez-vous dans l'onglet **Exclusions**.
6. Cochez la case **Ne pas contrôler les adresses exclues** pour empêcher Kaspersky Embedded Systems Security d'analyser le trafic réseau entrant à la recherche d'adresses IP exclues.
7. Cliquez sur **Ajouter**.
8. Dans la fenêtre **Exclusion**, saisissez l'adresse IP de l'appareil à partir duquel les attaques réseau ne seront pas bloquées.
9. Si nécessaire, sélectionnez le protocole et spécifiez les ports via lesquels les données sont transmises.
10. Cliquez sur le bouton **OK**.
11. Suivez les étapes C à F pour chaque exclusion ajoutée.
12. Enregistrez vos modifications.

Comment créer une exclusion du blocage dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez **Contrôle de l'activité réseau → Protection contre les menaces réseau** et cliquez sur le bouton **Configurer**.

5. Rendez-vous dans l'onglet **Exclusions**.

6. Cochez la case **Ne pas contrôler les adresses IP exclues** pour empêcher Kaspersky Embedded Systems Security d'analyser le trafic réseau entrant à la recherche d'adresses IP exclues.

7. Cliquez sur **Ajouter**.

8. Dans la fenêtre **Ajouter des exclusions**, saisissez l'adresse IP de l'appareil à partir duquel les attaques réseau ne seront pas bloquées.

9. Si nécessaire, sélectionnez le protocole et spécifiez les ports via lesquels les données sont transmises.

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

11. Suivez les étapes C à F pour chaque exclusion ajoutée.

12. Enregistrez vos modifications.

Comment créer une exclusion du blocage dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez le nœud **Protection en temps réel de l'ordinateur → Protection contre les menaces réseau**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Propriétés : Protection contre les menaces réseau** s'ouvre.

3. Rendez-vous dans l'onglet **Exclusions**.

4. Cochez la case **Ne pas contrôler les adresses exclues** pour empêcher Kaspersky Embedded Systems Security d'analyser le trafic réseau entrant à la recherche d'adresses IP exclues.

5. Cliquez sur **Ajouter**.

6. Dans la fenêtre **Exclusion**, saisissez l'adresse IP de l'appareil à partir duquel les attaques réseau ne seront pas bloquées.

7. Si nécessaire, sélectionnez le protocole et spécifiez les ports via lesquels les données sont transmises.

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

9. Suivez les étapes C à F pour chaque exclusion ajoutée.

10. Enregistrez vos modifications.

Exportation et importation d'une liste d'exclusions de la protection des dossiers partagés contre le chiffrement externe

Vous pouvez exporter la liste des exclusions dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'adresses du même type. Vous pouvez également utiliser la fonction d'exportation/importation pour sauvegarder la liste des exclusions ou pour procéder à la migration de la liste vers un autre serveur.

Comment exporter et importer une liste d'exclusions dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité réseau**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection contre les menaces réseau**.

   La fenêtre **Protection contre les menaces réseau** s'ouvre.
5. Rendez-vous dans l'onglet **Exclusions**.
6. Pour exporter la liste des règles, exécutez une des actions suivantes :

   - À l'aide des cases, sélectionnez les exclusions que vous souhaitez exporter. Cliquez sur la flèche et, dans la liste déroulante, sélectionnez **Exporter la sélection**.
   - Pour exporter la liste complète des exclusions, cliquez sur la flèche et, dans la liste déroulante, sélectionnez **Exporter**.

     Kaspersky Embedded Systems Security enregistre le fichier networkExclusions.xml dans le dossier de téléchargement standard.
7. Pour importer la liste des exclusions, procédez comme suit :

   a. Cliquez sur la flèche et sélectionnez **Importer**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

   c. Ouvrez le fichier.

   Si l'ordinateur dispose déjà d'une liste d'exclusions, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.
8. Enregistrez vos modifications.

Comment exporter et importer une liste d'exclusions dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Protection contre les menaces réseau** et cliquez sur le bouton **Configurer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Exclusions**.
6. Pour exporter la liste des règles, procédez comme suit :

   a. Si nécessaire, sélectionnez les exclusions que vous souhaitez exporter.

   b. Cliquez sur le bouton **Exporter**, puis sélectionnez le mode d'exportation : exportez toute la liste des exclusions, ou uniquement une sélection d'exclusions.

   c. Cliquez sur **Exporter**.

   Kaspersky Embedded Systems Security enregistre le fichier networkExclusions.xml dans le dossier de téléchargement standard.
7. Pour importer la liste des exclusions, procédez comme suit :

   a. Cliquez sur le bouton **Importer** et sélectionnez un mode d'importation : **Ajouter aux entrées existantes** ou **Remplacer les entrées existantes**.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des exclusions.

   c. Ouvrez le fichier.

   Kaspersky Embedded Systems Security importe les exclusions selon le mode sélectionné.
8. Enregistrez vos modifications.

Analyseur AMSI

Pendant l'exécution de la tâche Scanner AMSI, Kaspersky Embedded Systems Security contrôle l'exécution des scripts créés à l'aide des technologies de création de scripts Microsoft Windows (Active Scripting) telles que VBScript ou JScript. L'application peut également traiter les scripts PowerShell et les scripts exécutés dans les applications Microsoft Office sur les systèmes d'exploitation dotés de l'interface de l'Antimalware Scan Interface (AMSI).

AMSI permet aux applications et aux services de s'intégrer à n'importe quelle application de lutte contre les applications malveillantes installée sur l'appareil afin que tous les scripts exécutés soient interceptés et analysés par la solution anti-applications malveillantes. Vous trouverez plus d'informations sur la fonctionnalité AMSI sur le site de Microsoft.

Dans les paramètres du module, vous pouvez autoriser ou refuser l'exécution de scripts dangereux. Si Kaspersky Embedded Systems Security identifie un script comme dangereux, il bloque ou autorise l'exécution du script en fonction de l'action que vous avez sélectionnée. Si vous sélectionnez l'action **Bloquer**, l'application bloque les scripts dangereux et autorise les autres scripts.

Kaspersky Embedded Systems Security prend en charge la technologie AMSI dans Microsoft Windows 10 et Microsoft Windows Server 2016 ou versions ultérieures.

Activation et désactivation du Scanner AMSI

Comment activer ou désactiver le Scanner AMSI dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Protection en temps réel de l'ordinateur**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Scanner AMSI**.
   La fenêtre **Scanner AMSI** s'ouvre sous l'onglet **Général**.
5. Réalisez une des opérations suivantes :
   - Cochez la case **Scanner AMSI** si vous souhaitez activer le Scanner AMSI.
   - Décochez la case **Scanner AMSI** si vous souhaitez désactiver le Scanner AMSI.
6. Enregistrez vos modifications.

Comment activer le Scanner AMSI dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Protection en temps réel de l'ordinateur → Scanner AMSI**.
2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.
   La fenêtre **Scanner AMSI** s'ouvre sous l'onglet **Général**.

3. Réalisez une des opérations suivantes :

   - Cochez la case **Scanner AMSI** si vous souhaitez activer le Scanner AMSI.
   - Décochez la case **Scanner AMSI** si vous souhaitez désactiver le Scanner AMSI.

4. Cliquez sur le bouton **OK** dans le groupe **Scanner AMSI**.

Comment activer le scanner AMSI dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur le bouton **Configurer** dans le groupe **Scanner AMSI**.
   La fenêtre **Scanner AMSI** s'ouvre.
6. Réalisez une des opérations suivantes :

   - Cochez la case **Scanner AMSI** si vous souhaitez activer le Scanner AMSI.
   - Décochez la case **Scanner AMSI** si vous souhaitez désactiver le Scanner AMSI.

7. Enregistrez vos modifications.

Paramètres du Scanner AMSI

Comment configurer les paramètres du Scanner AMSI dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Protection en temps réel de l'ordinateur**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Scanner AMSI**.
   La fenêtre **Scanner AMSI** s'ouvre sous l'onglet **Général**.
5. Sélectionnez l'action que Kaspersky Embedded Systems Security doit effectuer lorsqu'un script dangereux est exécuté :

   - **Informer**. L'application autorise l'exécution de scripts probablement dangereux. L'événement correspondant est consigné dans le journal des tâches.
   - **Bloquer**. L'application bloque les scripts probablement dangereux.

6. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets de distribution ou fichiers au format Office.

7. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Pour empêcher que le module Scanner AMSI ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés volumineux** et indiquez la valeur requise dans le champ **Taille maximale du fichier (Mo)**. Le module Scanner AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.

   - Pour autoriser le module Scanner AMSI à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés volumineux**.

   Le module Scanner AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.

8. Cliquez sur le bouton **OK** dans le groupe **Scanner AMSI**.

9. Dans la fenêtre **Propriétés : <Nom de la stratégie>**, cliquez sur le bouton **OK**.

Comment configurer les paramètres du Scanner AMSI dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Protection en temps réel de l'ordinateur → Scanner AMSI**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Scanner AMSI** s'ouvre sous l'onglet **Général**.

3. Sélectionnez l'action que Kaspersky Embedded Systems Security doit effectuer lorsqu'un script dangereux est exécuté :

   - **Informer**. L'application autorise l'exécution de scripts probablement dangereux. L'événement correspondant est consigné dans le journal des tâches.

   - **Bloquer**. L'application bloque les scripts probablement dangereux.

4. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets de distribution ou fichiers au format Office.

5. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Pour empêcher que le module Scanner AMSI ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés volumineux** et indiquez la valeur requise dans le champ **Taille maximale du fichier (Mo)**. Le module Scanner AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.

   - Pour autoriser le module Scanner AMSI à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés volumineux**.

Le module Scanner AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.

6. Cliquez sur le bouton **OK** dans le groupe **Scanner AMSI**.

Comment configurer les paramètres du Scanner AMSI dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Protection en temps réel de l'ordinateur**.
5. Cliquez sur le bouton **Configurer** dans le groupe **Scanner AMSI**.

   La fenêtre **Scanner AMSI** s'ouvre.
6. Sélectionnez l'action que Kaspersky Embedded Systems Security doit effectuer lorsqu'un script dangereux est exécuté :

   - **Informer**. L'application autorise l'exécution de scripts probablement dangereux. L'événement correspondant est consigné dans le journal des tâches.
   - **Bloquer**. L'application bloque les scripts probablement dangereux.
7. Dans le groupe **Analyse des fichiers composés**, indiquez les types de fichiers composés que vous souhaitez analyser : archives, paquets de distribution ou fichiers au format Office.
8. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Pour empêcher que le module Scanner AMSI ne décompresse des fichiers composés de grande taille, cochez la case **Ne pas décompresser les fichiers composés volumineux** et indiquez la valeur requise dans le champ **Taille maximale du fichier (Mo)**. Le module Scanner AMSI ne va pas décompresser les fichiers composés dont la taille est supérieure à la valeur indiquée.
   - Pour autoriser le module Scanner AMSI à décompresser les fichiers composés de grande taille, décochez la case **Ne pas décompresser les fichiers composés volumineux**.

   Le module Scanner AMSI analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompresser les fichiers composés volumineux** soit cochée ou non.
9. Cliquez sur le bouton **OK** dans la fenêtre **Scanner AMSI**.
10. Dans la fenêtre **<Nom de la stratégie>**, cliquez sur le bouton **Enregistrer**.

Contrôle du lancement des applications

Le module Contrôle du lancement des applications de Kaspersky Embedded Systems Security protège les appareils contre le lancement d'applications non autorisées. Le Contrôle du lancement des applications repose sur le principe Interdire par défaut, ce qui signifie que toute application qui n'est pas autorisée dans les paramètres du module sera bloquée automatiquement. Vous pouvez autoriser le lancement d'applications en créant des règles d'autorisation du module pour celles-ci.

Lorsque les règles du Contrôle du lancement des applications sont créées de manière aussi exhaustive que possible, Kaspersky Embedded Systems Security bloque le lancement de toute nouvelle application qui n'a pas été vérifiée par l'administrateur du réseau local de l'organisation, tout en garantissant le fonctionnement du système d'exploitation et des applications vérifiées dont les utilisateurs ont besoin pour remplir leurs fonctions. Vous pouvez obtenir des informations sur les applications installées sur les appareils protégés à l'aide de la tâche *Générateur de règles pour le Contrôle du lancement des applications*.

Si le module Contrôle du lancement des applications est activé, Kaspersky Embedded Systems Security intercepte chaque événement du système d'exploitation lié à une demande de création d'un processus qui se produit lors du lancement d'un fichier exécutable sur un appareil protégé. L'application collecte ensuite des informations sur le fichier exécutable, le script ou le package MSI en cours de lancement et les compare aux conditions de déclenchement des règles du Contrôle du lancement des applications. Si toutes les conditions d'au moins une règle d'autorisation sont remplies, Kaspersky Embedded Systems Security autorise le lancement de l'application. Si l'application en cours de lancement ne remplit les conditions d'aucune règle d'autorisation ou si une règle de blocage est déclenchée, Kaspersky Embedded Systems Security bloque la tentative de lancement de l'application en annulant la création du processus.

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

Le module Contrôle du lancement des applications peut fonctionner dans un des deux modes suivants :

- **Bloquer**. Kaspersky Embedded Systems Security contrôle le lancement d'applications à l'aide des règles du Contrôle du lancement des applications. La zone d'application des règles du Contrôle du lancement des applications peut être définie dans les paramètres généraux du module Contrôle du lancement des applications. Si une application répond aux règles du Contrôle du lancement des applications, mais qu'aucune des règles ne correspond à la zone d'action des règles du Contrôle du lancement des applications, l'exécution de cette application est bloquée.

  Il est interdit d'exécuter des applications qui ne sont pas couvertes par les règles du Contrôle du lancement des applications.

  Il est impossible de lancer le module Contrôle du lancement des applications en mode Actif, si aucune règle du Contrôle du lancement des applications n'a été créée ou si plus de 65 535 règles du Contrôle du lancement des applications existent pour un appareil protégé.

- **Informer**. Kaspersky Embedded Systems Security autorise le lancement de toutes les applications. Sont enregistrées uniquement des informations relatives à tous les lancements d'applications, aux règles qui couvrent les applications lancées, et aux actions qui seraient effectuées si la tâche était exécutée dans le mode **Bloquer**. Il s'agit du mode par défaut.

Lorsque vous créez des règles du Contrôle du lancement des applications, nous vous recommandons de veiller à ce qu'elles n'empêchent pas l'exécution des applications de votre système d'exploitation.

Kaspersky Embedded Systems Security intercepte également les processus lancés sous le Sous-système Windows pour Linux (sauf les scripts exécutés à partir du shell UNIX™ ou d'interpréteurs de ligne de commande). Pour ces processus, le module Contrôle du lancement des applications applique les actions définies par la configuration actuelle. La tâche *Générateur de règles pour le Contrôle du lancement des applications* détecte les lancements de l'application et génère les règles correspondantes pour les applications exécutées sous le Sous-système Windows pour Linux.

À propos des règles du Contrôle du lancement des applications

Principe de fonctionnement des règles du Contrôle du lancement des applications

Le fonctionnement des règles du Contrôle du lancement des applications est basé sur les modules suivantes :

- Type de règle.

  Les règles du Contrôle du lancement des applications peuvent autoriser ou interdire le lancement des applications. Pour cette raison, il peut s'agir de règles *d'autorisation* ou de règles *d'interdiction*.

- Zone d'application des règles.

  Les règles du Contrôle du lancement des applications peuvent s'appliquer aux *fichiers exécutables des applications*, aux *scripts* et aux *paquets MSI*.

- Condition de déclenchement de la règle.

  Les règles du Contrôle du lancement des applications régissent le lancement de fichiers qui remplissent au moins l'une des conditions de déclenchement spécifiées dans les paramètres des règles. Par exemple, les fichiers exécutables sont signés avec le *certificat numérique* spécifié, possèdent le *hachage SHA256* spécifié, se trouvent à l'emplacement *chemin d'accès* spécifié, et correspondent aux arguments de *ligne de commande* spécifiés. Vous devez ajouter au moins une condition de déclenchement de la règle. Dans le cas contraire, la règle du Contrôle du lancement des applications n'est pas ajoutée.

- Exclusions de la règle.

  Vous pouvez configurer des exclusions pour la règle du Contrôle du lancement des applications, qui peuvent être basées sur les mêmes critères que les conditions de déclenchement de la règle. Des exclusions des règles du Contrôle du lancement des applications peuvent se justifier pour certaines règles d'autorisation : par exemple, si vous souhaitez permettre aux utilisateurs de lancer les applications depuis le chemin C:\Windows, mais que vous souhaitez interdire l'exécution du fichier Regedit.exe.

- Utilisateur ou groupe d'utilisateurs.

  Les règles du Contrôle du lancement des applications contrôlent les lancements des applications définies par l'utilisateur et / ou le groupe d'utilisateurs spécifié.

Lors de la création de règles du Contrôle du lancement des applications, nous vous recommandons de vous assurer que les nouvelles règles ne bloquent pas l'exécution des applications de votre système d'exploitation.

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 manuellement.
- Créer et ajouter des règles automatiquement.
- Supprimer.
- Importer et exporter.
- Filtrez la liste des règles.

À propos du contrôle de la distribution des logiciels

Générer un Contrôle du lancement des applications peut s'avérer plus compliqué si vous souhaitez contrôler la distribution des logiciels. Par exemple, il se peut que vous souhaitiez le faire sur des appareils protégés où les logiciels installés sont automatiquement mis à jour à intervalles réguliers. Dans ce cas, la liste de règles d'autorisation doit être mise à jour après chaque mise à jour de logiciel afin que les fichiers juste créés soient pris en compte dans les paramètres du module Contrôle du lancement des applications. Pour simplifier le contrôle du lancement dans les scénarios de distribution des logiciels, vous pouvez utiliser le Contrôle de la distribution des logiciels.

Un *paquet d'installation* (ci-après appelé « paquet ») représente une ou plusieurs applications à installer sur un appareil protégé. Un paquet d'installation peut également contenir des mises à jour et des commandes distinctes.

Le sous-système Contrôle de la distribution des logiciels est mis en œuvre en tant que liste supplémentaire d'exclusions. Quand un paquet d'installation est ajouté à la liste, il devient un paquet de confiance. Le décompression est autorisé pour les paquets de confiance, et le lancement automatique est autorisé pour les applications installées ou mises à jour à partir de paquets de confiance. Les fichiers extraits peuvent hériter de l'attribut de confiance du paquet de distribution principal. Un *paquet de distribution principal* est un paquet qui a été ajouté à la liste d'exclusions du Contrôle de la distribution des logiciels par l'utilisateur et qui est devenu un paquet de confiance.

Kaspersky Embedded Systems Security ne contrôle que le cycle complet de distribution des applications et ne peut pas traiter correctement le lancement des fichiers qui sont modifiés par un paquet de confiance si, lors du premier lancement du paquet, le Contrôle de la distribution des logiciels est désactivé ou si le module Contrôle du lancement des applications n'est pas installé.

Pour utiliser le Contrôle de la distribution des logiciels, vous devez activer la fonctionnalité **Appliquer des règles aux fichiers exécutables** dans les paramètres généraux du module Contrôle du lancement des applications.

Cache de la distribution des logiciels

Kaspersky Embedded Systems Security établit le rapport entre les paquets de confiance et les fichiers créés lors de la distribution des logiciels à l'aide d'un cache de la distribution des logiciels généré automatiquement (ci-après appelé « cache de distribution »). Au premier lancement d'un paquet, Kaspersky Embedded Systems Security détecte tous les fichiers créés par ce paquet lors de du processus de distribution de logiciels et stocke les sommes de contrôles et les chemins d'accès des fichiers dans le cache de distribution. Ensuite, par défaut, tous les fichiers contenant des informations enregistrées dans le cache de distribution sont autorisés à démarrer.

Vous ne pouvez pas réviser, supprimer ou modifier manuellement le cache de distribution via l'interface utilisateur. Le cache est rempli et contrôlé par Kaspersky Embedded Systems Security.

Vous pouvez exporter le cache de distribution dans un fichier de configuration (au format XML) ou supprimer le cache de distribution via la ligne de commande.

Kaspersky Embedded Systems Security met à jour le cache de distribution toutes les 24 heures. En cas de modification de la somme de contrôle d'un fichier qui était autorisé, l'application supprime l'enregistrement de ce fichier dans le cache de distribution. Si le module Contrôle du lancement des applications fonctionne en mode Actif, les tentatives de lancement ultérieures de ce fichier sont bloquées. Si le chemin complet d'accès au fichier précédemment autorisé est modifié, les tentatives ultérieures de démarrer ce fichier ne seront pas bloquées car la somme de contrôle est stockée dans le cache de distribution.

Traitement des fichiers extraits

Les fichiers extraits et les paquets créés par un paquet de distribution de confiance principal (au premier niveau d'imbrication) acquièrent l'attribut de confiance quand leurs sommes de contrôle sont ajoutées au cache de distribution lorsque le paquet de distribution de logiciels de la liste d'exclusions est ouvert pour la première fois. Par conséquent, le paquet de distribution proprement dit et tous les fichiers inclus sont également de confiance.

Par exemple, si test.msi, un paquet contenant plusieurs paquets et applications, est ajouté à la liste des exclusions et que la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance** est activée, tous les paquets et applications contenus dans le paquet test.msi peuvent être décompressés et exécutés, même s'ils contiennent d'autres fichiers imbriqués. Ce scénario est valable pour les fichiers extraits sur tous les niveaux imbriqués.

Si le paquet test.msi est ajouté à la liste des exclusions et si la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance** est désactivée, l'application assigne l'attribut de confiance uniquement aux paquets et aux fichiers exécutables qui ont été extraits directement du paquet de confiance (au premier niveau d'imbrication). Les sommes de contrôle de ces fichiers sont stockées dans le cache de distribution. Tous les fichiers imbriqués au second niveau et plus sont bloqués par le principe Interdire par défaut.

Les fichiers extraits conservent l'attribut de confiance après le redémarrage du système d'exploitation.

Pour supprimer l'attribut d'héritage de tous les fichiers extraits, vous devez supprimer le cache de distribution et désactiver la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance** avant d'exécuter de nouveau le paquet d'installation de confiance.

Utilisation de la liste des règles du Contrôle du lancement des applications

La liste des paquets du Contrôle de la distribution des logiciels est une liste d'exclusions, ce qui amplifie, mais ne remplace pas la liste générale de règles de contrôle du lancement des applications.

Les règles d'interdiction de contrôle du lancement des applications a la priorité la plus élevé : la décompression des paquets de confiance et le démarrage de fichiers nouveaux ou modifiés sont bloqués si ces paquets est fichiers sont affectés par les règles d'interdiction du contrôle du lancement des applications.

Les exclusions de contrôle de la distribution des logiciels sont appliquées à la fois pour les paquets de confiance et les fichiers créés ou modifiés par ces paquets si aucune règle d'interdiction dans la liste de contrôle du lancement des applications n'est appliquée pour ces paquets et fichiers.

À propos de la Génération des règles du Contrôle du lancement des applications

Vous pouvez créer des listes de règles du Contrôle du lancement des applications à l'aide de tâches et de stratégies de Kaspersky Security Center simultanément pour tous les appareils protégés et groupes d'appareils protégés du réseau de l'organisation. Les scénarios énumérés ci-dessous sont recommandés si le réseau de l'organisation ne comporte pas une machine modèle et si vous n'êtes pas en mesure de créer une liste de règles d'autorisation sur la base des applications installées sur cette machine modèle.

Vous pouvez exécuter localement la tâche *Générateur de règles pour le Contrôle du lancement des applications* via la Console de l'application pour créer une liste de règles basées sur les applications exécutées sur un seul appareil protégé.

Vous pouvez créer des listes de règles du Contrôle du lancement des applications dans Kaspersky Security Center d'une des manières suivantes :

- À l'aide de la tâche de groupe *Générateur de règles pour le Contrôle du lancement des applications*.

  Selon les paramètres définis, la tâche *Générateur de règles pour le Contrôle du lancement des applications* peut collecter des informations sur les applications en cours d'exécution sur les appareils protégés, ainsi que sur les fichiers exécutables et les scripts situés dans les zones indiquées. Sur la base des informations collectées, la tâche génère une liste de règles d'autorisation pour le module Contrôle du lancement des applications.

  Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles du module Contrôle du lancement des applications ou importer manuellement les règles générées.

  Il est recommandé d'utiliser ce scénario quand il faut créer rapidement des listes de règles du Contrôle du lancement des applications. Nous recommandons de configurer le lancement de la tâche *Générateur de règles pour le Contrôle du lancement des applications* selon une planification uniquement si la zone d'application des règles d'autorisation contient des dossiers et des fichiers réputés sûrs.

- Sur la base du rapport d'événements généré dans Kaspersky Security Center pour le module Contrôle du lancement des applications, en mode *Informer*.

Dans le cadre de ce scénario, Kaspersky Embedded Systems Security n'interdit pas le lancement des applications. Au contraire, alors que le module Contrôle du lancement des applications fonctionne en mode *Informer*, il signale toutes les interdictions et autorisations de lancement d'application sur l'ensemble des appareils protégés du réseau dans la section **Événements** de l'espace de travail du nœud du Serveur d'administration dans Kaspersky Security Center. Kaspersky Security Center utilise les rapports pour crée une liste unique d'événements caractérisés par l'interdiction du lancement de l'application.

Pendant l'exécution du module, tous les scénarios possibles pour les appareils protégés et les groupes d'appareils protégés doivent être exécutés, y compris au moins un redémarrage d'un appareil protégé. Vous pouvez ensuite importer les données relatives aux lancements d'application depuis le fichier de rapport sur les événements de Kaspersky Security Center enregistré au format TXT et créer, sur la base de ces données, des règles d'autorisation pour le Contrôle du lancement des applications.

Ce scénario est recommandé si le réseau de l'entreprise compte un nombre important d'appareils protégés de types différents (et dotés de logiciels différents).

- Sur la base des événements d'interdiction de lancement des applications reçus via Kaspersky Security Center, sans création et importation du fichier de configuration.

  Pour pouvoir utiliser cette fonctionnalité, le module Contrôle du lancement des applications de l'appareil protégé doit fonctionner dans le cadre d'une stratégie active de Kaspersky Security Center. Dans ce cas, tous les événements sur l'appareil protégés sont transmis au Serveur d'administration.

Nous conseillons d'actualiser les listes de règles après toute modification de la composition des applications installées sur les appareils protégés du réseau (par exemple, en cas d'installation d'une mise à jour ou de réinstallation du système d'exploitation). Il est conseillé de créer une liste mise à jour de règles en exécutant la tâche *Générateur de règles pour le Contrôle du lancement des applications* ou le module Contrôle du lancement des applications en mode *Informer* sur les appareils protégés du groupe d'administration test. Le groupe d'administration d'essai réunit les appareils protégés indispensables à la vérification du lancement de nouvelles applications avant leur installation sur les appareils protégés du réseau.

Les fichiers XML qui contiennent la liste des règles d'autorisation, sont créés sur la base de l'analyse des applications lancées sur l'appareil protégé. Pour comptabiliser toutes les applications utilisées sur le réseau lors de la création des listes de règles, il est conseillé de lancer la tâche *Générateur de règles pour le Contrôle du lancement des applications* et le module Contrôle du lancement des applications en mode *Informer* sur une machine modèle.

Avant de créer des règles d'autorisation sur la base des applications lancées sur une machine modèle, assurez-vous que celle-ci est sûre et qu'elle n'est infectée par aucune application malveillante.

Avant d'ajouter des règles d'autorisation, sélectionnez un des modes d'application de règle disponible. La liste des règles de la stratégie de Kaspersky Security Center affiche uniquement les règles définies dans cette stratégie, quel que soit le mode d'application des règles. La liste des règles locale affiche toutes les règles appliquées, quelles soient locales ou ajoutées via une stratégie.

Activation et configuration du Contrôle du lancement des applications

Comment activer et configurer les paramètres généraux du Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
5. Cochez la case **Contrôle du lancement des applications**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Bloquer**. Kaspersky Embedded Systems Security applique toutes les règles du Contrôle du lancement des applications.
   - **Informer**. Kaspersky Embedded Systems Security n'utilise pas les règles du Contrôle du lancement des applications. Il enregistre uniquement les informations sur le lancement des applications dans le journal du module. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles du Contrôle du lancement des applications sur la base des informations relatives aux lancements d'applications interdits qui ont été consignées dans le journal d'exécution du module.
7. Configurez les paramètres du module (cf. tableau ci-après).
8. Enregistrez vos modifications.

   Kaspersky Embedded Systems Security applique immédiatement les paramètres du nouveau module. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres avant et après leur modification, seront enregistrées dans le journal d'audit système.

Comment activer et configurer les paramètres généraux du Contrôle du lancement des applications dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Contrôle du lancement des applications**.
2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
3. Cochez la case **Contrôle du lancement des applications**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Bloquer**. Kaspersky Embedded Systems Security applique toutes les règles du Contrôle du lancement des applications.

   - **Informer**. Kaspersky Embedded Systems Security n'utilise pas les règles du Contrôle du lancement des applications. Il enregistre uniquement les informations sur le lancement des applications dans le journal du module. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles du Contrôle du lancement des applications sur la base des informations relatives aux lancements d'applications interdits qui ont été consignées dans le journal d'exécution du module.

5. Configurez les paramètres du module (cf. tableau ci-après).

6. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique immédiatement les paramètres du nouveau module. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres avant et après leur modification, seront enregistrées dans le journal d'audit système.

Comment activer et configurer les paramètres généraux du Contrôle du lancement des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

6. Cochez la case **Activer le Contrôle du lancement des applications**.

7. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Bloquer**. Kaspersky Embedded Systems Security applique toutes les règles du Contrôle du lancement des applications.

   - **Informer**. Kaspersky Embedded Systems Security n'utilise pas les règles du Contrôle du lancement des applications. Il enregistre uniquement les informations sur le lancement des applications dans le journal du module. Le lancement de toutes les applications est autorisé. Vous pouvez utiliser ce mode pour la composition d'une liste de règles du Contrôle du lancement des applications sur la base des informations relatives aux lancements d'applications interdits qui ont été consignées dans le journal d'exécution du module.

8. Configurez les paramètres du module (cf. tableau ci-après).

9. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique immédiatement les paramètres du nouveau module. Les informations sur la date et l'heure de modification des paramètres, ainsi que les valeurs des paramètres avant et après leur modification, seront enregistrées dans le journal d'audit système.

Paramètres généraux du Contrôle du lancement des applications

Paramètre	Description
Répéter l'action prise pour le premier lancement de fichier sur tous les lancements ultérieurs de ce fichier	L'option active ou désactive le contrôle d'un nouveau lancement de l'application en fonction des informations d'incidents stockées dans le cache. Si l'option est activée, Kaspersky Embedded Systems Security autorise ou interdit les lancements ultérieurs d'une application sur la base de la conclusion du module suite au premier lancement de l'application. Par exemple, si le premier lancement de l'application avait été autorisé par les règles, l'enregistrement relatif à cet événement est enregistré dans le cache et les lancements ultérieurs de cette application sont également autorisés, sans vérification additionnelle. Si l'application est installée sur un ordinateur fonctionnant sous Windows XP, les conclusions du premier démarrage de l'application peuvent être écrasées lors de l'utilisation de fichiers via l'Explorateur, ce qui empêche la fonction de fonctionner correctement. Si l'option est désactivée, Kaspersky Embedded Systems Security analyse l'application à chacune des tentatives de lancement.
Refuser le lancement des interpréteurs de commande sans commande à exécuter	Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security refuse le lancement d'un interpréteur de ligne de commande lorsque l'une des conditions suivantes est remplie : • Le lancement d'un interpréteur de ligne de commande est interdit par les règles du Contrôle de lancement des applications. • L'interpréteur de ligne de commande démarre sans paramètres. Si l'option est désactivée, Kaspersky Embedded Systems Security tient uniquement compte des règles d'autorisation pour lancer un interpréteur de ligne de commande. Le lancement est bloqué si aucune des règles d'autorisation du Contrôle du lancement des applications n'est applicable. Si la règle d'autorisation du Contrôle du lancement des applications s'applique, il est possible de lancer un interpréteur de ligne de commande avec ou sans commande à exécuter. Kaspersky Embedded Systems Security gère le lancement des interprètes de commande suivants : • cmd.exe • powershell.exe • python.exe • perl.exe • wscript.exe Par défaut, la fonctionnalité est désactivée.
Appliquer des règles aux fichiers exécutables	L'option active ou désactive le contrôle de lancement des fichiers exécutables. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security autorise ou interdit le lancement de fichiers exécutables à l'aide des règles du Contrôle du lancement des applications. Si cette fonctionnalité est désactivée, Kaspersky Embedded Systems Security ne contrôle pas le lancement de fichiers exécutables à l'aide des règles du Contrôle du lancement des applications. Le lancement des fichiers exécutables est autorisé. Cette option est activée par défaut.
Surveiller le chargement des modules DLL	Le contrôle du chargement des modules DLL peut avoir un impact sur les performances du système d'exploitation. Cette fonctionnalité est disponible si la fonctionnalité **Appliquer des règles aux fichiers exécutables** est activée. Cette fonctionnalité active ou désactive le contrôle du chargement des modules DLL. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security autorise ou interdit le chargement des modules DLL à l'aide des règles du Contrôle du lancement des applications. Si cette fonctionnalité est désactivée, Kaspersky Embedded Systems Security ne contrôle pas le chargement des modules DLL à l'aide des règles du Contrôle du lancement des applications. Le chargement des modules DLL est autorisé. Par défaut, la fonctionnalité est désactivée.

Paramètre	Description
Appliquer des règles aux scripts et aux paquets MSI	L'option active ou désactive le lancement des scripts et des paquets MSI. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security autorise ou interdit le lancement de scripts et paquets MSI à l'aide des règles du Contrôle du lancement des applications. Si la case est décochée, Kaspersky Embedded Systems Security ne contrôle pas le lancement de scripts et paquets MSI à l'aide des règles du Contrôle du lancement des applications. Le lancement des scripts et des paquets MSI est autorisé. Cette option est activée par défaut.
Ignorer l'absence d'horodatage d'une signature lors de la validation de certificats	Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security autorise le lancement d'applications signées avec des certificats qui ont expiré ou dont la date d'expiration n'est pas définie. Si cette fonctionnalité est désactivée, Kaspersky Embedded Systems Security interdit le lancement d'applications signées avec des certificats qui ont expiré ou dont la date d'expiration n'est pas définie. Par défaut, la fonctionnalité est désactivée.

Configuration du contrôle de la distribution des logiciels

Configuration du Contrôle de la distribution des logiciels dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
5. Sélectionnez l'onglet **Contrôle de la distribution des logiciels**.
6. Activez la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets répertoriés**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide de fichiers exécutables et de paquets d'installation indiqués dans la liste.

   Vous pouvez activer la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets répertoriés** si sous l'onglet **Général**, la fonctionnalité **Appliquer des règles aux fichiers exécutables** est activée.
7. Si nécessaire, désactivez la fonctionnalité **Toujours autoriser la distribution de logiciels via Windows Installer**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide du programme d'installation Windows.

   La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.
8. Si nécessaire, activez la fonctionnalité **Toujours autoriser la distribution de logiciels via SCCM à l'aide du service de transfert intelligent en arrière-plan**. Cette fonctionnalité permet de distribuer des logiciels à l'aide de la solution System Center Configuration Manager.

Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security permet de déployer Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de distribuer des logiciels uniquement via Background Intelligent Transfer Service. L'application contrôle l'exécution des fichiers exécutables présentant les extensions .EXE et .MSI.

L'application contrôle le cycle de distribution de logiciels sur l'appareil protégé, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de Kaspersky Embedded Systems Security sur l'appareil protégé.

9. Ajoutez les fichiers exécutables et les paquets d'installation dont vous souhaitez autoriser le lancement :

- **Ajoutez-en un manuellement**

  a. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Ajouter un paquet de distribution**.

  b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir...**.

  c. Sélectionnez le fichier exécutable ou le paquet de distribution.

  Les champs sous **Critères de confiance** sont automatiquement remplis avec des informations relatives au fichier sélectionné.

  d. Si nécessaire, activez la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance**.

  e. Sélectionnez le critère qui décidera de la confiance du fichier exécutable ou du paquet d'installation : **Détails du certificat** ou **Hachage SHA256**.

  f. Cliquez sur le bouton **OK**.

  Le fichier exécutable ou le paquet d'installation est ajouté à la liste.

- **Ajouter plusieurs selon le hash**

  a. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Ajouter plusieurs paquets par hachage**.

  b. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez n'importe quel nombre de fichiers ou de paquets d'installation.

  c. Cliquez sur **Ouvrir**.

  Les fichiers exécutables ou les paquets d'installation sont ajoutés à la liste. Le hachage SHA256 est spécifié dans leurs propriétés.

- **Importer depuis un fichier**

  a. Cliquez sur **Importer**.

  b. Dans la fenêtre qui s'ouvre, sélectionnez un fichier TXT contenant les informations sur les fichiers exécutables et les paquets d'installation.

  c. Cliquez sur **Ouvrir**.

Les fichiers exécutables ou les paquets d'installation sont ajoutés à la liste. Le hachage SHA256 est spécifié dans leurs propriétés.

Si vous créez un paquet de distribution de confiance basé sur un fichier exécutable et que vous avez ajouté un processus dans les paramètres de la zone de confiance basé sur ce même fichier exécutable et l'avez rendu de confiance pour le module Contrôle du lancement des applications, les paramètres de la Zone de confiance ont une priorité plus élevée. Kaspersky Embedded Systems Security bloque le lancement de ce fichier exécutable, mais considère que le processus d'exécution du fichier exécutable est de confiance.

10. Si nécessaire, modifiez la liste des fichiers exécutables et des paquets d'installation ajoutés en cliquant sur le bouton **Modifier**.

11. Si nécessaire, supprimez les fichiers exécutables et les paquets d'installation ajoutés en cliquant sur le bouton **Supprimer**. Dans ce cas, les fichiers exécutables décompressés sont autorisés.

Pour empêcher l'exécution de fichiers exécutables décompressés, vous devez supprimer Kaspersky Embedded Systems Security de l'appareil protégé ou créer des règles de refus du Contrôle du lancement des applications pour les fichiers décompressés.

12. Cliquez sur **OK**.

Comment configurer le Contrôle de la distribution des logiciels dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Contrôle du lancement des applications**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

3. Sélectionnez l'onglet **Contrôle de la distribution des logiciels**.

4. Activez la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets répertoriés**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide de fichiers exécutables et de paquets d'installation indiqués dans la liste.

Vous pouvez activer la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets répertoriés** si sous l'onglet **Général**, la fonctionnalité **Appliquer des règles aux fichiers exécutables** est activée.

5. Si nécessaire, désactivez la fonctionnalité **Toujours autoriser la distribution de logiciels via Windows Installer**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide du programme d'installation Windows.

La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.

6. Si nécessaire, activez la fonctionnalité **Toujours autoriser la distribution de logiciels via SCCM à l'aide du service de transfert intelligent en arrière-plan**. Cette fonctionnalité permet de distribuer des logiciels à l'aide de la solution System Center Configuration Manager.

   Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security permet de déployer Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de distribuer des logiciels uniquement via Background Intelligent Transfer Service. L'application contrôle l'exécution des fichiers exécutables présentant les extensions .EXE et .MSI.

   L'application contrôle le cycle de distribution de logiciels sur l'appareil protégé, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de Kaspersky Embedded Systems Security sur l'appareil protégé.

7. Ajoutez les fichiers exécutables et les paquets d'installation dont vous souhaitez autoriser le lancement :

   - **Ajoutez-en un manuellement**

     a. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Ajouter un paquet de distribution**.

     b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Parcourir...**.

     c. Sélectionnez le fichier exécutable ou le paquet de distribution.

     Les champs sous **Critères de confiance** sont automatiquement remplis avec des informations relatives au fichier sélectionné.

     d. Si nécessaire, activez la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance**.

     e. Sélectionnez le critère qui décidera de la confiance du fichier exécutable ou du paquet d'installation : **Détails du certificat** ou **Hachage SHA256**.

     f. Cliquez sur le bouton **OK**.

     Le fichier exécutable ou le paquet d'installation est ajouté à la liste.

   - **Ajouter plusieurs selon le hash**

     a. Dans le menu contextuel du bouton **Ajouter**, sélectionnez l'option **Ajouter plusieurs paquets par hachage**.

     b. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez n'importe quel nombre de fichiers ou de paquets d'installation.

     c. Cliquez sur **Ouvrir**.

     Les fichiers exécutables ou les paquets d'installation sont ajoutés à la liste. Le hachage SHA256 est spécifié dans leurs propriétés.

- **Importer depuis un fichier**

  a. Cliquez sur **Importer**.

  b. Dans la fenêtre qui s'ouvre, sélectionnez un fichier TXT contenant les informations sur les fichiers exécutables et les paquets d'installation.

  c. Cliquez sur **Ouvrir**.

  Les fichiers exécutables ou les paquets d'installation sont ajoutés à la liste. Le hachage SHA256 est spécifié dans leurs propriétés.

Si vous créez un paquet de distribution de confiance basé sur un fichier exécutable et que vous avez ajouté un processus dans les paramètres de la zone de confiance basé sur ce même fichier exécutable et l'avez rendu de confiance pour le module Contrôle du lancement des applications, les paramètres de la Zone de confiance ont une priorité plus élevée. Kaspersky Embedded Systems Security bloque le lancement de ce fichier exécutable, mais considère que le processus d'exécution du fichier exécutable est de confiance.

8. Si nécessaire, modifiez la liste des fichiers exécutables et des paquets d'installation ajoutés en cliquant sur le bouton **Modifier**.

9. Si nécessaire, supprimez les fichiers exécutables et les paquets d'installation ajoutés en cliquant sur le bouton **Supprimer**. Dans ce cas, les fichiers exécutables décompressés sont autorisés.

Pour empêcher l'exécution de fichiers exécutables décompressés, vous devez supprimer Kaspersky Embedded Systems Security de l'appareil protégé ou créer des règles de refus du Contrôle du lancement des applications pour les fichiers décompressés.

10. Cliquez sur **OK**.

Comment configurer le Contrôle de la distribution des logiciels dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

6. Sélectionnez l'onglet **Contrôle de la distribution des logiciels**.

7. Activez la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets de la liste**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide de fichiers exécutables et de paquets d'installation indiqués dans la liste.

   Vous pouvez activer la fonctionnalité **Autoriser automatiquement la distribution de logiciels via les applications et les paquets de la liste** si sous l'onglet **Général**, la fonctionnalité **Utiliser les règles pour les fichiers exécutables** est activée.

8. Si nécessaire, désactivez la fonctionnalité **Toujours autoriser la distribution de logiciels via Windows Installer**. Cette fonctionnalité crée automatiquement des exclusions pour tous les fichiers lancés à l'aide du programme d'installation Windows.

   La désactivation de cette fonction peut provoquer des problèmes au niveau de la mise à jour des fichiers du système d'exploitation ou empêcher le lancement des fichiers extraits d'un paquet de distribution.

9. Si nécessaire, activez la fonctionnalité **Toujours autoriser la distribution de logiciels via SCCM à l'aide du service de transfert intelligent en arrière-plan (BITS)**. Cette fonctionnalité permet de distribuer des logiciels à l'aide de la solution System Center Configuration Manager.

   Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security permet de déployer Microsoft Windows à l'aide de System Center Configuration Manager. L'application permet de distribuer des logiciels uniquement via Background Intelligent Transfer Service. L'application contrôle l'exécution des fichiers exécutables présentant les extensions .EXE et .MSI.

   L'application contrôle le cycle de distribution de logiciels sur l'appareil protégé, depuis la remise du paquet jusqu'à l'installation/la mise à jour. L'application ne contrôle pas les processus si une étape quelconque de la distribution avait été réalisée avant l'installation de Kaspersky Embedded Systems Security sur l'appareil protégé.

10. Ajoutez les fichiers exécutables et les paquets d'installation dont vous souhaitez autoriser le lancement :

    - **Manuellement**

      a. Cliquez sur **Ajouter**.

      b. Sous **Critères de confiance**, sélectionnez le critère qui décidera de la confiance du fichier exécutable ou du paquet d'installation : **Utiliser le certificat numérique** ou **Utiliser le hachage SHA256**.

      c. Si vous avez sélectionné **Utiliser le certificat numérique**, saisissez l'en-tête et l'empreinte du certificat avec lequel le fichier exécutable ou le paquet d'installation est signé, ainsi que le nom du fichier exécutable ou du paquet d'installation.

      d. Si vous avez sélectionné **Utiliser le hachage SHA256**, cliquez sur **Parcourir...** pour sélectionner le fichier exécutable ou le paquet d'installation.

      e. Si nécessaire, activez la fonctionnalité **Autoriser le lancement de tous les fichiers enfants comme paquets de distribution de confiance**.

      f. Cliquez sur le bouton **OK**.

    Le fichier exécutable ou le paquet d'installation est ajouté à la liste.

- **Importer depuis un fichier**

  a. Cliquez sur **Importer**.

  b. Dans la fenêtre qui s'ouvre, sélectionnez un fichier TXT contenant les informations sur les fichiers exécutables et les paquets d'installation.

  c. Appuyez sur le bouton **Ouvrir**.

  Les fichiers exécutables ou les paquets d'installation sont ajoutés à la liste. Le hachage SHA256 est spécifié dans leurs propriétés.

Si vous créez un paquet de distribution de confiance basé sur un fichier exécutable et que vous avez ajouté un processus dans les paramètres de la zone de confiance basé sur ce même fichier exécutable et l'avez rendu de confiance pour le module Contrôle du lancement des applications, les paramètres de la Zone de confiance ont une priorité plus élevée. Kaspersky Embedded Systems Security bloque le lancement de ce fichier exécutable, mais considère que le processus d'exécution du fichier exécutable est de confiance.

11. Si nécessaire, modifiez la liste des fichiers exécutables et des paquets d'installation ajoutés en cliquant sur le bouton **Modifier**.
12. Si nécessaire, supprimez les fichiers exécutables et les paquets d'installation ajoutés en cliquant sur le bouton **Supprimer**. Dans ce cas, les fichiers exécutables décompressés sont autorisés.

    Pour empêcher l'exécution de fichiers exécutables décompressés, vous devez supprimer Kaspersky Embedded Systems Security de l'appareil protégé ou créer des règles de refus du Contrôle du lancement des applications pour les fichiers décompressés.

13. Cliquez sur **OK**.
14. Cliquez sur le bouton **OK** dans la fenêtre **Contrôle du lancement des applications**.

Utilisation des règles du Contrôle du lancement des applications

Cette section contient des instructions permettant de créer une liste de règles pour le Contrôle du lancement des applications.

Ajout des règles du Contrôle du lancement des applications

Comment ajouter des règles du Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

5. Sélectionnez l'onglet **Règles**.

6. De la liste déroulante **Utilisation des règles**, sélectionnez le mode d'application de la règle :

   - **Ajouter les règles de la stratégie aux règles locales**. L'application applique la liste de règles définie dans la stratégie en même temps que les listes de règles locales.

   - **Remplacer les règles locales par les règles de la stratégie**. L'application applique la liste de règles indiquées dans la stratégie dans le cadre du contrôle du lancement des applications sur le groupe d'appareils protégés. La création, la modification ou l'application de règles locales ne sont pas disponibles.

7. Si nécessaire, activez la fonctionnalité **Interdire la modification des règles locales par les utilisateurs**.

   Si cette fonctionnalité est activée, l'application ne permet pas de modifier les règles du Contrôle du lancement des applications localement dans la Console de l'application. Par défaut, la fonctionnalité est désactivée.

8. Ajoutez des règles de Contrôle du lancement des applications à l'aide d'une des méthodes suivantes :

   - **Manuellement**

     a. Cliquez sur **Ajouter**.

        La fenêtre **Contrôle du lancement des applications** s'ouvre.

     b. Dans le champ **Nom**, saisissez le nom de la règle.

     c. Si nécessaire, dans le champ **Description**, saisissez une description de la règle.

     d. Dans la liste déroulante **Type**, sélectionnez le type de règle :

        - **Autoriser** si vous souhaitez que la règle autorise l'exécution des applications décrites par la règle.

        - **Refuser** si vous souhaitez que la règle bloque l'exécution des applications décrites par la règle.

     e. Dans la liste déroulante **Zone**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :

        - **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.

        - **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et des paquets MSI. Les fichiers avec les extensions suivantes sont pris en charge : .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh et .sct.

     f. Cochez la case **Programmes de mise à jour de confiance** si vous voulez que Kaspersky Embedded Systems Security considère les applications correspondant aux conditions de déclenchement de la règle comme des programmes de mise à jour de confiance. Les programmes de mise à jour de confiance sont des applications qui sont autorisées à créer d'autres fichiers exécutables qui seront autorisés à s'exécuter par la suite.

Si une application déclenche plusieurs règles, Kaspersky Embedded Systems Security active l'indicateur *Programmes de mise à jour de confiance* si les conditions suivantes sont remplies :

- Toutes les règles permettent à l'application de fonctionner.
- La case **Programmes de mise à jour de confiance** est cochée pour au moins une règle.

g. Ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications.

h. Ajouter des exclusions aux conditions de déclenchement pour la règle du Contrôle du lancement des applications.

i. Ajouter des utilisateurs et/ou des groupes d'utilisateurs autorisés ou non autorisés à lancer des applications conformes à la règle.

j. Cliquez sur le bouton **OK**.

- **En important un fichier XML contenant les règles du Contrôle du lancement des applications**

a. Dans le menu contextuel du bouton , sélectionnez l'option **Importer → À partir d'un fichier XML**.

b. Choisissez comment ajouter les règles du Contrôle des appareils depuis un fichier XML à celles disponibles dans la stratégie :

- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques ne sont pas dupliquées. Si au moins un paramètre de règle est unique, la règle est ajoutée.

c. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au fichier XML qui a été créé à l'issue de la tâche locale ou de la tâche de groupe *Générateur de règles pour le Contrôle du lancement des applications*.

d. Cliquez sur **Ouvrir**.

- **Sur la base des événements de Kaspersky Security Center à l'aide d'une requête**

a. Dans le menu contextuel du bouton , sélectionnez l'option **Importer → Créer des règles d'autorisation à partir des événements de Kaspersky Security Center (requête)**.

b. Sélectionnez le principe d'ajout des règles à la liste des règles du Contrôle du lancement des applications déjà créées :

- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles possédant des paramètres identiques ne sont pas ajoutées ; la règle est ajoutée si au moins un des paramètres a une valeur différente.

La fenêtre **Génération des règles du Contrôle du lancement des applications** s'ouvre.

c. Sélectionnez les types d'événements sur la base desquels l'application créera les règles du Contrôle du lancement des applications :

- **Lancement de l'application refusé**.
- **Mode Statistiques seulement : lancement de l'application refusé**.

d. Sélectionnez une période dans la liste déroulante **Demander les événements qui ont été générés au cours de la période**.

e. Cochez ou décochez la case **Accorder une priorité supérieure à l'utilisation du hachage lors de la création de règles**.

Si la case est cochée, Kaspersky Embedded Systems Security utilise la somme de contrôle du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

Si la case n'est pas cochée, Kaspersky Embedded Systems Security utilise le certificat numérique du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

f. Cliquez sur **Générer les règles**.

g. Cliquez sur **OK**.

- **En important un fichier TXT avec une sélection d'événements d'applications bloquées de Kaspersky Security Center**

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Journaux et notifications**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Journaux des tâches**.

   La fenêtre **Notifications** s'ouvre.
5. Développez le nœud **Contrôle de l'activité locale**.
6. Sélectionnez la section **Contrôle du lancement des applications**.
7. Dans la liste des événements Contrôle du lancement des applications, dans la colonne **Envoyer les événements à Kaspersky Security Center**, cochez les cases en regard de *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test*.
8. Enregistrez vos modifications.

9. Dans la section **Configuration de l'événement** de la stratégie, assurez-vous que la durée de stockage des événements spécifiée dans le champ **&Conserver dans la base de données du Serveur d'administration pendant (jours)** est supérieure à la période pour laquelle vous prévoyez de rassembler des informations sur les lancements d'applications bloqués (30 jours par défaut).

   À l'expiration de la période de conservation des journaux du module Contrôle du lancement des applications, les événements consignés seront supprimés et n'apparaîtront plus dans le rapport.

10. Activez la stratégie configurée pour collecter des données sur les lancements d'applications interdits.

11. Si nécessaire, modifiez le mode de fonctionnement du module Contrôle du lancement des applications.

12. Lorsque le délai pour la collecte d'informations sur les lancements d'applications bloqués expire, effectuez une sélection parmi les événements *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test* et exportez-la vers un fichier TXT. Pour en savoir plus, reportez-vous à la section « Sélections d'événements » de l'Aide de Kaspersky Security Center.

13. Ouvrez le fichier TXT exporté.

14. Si nécessaire, modifiez la liste des événements.

Les règles du Contrôle du lancement des applications ajoutées s'affichent dans la liste.

9. Si nécessaire, exécutez l'étape 5 pour ajouter d'autres règles du Contrôle du lancement des applications.

10. Si nécessaire, modifiez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Modifier**.

11. Si nécessaire, supprimez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Supprimer**.

12. Cliquez sur **OK**.

Comment ajouter des règles du Contrôle du lancement des applications dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Contrôle du lancement des applications**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

3. Sélectionnez l'onglet **Règles**.

4. Ajoutez des règles de Contrôle du lancement des applications à l'aide d'une des méthodes suivantes :

   - **Manuellement**

     a. Cliquez sur **Ajouter**.

     La fenêtre **Contrôle du lancement des applications** s'ouvre.

     b. Dans le champ **Nom**, saisissez le nom de la règle.

     c. Si nécessaire, dans le champ **Description**, saisissez une description de la règle.

d. Dans la liste déroulante **Type**, sélectionnez le type de règle :

- **Autoriser** si vous souhaitez que la règle autorise l'exécution des applications décrites par la règle.
- **Refuser** si vous souhaitez que la règle bloque l'exécution des applications décrites par la règle.

e. Dans la liste déroulante **Zone**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :

- **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
- **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et des paquets MSI. Les fichiers avec les extensions suivantes sont pris en charge : .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh et .sct.

f. Cochez la case **Programmes de mise à jour de confiance** si vous voulez que Kaspersky Embedded Systems Security considère les applications correspondant aux conditions de déclenchement de la règle comme des programmes de mise à jour de confiance. Les programmes de mise à jour de confiance sont des applications qui sont autorisées à créer d'autres fichiers exécutables qui seront autorisés à s'exécuter par la suite.

Si une application déclenche plusieurs règles, Kaspersky Embedded Systems Security active l'indicateur *Programmes de mise à jour de confiance* si les conditions suivantes sont remplies :

- Toutes les règles permettent à l'application de fonctionner.
- La case **Programmes de mise à jour de confiance** est cochée pour au moins une règle.

g. Ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications.

h. Ajouter des exclusions aux conditions de déclenchement pour la règle du Contrôle du lancement des applications.

i. Ajouter des utilisateurs et/ou des groupes d'utilisateurs autorisés ou non autorisés à lancer des applications conformes à la règle.

j. Cliquez sur le bouton **OK**.

- **En important un fichier XML contenant les règles du Contrôle du lancement des applications**

a. Dans le menu contextuel du bouton , sélectionnez l'option **Importer → À partir d'un fichier XML**.

b. Choisissez comment ajouter les règles du Contrôle des appareils depuis un fichier XML à celles disponibles dans la stratégie :

- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.
- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Fusionner avec les règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques ne sont pas dupliquées. Si au moins un paramètre de règle est unique, la règle est ajoutée.

c. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au fichier XML qui a été créé à l'issue de la tâche locale ou de la tâche de groupe *Générateur de règles pour le Contrôle du lancement des applications*.

d. Cliquez sur **Ouvrir**.

Les règles du Contrôle du lancement des applications ajoutées s'affichent dans la liste.

5. Si nécessaire, exécutez l'étape 5 pour ajouter d'autres règles du Contrôle du lancement des applications.

6. Si nécessaire, modifiez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Modifier**.

7. Si nécessaire, supprimez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Supprimer**.

8. Cliquez sur **OK**.

Comment ajouter des règles du Contrôle du lancement des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

6. Sélectionnez l'onglet **Règles**.

7. De la liste déroulante **Application des règles**, sélectionnez le mode d'application de la règle :

   - **Ajouter les règles de la stratégie aux règles locales**. L'application applique la liste de règles définie dans la stratégie en même temps que les listes de règles locales.

   - **Remplacer les règles locales par les règles de la stratégie**. L'application applique la liste de règles indiquées dans la stratégie dans le cadre du contrôle du lancement des applications sur le groupe d'appareils protégés. La création, la modification ou l'application de règles locales ne sont pas disponibles.

8. Si nécessaire, activez la fonctionnalité **Interdire la modification des règles locales par les utilisateurs**.

   Si cette fonctionnalité est activée, l'application ne permet pas de modifier les règles du Contrôle du lancement des applications localement dans la Console de l'application. Par défaut, la fonctionnalité est désactivée.

9. Ajoutez des règles de Contrôle du lancement des applications à l'aide d'une des méthodes suivantes :

   - **Manuellement**

     a. Cliquez sur **Ajouter**.

        La fenêtre **Paramètres de règle** s'ouvre.

     b. Dans le champ **Nom**, saisissez le nom de la règle.

c. Dans la liste déroulante **Type**, sélectionnez le type de règle :

- **Autoriser** si vous souhaitez que la règle autorise l'exécution des applications décrites par la règle.
- **Refuser** si vous souhaitez que la règle bloque l'exécution des applications décrites par la règle.

d. Dans la liste déroulante **Zone**, sélectionnez le type de fichiers dont le lancement sera contrôlé par la règle :

- **Fichiers exécutables**, si vous souhaitez que la règle contrôle le lancement des fichiers exécutables.
- **Scripts et paquets MSI**, si vous souhaitez que la règle contrôle le lancement des scripts et des paquets MSI.

e. Cochez la case **Interdire aux autres utilisateurs** si vous souhaitez que l'application bloque le lancement des applications décrites par la règle pour tous les utilisateurs qui ne sont pas listés sous l'onglet **Utilisateur ou groupe**.

f. Cochez la case **Programmes de mise à jour de confiance** si vous voulez que Kaspersky Embedded Systems Security considère les applications correspondant aux conditions de déclenchement de la règle comme des programmes de mise à jour de confiance. Les programmes de mise à jour de confiance sont des applications qui sont autorisées à créer d'autres fichiers exécutables qui seront autorisés à s'exécuter par la suite.

Si une application déclenche plusieurs règles, Kaspersky Embedded Systems Security active l'indicateur *Programmes de mise à jour de confiance* si les conditions suivantes sont remplies :

- Toutes les règles permettent à l'application de fonctionner.
- La case **Programmes de mise à jour de confiance** est cochée pour au moins une règle.

g. Ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications.

h. Ajouter des exclusions aux conditions de déclenchement pour la règle du Contrôle du lancement des applications.

i. **Ajouter des utilisateurs et/ou des groupes d'utilisateurs autorisés ou non autorisés à lancer des applications conformes à la règle**.

a. Sélectionnez l'onglet **Utilisateur ou groupe**.

b. Cliquez sur **Ajouter**.

c. Une fenêtre s'ouvre ; dans cette fenêtre, saisissez ou sélectionnez le nom d'un utilisateur ou d'un groupe d'utilisateurs.

d. Cliquez sur **Sélectionner**.

e. Suivez les étapes B à D pour chaque utilisateur ou groupe d'utilisateurs.

j. Cliquez sur le bouton **OK**.

Les règles du Contrôle du lancement des applications ajoutées s'affichent dans la liste.

- **En important un fichier XML contenant les règles du Contrôle du lancement des applications**

  a. Cliquez sur **Importer**.

  b. Cliquez sur le bouton **Sélectionner** dans la fenêtre **Importer du fichier** qui s'affiche.

  c. Spécifiez le chemin d'accès au fichier XML qui a été créé à l'issue de la tâche locale ou de la tâche de groupe pour la *Générateur de règles pour le Contrôle du lancement des applications*.

  d. Cliquez sur **Ouvrir**.

  e. Cliquez sur **Importer**.

  Les règles importées du Contrôle du lancement des applications sont ajoutées à la liste des règles existantes. Les règles dont les paramètres sont identiques ne sont pas dupliquées. Si au moins un paramètre de règle est unique, la règle est ajoutée.

- **En important un fichier XML contenant les règles du Contrôle du lancement des applications de Kaspersky Embedded Systems Security 3.4**

  a. Cliquez sur **Importer depuis la version antérieure**.

  b. Cliquez sur le bouton **Sélectionner** dans la fenêtre **Importer du fichier** qui s'affiche.

  c. Spécifiez le chemin d'accès au fichier XML contenant les règles du Contrôle du lancement des applications qui a été exporté depuis Kaspersky Embedded Systems Security 3.4.

  d. Cliquez sur **Ouvrir**.

  e. Cliquez sur **Importer**.

  Les règles importées du Contrôle du lancement des applications sont ajoutées à la liste des règles existantes. Les règles dont les paramètres sont identiques ne sont pas dupliquées. Si au moins un paramètre de règle est unique, la règle est ajoutée.

- **En important des règles à partir d'un fichier de rapport de Kaspersky Security Center**

  a. Cliquez sur **Importer depuis le rapport KSC**.

  b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier TXT dans lequel les événements du rapport ont été exportés.

  c. Cliquez sur **Ouvrir**.

  Les règles basées sur le rapport Kaspersky Security Center sont ajoutées à la liste des règles dans la stratégie.

- **Sur la base des événements de Kaspersky Security Center à l'aide d'une requête**

  a. Cliquez sur **Règles d'autorisation des événements KSC**.

  La fenêtre **Générateur de règles pour le Contrôle du lancement des applications** s'ouvre.

b. Sélectionnez le type d'événements sur la base desquels l'application créera les règles du Contrôle du lancement des applications :

- **Tous les événements**.
- **Lancement de l'application interdit**.
- **Mode Statistiques seulement : lancement de l'application interdit**.

c. Sélectionnez une période dans la liste déroulante **Utiliser les événements générés au cours de la période**.

d. Cochez ou décochez la case **Accorder une priorité supérieure à l'utilisation du hash lors de la création de règles**.

Si la case est cochée, Kaspersky Embedded Systems Security utilise la somme de contrôle du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

Si la case n'est pas cochée, Kaspersky Embedded Systems Security utilise le certificat numérique du fichier pour créer la règle lorsque la somme de contrôle et le certificat du fichier sont disponibles.

e. Si nécessaire, spécifiez le nom du groupe des appareils gérés dans le champ **Utiliser les événements générés pour un groupe d'appareils administrés**.

f. Cliquez sur **Créer des règles**.

g. Dans la liste déroulante **Règle à ajouter à la liste principale**, sélectionnez le principe d'ajout des règles à la liste des règles du Contrôle du lancement des applications déjà créées :

- **Ajouter aux règles existantes**, si vous souhaitez que les règles à importer viennent compléter la liste des règles existantes. Les règles dont les paramètres sont identiques sont dédoublées.
- **Remplacer les règles existantes**, si vous souhaitez que les règles à importer remplacent les règles existantes.

h. Sélectionnez les règles que vous souhaitez exporter vers les règles du Contrôle du lancement des applications de la stratégie, puis cliquez sur le bouton **Exporter**.

i. Enregistrez vos modifications.

10. Si nécessaire, exécutez l'étape 5 pour ajouter d'autres règles du Contrôle du lancement des applications.
11. Si nécessaire, modifiez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Modifier**.
12. Si nécessaire, supprimez les règles du Contrôle du lancement des applications ajoutées en cliquant sur le bouton **Supprimer**.
13. Cliquez sur **OK**.

Ajout de conditions de déclenchement de la règle du Contrôle du lancement des applications

Comment ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
5. Sélectionnez l'onglet **Règles**.
6. Réalisez une des opérations suivantes :

   a. Cliquez sur le bouton **Ajouter** si vous ajoutez une nouvelle règle du Contrôle du lancement des applications.

   b. Dans la liste des règles du Contrôle du lancement des applications, choisissez la règle à laquelle vous souhaitez ajouter des conditions de déclenchement, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.
7. Sous l'onglet **Conditions**, dans le menu contextuel du bouton **Ajouter**, sélectionnez une condition de déclenchement pour la règle du Contrôle du lancement des applications :

   - **Informations du fichier**. Les **informations du fichier sélectionné** sont utilisées comme condition de déclenchement de la règle.

     a. Cliquez sur le bouton **Parcourir** dans la fenêtre **Informations du fichier**.

     La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

     b. Sélectionnez le fichier.

     c. Cliquez sur **Ouvrir**.

     Les informations sur le fichier sélectionné s'affichent dans la fenêtre **Informations du fichier**.

     d. Sélectionnez au moins une option :

     - **Propriétés des fichiers**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.
     - **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.

- **Hachage du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.
- **Chemin d'accès au fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

e. Si nécessaire, dans le champ **Ligne de commande**, saisissez la commande de lancement de l'application sur la ligne de commande. La règle contrôle le lancement de cette application. Vous pouvez utiliser les caractères ? et * pour saisir le masque.

> Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inverse (« \ ») dans les chemins d'accès.

f. Cliquez sur **OK**.

- **Type de lecteur**. La règle contrôle le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
- **Catégorie KL**. La règle contrôle le lancement des applications qui appartiennent aux catégories KL sélectionnées.
- **De confiance par KSN**. La règle contrôle le lancement des applications de confiance dans KSN.
- **Douteux par KSN**. La règle contrôle le lancement des applications douteuses dans KSN.
- **De confiance par SE**. La règle contrôle le lancement des applications de confiance dans le système d'exploitation.

La condition ajoutée s'affichera dans la liste.

8. Si nécessaire, suivez l'étape précédente des instructions pour chacune des conditions de déclenchement de la règle suivantes.
9. Si nécessaire, modifiez les conditions de déclenchement de la règle en cliquant sur le bouton **Modifier**.
10. Enregistrez vos modifications.

Comment ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Contrôle du lancement des applications**.
2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
3. Sélectionnez l'onglet **Règles**.
4. Réalisez une des opérations suivantes :

   a. Cliquez sur le bouton **Ajouter** si vous ajoutez une nouvelle règle du Contrôle du lancement des applications.

   b. Dans la liste des règles du Contrôle du lancement des applications, choisissez la règle à laquelle vous souhaitez ajouter des conditions de déclenchement, puis cliquez sur le bouton **Modifier**.

La fenêtre **Contrôle du lancement des applications** s'ouvre.

5. Sous l'onglet **Conditions**, dans le menu contextuel du bouton **Ajouter**, sélectionnez une condition de déclenchement pour la règle du Contrôle du lancement des applications :

   - **Informations du fichier**. Les **informations du fichier sélectionné** sont utilisées comme condition de déclenchement de la règle.

     a. Cliquez sur le bouton **Parcourir** dans la fenêtre **Informations du fichier**.

     La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

     b. Sélectionnez le fichier.

     c. Cliquez sur **Ouvrir**.

     Les informations sur le fichier sélectionné s'affichent dans la fenêtre **Informations du fichier**.

     d. Sélectionnez au moins une option :

     - **Propriétés des fichiers**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.
     - **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.
     - **Hachage du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.
     - **Chemin d'accès au fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

     e. Si nécessaire, dans le champ **Ligne de commande**, saisissez la commande de lancement de l'application sur la ligne de commande. La règle contrôle le lancement de cette application. Vous pouvez utiliser les caractères ? et * pour saisir le masque.

     > Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inverse (« \ ») dans les chemins d'accès.

     f. Cliquez sur **OK**.

   - **Type de lecteur**. La règle contrôle le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
   - **Catégorie KL**. La règle contrôle le lancement des applications qui appartiennent aux catégories KL sélectionnées.
   - **De confiance par KSN**. La règle contrôle le lancement des applications de confiance dans KSN.
   - **Douteux par KSN**. La règle contrôle le lancement des applications douteuses dans KSN.
   - **De confiance par SE**. La règle contrôle le lancement des applications de confiance dans le système d'exploitation.

   La condition ajoutée s'affichera dans la liste.

6. Si nécessaire, suivez l'étape précédente des instructions pour chacune des conditions de déclenchement de la règle suivantes.

7. Si nécessaire, modifiez les conditions de déclenchement de la règle en cliquant sur le bouton **Modifier**.

8. Enregistrez vos modifications.

Comment ajouter des conditions de déclenchement pour la règle du Contrôle du lancement des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

6. Sélectionnez l'onglet **Règles**.

7. Cliquez sur **Ajouter**.

   La fenêtre **Paramètres de règle** s'ouvre.

8. Sous l'onglet **Conditions**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres de règle** s'ouvre.

9. Sélectionnez une condition de déclenchement pour la règle du Contrôle du lancement des applications :

   - **Informations du fichier**. Les **informations du fichier** sont utilisées comme condition de déclenchement de la règle.

     a. Sous **Critères de déclenchement de la règle**, spécifiez une valeur pour au moins un critère :

     - **Certificat numérique**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.

     - **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.

     - **Hachage SHA256**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.

     - **Chemin du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

     b. Cliquez sur **OK**.

   - **À partir de la catégorie KL**. La règle contrôle le lancement des applications qui appartiennent aux catégories KL sélectionnées.

- **Disque amovible**. La règle contrôle le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
- **De confiance par SE**. La règle contrôle le lancement des applications de confiance dans le système d'exploitation.

La condition ajoutée s'affichera dans la liste.

10. Si nécessaire, suivez les étapes 4 à 5 des instructions pour chacune des conditions de déclenchement de la règle suivantes.
11. Si nécessaire, modifiez les conditions de déclenchement de la règle en cliquant sur le bouton **Modifier**.
12. Enregistrez vos modifications.

Ajout d'exclusions d'une zone de règles du Contrôle du lancement des applications

Comment ajouter des exclusions à la zone d'action de la règle du Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.
   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
5. Sélectionnez l'onglet **Règles**.
6. Réalisez une des opérations suivantes :
   a. Cliquez sur le bouton **Ajouter** si vous ajoutez une nouvelle règle du Contrôle du lancement des applications.
   b. Dans la liste des règles du Contrôle du lancement des applications, sélectionnez la règle pour laquelle vous souhaitez ajouter des exclusions, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.
7. Sous l'onglet **Exclusions**, dans le menu contextuel du bouton **Ajouter**, sélectionnez un critère de création d'exclusions à la zone d'action de la règle du Contrôle du lancement des applications :
   - **Informations du fichier**. Les **informations du fichier sélectionné** sont utilisées comme critère.
     a. Cliquez sur le bouton **Parcourir** dans la fenêtre **Informations du fichier**.
        La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.
     b. Sélectionnez le fichier.

c. Cliquez sur **Ouvrir**.

Les informations sur le fichier sélectionné s'affichent dans la fenêtre **Informations du fichier**.

d. Sélectionnez au moins une option :

- **Propriétés des fichiers**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.
- **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.
- **Hachage du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.
- **Chemin d'accès au fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

e. Si nécessaire, dans le champ **Ligne de commande**, saisissez la commande de lancement de l'application sur la ligne de commande. La règle ne contrôle pas le lancement de cette application. Vous pouvez utiliser les caractères ? et * pour saisir le masque.

> Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inverse (« \ ») dans les chemins d'accès.

f. Cliquez sur **OK**.

- **Type de lecteur**. La règle ne contrôle pas le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
- **Catégorie KL**. La règle ne contrôle pas le lancement des applications qui appartiennent aux catégories KL sélectionnées.
- **De confiance par KSN**. La règle ne contrôle pas le lancement des applications de confiance dans KSN.
- **Douteux par KSN**. La règle ne contrôle pas le lancement des applications douteuses dans KSN.
- **De confiance par SE**. La règle ne contrôle pas le lancement des applications de confiance dans le système d'exploitation.

L'exclusion ajoutée s'affichera dans la liste.

8. Si nécessaire, suivez l'étape précédente des instructions pour ajouter chaque exclusion ultérieure à la zone d'action de la règle du Contrôle du lancement des applications.
9. Si nécessaire, modifiez les exclusions en cliquant sur le bouton **Modifier**.
10. Enregistrez vos modifications.

Comment ajouter des exclusions à la zone d'action de la règle du Contrôle du lancement des applications dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur** → **Contrôle du lancement des applications**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

3. Sélectionnez l'onglet **Règles**.

4. Réalisez une des opérations suivantes :

   a. Cliquez sur le bouton **Ajouter** si vous ajoutez une nouvelle règle du Contrôle du lancement des applications.

   b. Dans la liste des règles du Contrôle du lancement des applications, sélectionnez la règle pour laquelle vous souhaitez ajouter des exclusions, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre.

5. Sous l'onglet **Exclusions**, dans le menu contextuel du bouton **Ajouter**, sélectionnez un critère de création d'exclusions à la zone d'action de la règle du Contrôle du lancement des applications :

   - **Informations du fichier**. Les **informations du fichier sélectionné** sont utilisées comme critère.

     a. Cliquez sur le bouton **Parcourir** dans la fenêtre **Informations du fichier**.

     La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

     b. Sélectionnez le fichier.

     c. Cliquez sur **Ouvrir**.

     Les informations sur le fichier sélectionné s'affichent dans la fenêtre **Informations du fichier**.

     d. Sélectionnez au moins une option :

     - **Propriétés des fichiers**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.
     - **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.
     - **Hachage du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.
     - **Chemin d'accès au fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

e. Si nécessaire, dans le champ **Ligne de commande**, saisissez la commande de lancement de l'application sur la ligne de commande. La règle ne contrôle pas le lancement de cette application. Vous pouvez utiliser les caractères ? et * pour saisir le masque.

> Kaspersky Embedded Systems Security ne reconnaît pas les chemins qui contiennent des barres obliques "/". Utilisez la barre oblique inverse (« \ ») dans les chemins d'accès.

f. Cliquez sur **OK**.

- **Type de lecteur**. La règle ne contrôle pas le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
- **Catégorie KL**. La règle ne contrôle pas le lancement des applications qui appartiennent aux catégories KL sélectionnées.
- **De confiance par KSN**. La règle ne contrôle pas le lancement des applications de confiance dans KSN.
- **Douteux par KSN**. La règle ne contrôle pas le lancement des applications douteuses dans KSN.
- **De confiance par SE**. La règle ne contrôle pas le lancement des applications de confiance dans le système d'exploitation.

L'exclusion ajoutée s'affichera dans la liste.

6. Si nécessaire, suivez l'étape précédente des instructions pour ajouter chaque exclusion ultérieure à la zone d'action de la règle du Contrôle du lancement des applications.
7. Si nécessaire, modifiez les exclusions en cliquant sur le bouton **Modifier**.
8. Enregistrez vos modifications.

Comment ajouter des exclusions à la zone d'action de la règle du Contrôle du lancement des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Contrôle de l'activité locale**.
5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.
6. Sélectionnez l'onglet **Règles**.
7. Cliquez sur **Ajouter**.

   La fenêtre **Paramètres de règle** s'ouvre.
8. Sous l'onglet **Exclusions**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Paramètres de règle** s'ouvre.

9. Sélectionnez un critère pour créer une exclusion du champ de la règle du Contrôle du lancement des applications :

   - **Informations du fichier**. La règle ne contrôle pas le lancement des applications dont les données correspondent aux **données dans le fichier**.

     a. Sous **Critères de déclenchement de la règle**, spécifiez une valeur pour au moins un critère :

     - **Certificat numérique**. Si la case est cochée, la règle ne contrôle pas le lancement des applications signées avec un certificat numérique et ayant les données spécifiées.
     - **Métadonnées**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant les métadonnées spécifiées.
     - **Hachage SHA256**. Si la case est cochée, la règle ne contrôle pas le lancement des applications possédant le hachage SHA256 indiqué.
     - **Chemin du fichier**. Si la case est cochée, la règle ne contrôle pas le lancement des applications par le chemin d'accès indiqué.

     b. Cliquez sur **OK**.

   - **Catégorie KL**. La règle ne contrôle pas le lancement des applications qui appartiennent aux catégories KL sélectionnées.
   - **Type de lecteur**. La règle ne contrôle pas le lancement des applications depuis tous les disques amovibles connectés à l'ordinateur protégé.
   - **De confiance par SE**. La règle ne contrôle pas le lancement des applications de confiance dans le système d'exploitation.

   La condition ajoutée s'affichera dans la liste.

10. Si nécessaire, suivez les étapes 4 et 5 des instructions pour ajouter chaque exclusion ultérieure à la zone d'action de la règle du Contrôle du lancement des applications.

11. Si nécessaire, modifiez les exclusions en cliquant sur le bouton **Modifier**.

12. Enregistrez vos modifications.

Autorisation du lancement de toutes les applications

Vous pouvez autoriser le lancement de toutes les applications à l'aide de règles d'autorisation du Contrôle du lancement des applications spécialement configurées.

Pour autoriser le lancement de toutes les applications, procédez comme suit :

1. Ajoutez manuellement deux règles d'autorisation du Contrôle du lancement des applications avec les paramètres suivants :

   - Type de règle : *Autoriser*, Champ d'application : *Fichiers exécutables*, Chemin d'accès aux fichiers : `?:\`.
   - Type de règle : *Autoriser*, Champ d'application : *Scripts et paquets MSI*, Chemin d'accès aux fichiers : `?:\`.

2. Si des règles de refus du Contrôle du lancement des applications ont été ajoutées, supprimez-les.

3. Supprimez les exclusions pour toutes les règles d'autorisation du Contrôle du lancement des applications précédemment créées.

4. Enregistrez vos modifications.

Exportation des règles du Contrôle du lancement des applications

Vous pouvez exporter la liste des règles du Contrôle du lancement des applications et la liste des paquets d'installation approuvés du Contrôle de la distribution des logiciels dans un fichier XML. Vous pouvez utiliser la fonction d'exportation pour sauvegarder la liste des règles du Contrôle du lancement des applications ou pour procéder à la migration de la liste vers un autre serveur.

Exportation des règles du Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

5. Accédez à l'onglet **Règles** pour exporter les règles du Contrôle du lancement des applications ou à l'onglet **Contrôle de la distribution des logiciels** pour exporter les règles du Contrôle de la distribution des logiciels.

6. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

7. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

   a. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

   b. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

8. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.

Exportation des règles du Contrôle du lancement des applications dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Contrôle du lancement des applications**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

3. Accédez à l'onglet **Règles** pour exporter les règles du Contrôle du lancement des applications ou à l'onglet **Contrôle de la distribution des logiciels** pour exporter les règles du Contrôle de la distribution des logiciels.

4. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

5. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

   a. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

   b. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

6. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.

Exportation des règles du Contrôle du lancement des applications dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Contrôle du lancement des applications**.

   La fenêtre **Contrôle du lancement des applications** s'ouvre sous l'onglet **Général**.

6. Accédez à l'onglet **Règles** pour exporter les règles du Contrôle du lancement des applications ou à l'onglet **Contrôle de la distribution des logiciels** pour exporter les règles du Contrôle de la distribution des logiciels.

7. À l'aide des cases à cocher, sélectionnez les règles que vous souhaitez exporter.

8. Cliquez sur le bouton **Exporter**. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez si vous souhaitez exporter les règles sélectionnées ou toutes les règles, puis cliquez sur **Exporter**.

   Si vous n'avez sélectionné aucune règle, Kaspersky Embedded Systems Security exportera toutes les règles.

Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.

Création d'un fichier TXT avec une sélection d'événements d'applications bloqués par Kaspersky Security Center

Vous pouvez exporter une sélection d'événements d'applications bloqués par Kaspersky Security Center dans un fichier TXT, puis importer ces données pour générer une liste de règles d'autorisation du Contrôle du lancement des applications dans la stratégie que vous configurez.

Comment générer un fichier TXT avec une sélection d'événements d'applications bloqués par Kaspersky Security Kaspersky Security Center à l'aide de la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Journaux et notifications**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Journaux des tâches**.

   La fenêtre **Notifications** s'ouvre.
5. Développez le nœud **Contrôle de l'activité locale**.
6. Sélectionnez la section **Contrôle du lancement des applications**.
7. Dans la liste des événements Contrôle du lancement des applications, dans la colonne **Envoyer les événements à Kaspersky Security Center**, cochez les cases en regard de *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test*.
8. Enregistrez vos modifications.
9. Dans la section **Configuration de l'événement** de la stratégie, assurez-vous que la durée de stockage des événements spécifiée dans le champ **&Conserver dans la base de données du Serveur d'administration pendant (jours)** est supérieure à la période pour laquelle vous prévoyez de rassembler des informations sur les lancements d'applications bloqués (30 jours par défaut).

   > À l'expiration de la période de conservation des journaux du module Contrôle du lancement des applications, les événements consignés seront supprimés et n'apparaîtront plus dans le rapport.
10. Activez la stratégie configurée pour collecter des données sur les lancements d'applications interdits.
11. Si nécessaire, modifiez le mode de fonctionnement du module Contrôle du lancement des applications.
12. Lorsque le délai pour la collecte d'informations sur les lancements d'applications bloqués expire, effectuez une sélection parmi les événements *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test* et exportez-la vers un fichier TXT. Pour en savoir plus, reportez-vous à la section « Sélections d'événements » de l'Aide de Kaspersky Security Center.
13. Ouvrez le fichier TXT exporté.
14. Si nécessaire, modifiez la liste des événements.

Comment générer un fichier TXT avec une sélection d'événements d'applications bloqués par Kaspersky Security Kaspersky Security Center à l'aide de Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Journaux et notifications**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Journaux des tâches**.

   La fenêtre **Journaux des tâches** s'ouvre.

6. Sélectionnez la section **Contrôle du lancement des applications**.

7. Dans la liste des événements Contrôle du lancement des applications, dans la colonne **Envoyer les événements à Kaspersky Security Center**, cochez les cases en regard de *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test*.

8. Enregistrez vos modifications.

9. Sous l'onglet **Configuration de l'événement** de la stratégie que vous configurez, assurez-vous que la durée de stockage des événements spécifiée dans le champ **Conserver dans la base de données du Serveur d'administration pendant (jours)** est supérieure à la période pour laquelle vous prévoyez de rassembler des informations sur les lancements d'applications bloqués (30 jours par défaut).

   > À l'expiration de la période de conservation des journaux du module Contrôle du lancement des applications, les événements consignés seront supprimés et n'apparaîtront plus dans le rapport.

10. Activez la stratégie configurée pour collecter des données sur les lancements d'applications interdits.

11. Si nécessaire, modifiez le mode de fonctionnement du module Contrôle du lancement des applications.

12. Lorsque le délai pour la collecte d'informations sur les lancements d'applications bloqués expire, effectuez une sélection parmi les événements *Le lancement de l'application est interdit* et *Le lancement de l'application est interdit en mode test* et exportez-la vers un fichier TXT. Pour en savoir plus, reportez-vous à la section « Sélections d'événements » de l'Aide de Kaspersky Security Center.

13. Ouvrez le fichier TXT exporté.

14. Si nécessaire, modifiez la liste des événements.

Configuration d'une tâche de groupe Génération des règles du Contrôle du lancement des applications

Comment configurer la tâche de groupe Générateur de règles pour le Contrôle du lancement des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, développez le nœud **Appareils administrés**.

2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.

3. Sélectionnez l'onglet **Tâches**.

4. Dans la liste des tâches de groupe, ouvrez la tâche *Générateur de règles pour le Contrôle du lancement des applications* en double-cliquant sur le nom de la tâche.

   La fenêtre **Propriétés : Générateur de règles pour le Contrôle du lancement des applications** s'ouvre.

5. Passez à la section **Options**.

6. Si nécessaire, sous l'onglet **Règles**, saisissez un préfixe pour les noms de règles.

7. Sous **Autoriser la zone d'application des règles**, spécifiez la méthode que vous souhaitez utiliser pour créer des règles d'autorisation :

   - Créer des règles d'autorisation basées sur les applications lancées
   - Créer des règles d'autorisation pour les applications à partir des dossiers

8. Sous l'onglet **Paramètres**, sélectionnez les critères que la tâche appliquera lors de la création des règles d'autorisation du Contrôle du lancement des applications :

   - **Utiliser le 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. Kaspersky Embedded Systems Security autorisera les fichiers accompagnés d'un certificat numérique. Nous recommandons cette option 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 sujet et l'empreinte du certificat numérique
   - Si le certificat est manquant, utiliser
   - **Utiliser le hachage SHA256**.

     Si cette option est sélectionnée, la somme de contrôle du fichier sur la base duquel est créée la règle sert de critère de déclenchement de la règle dans les paramètres des règles d'autorisation créées pour le Contrôle du lancement des applications. Kaspersky Embedded Systems Security autorisera le lancement d'applications à l'aide de fichiers dont la somme de contrôle est spécifiée. L'utilisation de la somme de contrôle SHA256 comme critère de déclenchement de la règle limite la zone d'application des règles à un seul fichier.

9. Configurez le paramètre **Ajouter un chemin d'accès pour les règles générées sur la base des sommes de hachages**.

   Si cette case est cochée, lors de l'exportation des règles, Kaspersky Embedded Systems Security ajoute les chemins d'accès complets aux fichiers exécutables dans le fichier XML. Les chemins d'accès complets peuvent vous aider à déterminer à quel logiciel appartient un fichier exécutable.

   Si la case est décochée, le fichier XML ne contient que les noms et les hachages SHA256 des fichiers exécutables. Par défaut, la case est décochée.

10. Ajoutez des utilisateurs et/ou des groupes d'utilisateurs autorisés à lancer des applications qui respectent les règles créées à l'aide de la tâche :

    a. Dans le menu contextuel du bouton **Ajouter**, sélectionnez le mode d'ajout d'utilisateurs.

    b. Une fenêtre s'ouvre ; dans cette fenêtre, saisissez ou sélectionnez le nom d'un utilisateur ou d'un groupe d'utilisateurs.

    c. Cliquez sur **OK**.

    d. Suivez les étapes A à C pour chaque utilisateur ou groupe d'utilisateurs.

11. Configurez les paramètres suivants dans le bloc **Une fois la tâche terminée** :

    - Ajouter les règles d'autorisation à la liste des règles du Contrôle du lancement des applications

- Principe d'ajout
- **Exporter les règles d'autorisation vers un fichier**.
- Ajouter les détails de l'appareil protégé au nom du fichier

12. Si nécessaire, sous l'onglet **Exclusions**, spécifiez les objets que vous souhaitez exclure de la zone d'action de la tâche.

13. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : Générateur de règles pour le Contrôle du lancement des applications**.

Comment configurer la tâche de groupe Générateur de règles pour le Contrôle du lancement des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

2. Dans la liste des tâches de groupe, ouvrez la tâche Générateur de règles pour le Contrôle du lancement des applications.

   La fenêtre **Générateur de règles pour le Contrôle du lancement des applications** s'ouvre.

3. Ouvrez l'onglet **Paramètres de l'application**.

4. Si nécessaire, dans la section **Zone d'application des règles d'autorisation**, saisissez un préfixe pour les noms de règles.

5. Sous **Zone d'application des règles d'autorisation**, spécifiez la méthode que vous souhaitez utiliser pour créer des règles d'autorisation :

   - Créer des règles d'autorisation sur la base des applications en cours d'exécution
   - Créer des règles d'autorisation pour les applications à partir des dossiers

6. Sous l'onglet **Paramètres**, sélectionnez les critères que la tâche appliquera lors de la création des règles d'autorisation du Contrôle du lancement des applications :

   - Utiliser un certificat numérique
   - Utiliser l'objet et l'empreinte du certificat numérique
   - En cas d'absence de certificat, utiliser
   - Utiliser le hachage SHA256

7. Configurez le paramètre **Ajouter un chemin d'accès pour les règles générées sur la base des sommes de hachages**.

   Si cette case est cochée, lors de l'exportation des règles, Kaspersky Embedded Systems Security ajoute les chemins d'accès complets aux fichiers exécutables dans le fichier XML. Les chemins d'accès complets peuvent vous aider à déterminer à quel logiciel appartient un fichier exécutable.

   Si la case est décochée, le fichier XML ne contient que les noms et les hachages SHA256 des fichiers exécutables. Par défaut, la case est décochée.

8. Ajoutez des utilisateurs et/ou des groupes d'utilisateurs autorisés à lancer des applications qui respectent les règles créées à l'aide de la tâche :

   a. Cliquez sur **Ajouter un utilisateur ou un groupe**.

   b. Une fenêtre s'ouvre ; dans cette fenêtre, saisissez ou sélectionnez le nom d'un utilisateur ou d'un groupe d'utilisateurs.

   c. Cliquez sur **Sélectionner**.

   d. Suivez les étapes A à C pour chaque utilisateur ou groupe d'utilisateurs.

9. Configurez les paramètres suivants dans le bloc **Une fois la tâche terminée** :

   - **Ajouter les règles d'autorisation à la liste des règles du Contrôle du lancement des applications**
   - **Principe d'ajout**
   - **Les règles d'autorisation seront exportées vers un fichier**. Dans le champ **Indiquez le chemin d'accès complet à un fichier avec extension .xml**, vous pouvez spécifier le chemin d'accès vers lequel Kaspersky Embedded Systems Security exportera les règles d'autorisation dans un fichier XML à l'issue de la tâche Générateur de règles pour le Contrôle du lancement des applications.
   - **Ajouter les informations concernant l'appareil protégé au nom du fichier**

10. Si nécessaire, sous l'onglet **Exclusions**, spécifiez les objets que vous souhaitez exclure de la zone d'action de la tâche.

11. Cliquez sur le bouton **OK** dans la fenêtre **Générateur de règles pour le Contrôle du lancement des applications**.

Création des règles à l'aide d'une tâche de groupe Génération des règles du Contrôle du lancement des applications.

Pour créer des règles à l'aide d'une tâche de groupe Générateur de règles pour le Contrôle du lancement des applications, procédez comme suit :

1. Créez une tâche de groupe *Générateur de règles pour le Contrôle du lancement des applications* ou sélectionnez une tâche existante.

2. Configurez la tâche Générateur de règles pour le Contrôle du lancement des applications.

3. Lancer la tâche Générateur de règles pour le Contrôle du lancement des applications.

Une fois la tâche terminée, en fonction de ses paramètres :

- Si vous avez spécifié l'action **Ajouter des règles d'autorisation à la liste des règles du Contrôle du lancement des applications** à l'issue de la tâche, les règles du Contrôle du lancement des applications générées sont ajoutées à la liste dans les paramètres du Contrôle du lancement des applications dans la Console de l'application.

- Si vous avez spécifié l'action **Les règles d'autorisation seront exportées dans un fichier** à l'issue de la tâche, les règles du Contrôle du lancement des applications générées sont enregistrées dans un fichier XML dans le chemin d'accès spécifié dans les paramètres de la tâche.

Les listes contiennent les règles d'autorisation pour le lancement des applications dont le type correspond aux paramètres de la tâche de groupe Générateur de règles pour le Contrôle du lancement des applications.

Contrôle des appareils

Le Contrôle des appareils gère l'accès des utilisateurs aux appareils installés ou connectés à un ordinateur (par exemple, disques durs, caméra ou module Wi-Fi). Cela permet de protéger l'ordinateur contre l'infection lors de la connexion de ces appareils et de prévenir la perte ou la fuite de données.

Le Contrôle des appareils offre les fonctionnalités suivantes :

- Gestion des autorisations d'accès des utilisateurs aux appareils de stockage (par exemple, disques amovibles, téléphones mobiles, lecteurs de CD/DVD, etc.).
- Contrôle de la connexion d'appareils sans système de fichiers (par exemple, modems externes, adaptateurs Bluetooth, claviers USB, etc.).
- Administration des connexions Wi-Fi.

Par défaut, le Contrôle des appareils est désactivé. Lorsque vous activez le Contrôle des appareils, Kaspersky Embedded Systems Security refuse l'accès par défaut aux types d'appareils suivants :

- Disques amovibles (y compris clés USB)
- Disquettes
- Lecteurs de CD/DVD
- Appareils portables (MTP)
- Modems.
- Appareils de lecture des cartes à puce
- Adaptateurs réseau externes
- Bluetooth (sauf appareils d'entrée)

Niveaux du Contrôle des appareils

Kaspersky Embedded Systems Security contrôle l'accès aux appareils aux niveaux suivants :

1. **Type d'appareil**.

   Lors de la connexion d'un appareil à l'ordinateur, le système d'exploitation détermine le type de l'appareil : imprimante, disque amovible, lecteur de CD/DVD, etc. À ce niveau, vous pouvez autoriser ou interdire la connexion d'appareils selon le type.

2. **Bus de connexion**.

   Un *bus de connexion* est l'interface permettant de connecter des appareils à l'ordinateur. Certains types d'appareils possèdent plusieurs interfaces de connexion. Par exemple, vous pouvez connecter une imprimante à un port USB ou à un port série (COM).

   Ce niveau permet d'autoriser ou d'interdire l'accès aux appareils en fonction du bus de connexion.

Par exemple, imaginons que vous ayez refusé l'accès via USB. Kaspersky Embedded Systems Security refuse l'accès à tous les types d'appareils avec le mode **Dépend du bus de connexion** lorsqu'il est connecté via USB.

> Si le mode d'accès **Autoriser** ou **Interdire** est sélectionné pour l'appareil, le contrôle d'accès ne tient pas compte du bus de connexion de l'appareil.

3. **Appareils de confiance**

   Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Modes de fonctionnement du Contrôle des appareils

Le Contrôle des appareils fonctionne dans les modes suivants :

- **Mode actif**.

  Kaspersky Embedded Systems Security interdit ou autorise des appareils en fonction des règles d'accès aux appareils configurées. L'application autorise également l'accès aux appareils de confiance. L'application enregistre les événements de connexion et de déconnexion des appareils.

- **Informer**.

  Kaspersky Embedded Systems Security autorise tous les appareils et consigne les événements correspondants. Tous les appareils sont autorisés. Il s'agit du mode par défaut. Vous pouvez activer ce mode pour réaliser un audit des appareils dans votre organisation et utiliser ces informations pour dresser une liste d'appareils de confiance.

Règles d'accès aux appareils

Une *règle d'accès aux appareils* est un ensemble de paramètres qui déterminent comment les utilisateurs peuvent accéder aux appareils qui sont installés sur l'ordinateur ou connectés à celui-ci. Ces paramètres comprennent l'accès à un appareil particulier, un calendrier d'accès, des autorisations de lecture ou d'écriture et d'autres. Chaque ensemble de paramètres de règle d'accès se distingue en fonction du type d'appareils.

Paramètres de règle d'accès

Appareils	Affectation des utilisateurs/groupes d'utilisateurs	Planification de l'accès à l'appareil	Autorisation en lecture/en écriture	Surveillance du bus de connexion
Disques durs	✓	✓	✓	✓
Disques amovibles (y compris clés USB)	✓	✓	✓	✓
Disquettes	✓	✓	✓	✓
Lecteurs de CD/DVD	✓	✓	✓	✓
Appareils portables (MTP)	✓	✓	✓	✓
Imprimantes locales	✓	–	–	✓
Imprimantes réseau	✓	–	–	–
Modems	–	–	–	✓
Bannières	–	–	–	✓

Appareils	Affectation des utilisateurs/groupes d'utilisateurs	Planification de l'accès à l'appareil	Autorisation en lecture/en écriture	Surveillance du bus de connexion
Appareils multifonctions	–	–	–	✓
Appareils de lecture des cartes à puce	–	–	–	✓
Appareils Windows CE USB ActiveSync	–	–	–	✓
Adaptateurs réseau externes	–	–	–	✓
Bluetooth	–	–	–	–
Caméras et scanners	–	–	–	✓
Wi-Fi	–	–	–	–
Claviers USB	–	–	–	✓
Souris USB	–	–	–	✓

Gestion de l'accès aux appareils par type

Contrôle des appareils permet de gérer l'accès aux appareils par type. Le type de l'appareil est déterminé par le système d'exploitation au moment de la connexion de l'appareil. Vous pouvez rechercher le type d'appareil à l'aide de l'outil Gestionnaire d'appareils intégré au système d'exploitation. Pour gérer l'accès aux appareils, vous devez configurer les règles. Une *règle d'accès aux appareils* est un ensemble de paramètres qui déterminent comment les utilisateurs peuvent accéder aux appareils qui sont installés sur l'ordinateur ou connectés à celui-ci. Ces paramètres comprennent l'accès à un appareil particulier, un calendrier d'accès, des autorisations de lecture ou d'écriture et d'autres. Chaque ensemble de paramètres de règle d'accès se distingue en fonction du type d'appareils.

Vous pouvez configurer l'accès des appareils de la manière suivante :

- **Autoriser**.

  Kaspersky Embedded Systems Security autorise l'accès complet aux appareils à tous les utilisateurs.

- **Interdire**.

  Kaspersky Embedded Systems Security bloque la connexion de l'appareil. L'application autorise uniquement la connexion aux appareils de confiance.

- **Dépend du bus de connexion**.

  Kaspersky Embedded Systems Security identifie le bus de connexion de l'appareil et effectue un contrôle d'accès conformément au mode d'accès du bus de connexion. L'application permet également de connecter des appareils fiables.

- **Selon les règles**.

  Pour certains types d'appareils, vous pouvez sélectionner des utilisateurs ou un groupe d'utilisateurs qui seront autorisés à utiliser les appareils et configurer un calendrier d'accès aux appareils et des autorisations de lecture et d'écriture. L'application autorise également la connexion aux appareils de confiance.

Soyez prudent lors de la configuration de l'accès aux appareils de type **Disques durs**. Si vous bloquez l'accès au disque système, l'application peut provoquer un blocage avec écran bleu (BSOD) lors du démarrage du système d'exploitation.

Si un appareil n'entre pas dans le schéma de classification du Contrôle des appareils, l'accès à cet appareil ne peut pas être restreint.

Comment contrôler l'accès aux appareils par type dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
5. Cochez la case **Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.
7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.
8. Configurer les règles d'accès aux appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus de connexion**, **Selon les règles**.

   Pour sélectionner le mode d'accès **Selon les règles**, vous devez double-cliquer dessus pour ouvrir les propriétés de la règle d'accès.

   b. Si vous avez sélectionné le mode d'accès **Dépend du bus de connexion**, accédez à l'écran **Bus de connexion** et configurez les règles d'accès aux interfaces de connexion.

   c. Pour les appareils de stockage (par exemple, les disques amovibles), vous pouvez configurer les privilèges d'accès de chaque utilisateur. Vous pouvez également configurer une planification d'accès aux appareils et configurer des autorisations de lecture et d'écriture.

   d. Si nécessaire, configurez les règles d'impression.

   e. Si nécessaire, configurez des règles de connexion Wi-Fi.
9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment contrôler l'accès aux appareils par type dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Contrôle de l'activité locale → Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.
5. Cochez la case **Activer le Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

8. Configurer les règles d'accès aux appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus de connexion**, **Selon les règles**.

      Si le mode d'accès ne se trouve pas dans le menu déroulant, ouvrez les propriétés de la règle d'accès en double-cliquant sur le type d'appareil.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus de connexion**, vous devez revenir à la fenêtre avec les paramètres généraux du Contrôle des appareils, cliquer sur **Bus de connexion** et configurer les règles d'accès aux interfaces de connexion.

   c. Pour les appareils de stockage (par exemple, les disques amovibles), vous pouvez configurer les privilèges d'accès de chaque utilisateur. Vous pouvez également configurer une planification d'accès aux appareils et configurer des autorisations de lecture et d'écriture.

   d. Si nécessaire, configurez les règles d'impression.

   e. Si nécessaire, configurez des règles de connexion Wi-Fi.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment contrôler l'accès aux appareils par type dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Configurer les règles d'accès aux appareils :

   a. Sélectionner le mode d'accès : **Autoriser**, **Interdire**, **Dépend du bus de connexion**, **Selon les règles**.

      Pour sélectionner le mode d'accès **Selon les règles**, vous devez double-cliquer dessus pour ouvrir les propriétés de la règle d'accès.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus de connexion**, vous devez configurer les règles d'accès aux interfaces de connexion sous l'onglet **Bus de connexion**.

   c. Pour les appareils de stockage (par exemple, les disques amovibles), vous pouvez configurer les privilèges d'accès de chaque utilisateur. Vous pouvez également configurer une planification d'accès aux appareils et configurer des autorisations de lecture et d'écriture.

d. Si nécessaire, configurez les règles d'impression.

e. Si nécessaire, configurez des règles de connexion Wi-Fi.

7. Enregistrez vos modifications.

Par conséquent, lorsqu'un utilisateur tente d'accéder à un appareil, l'application bloque l'accès conformément aux règles. Kaspersky Embedded Systems Security consigne également l'événement correspondant. Si vous souhaitez autoriser l'accès à des appareils isolés, vous pouvez ajoutez ces appareils à la liste des appareils de confiance.

Contrôle des connexions Wi-Fi

Le Contrôle des appareils permet de gérer la connexion Wi-Fi de l'ordinateur (terminal). Les réseaux Wi-Fi publics peuvent être non sécurisés, et leur utilisation peut entraîner une perte de données. Le Contrôle des appareils vous permet de bloquer la connexion d'un utilisateur au réseau Wi-Fi ou de l'autoriser à se connecter uniquement aux réseaux de confiance. Par exemple, vous pouvez autoriser la connexion uniquement au réseau Wi-Fi de l'entreprise qui est suffisamment sécurisé. Le Contrôle des appareils bloquera l'accès à tous les réseaux Wi-Fi, à l'exception de ceux qui figurent dans la liste des réseaux de confiance.

Sur les ordinateurs fonctionnant sous Windows 11, vous devez activer le service de localisation pour contrôler les connexions Wi-Fi. Pour ce faire, vous devez activer le **Services d'emplacement** dans les paramètres du système d'exploitation (**Paramètres** → **Confidentialité & sécurité** → **Emplacement**). Si le service de localisation est désactivé, Kaspersky Embedded Systems Security ne contrôle pas la connexion aux réseaux Wi-Fi.

Comment limiter les connexions Wi-Fi dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
5. Cochez la case **Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.
7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.

8. Pour les appareils **Wi-Fi**, configurez une règle d'accès :

    a. Sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Interdire avec des exceptions**.

    b. Si vous avez sélectionné le mode **Interdire avec des exceptions**, vous devez créer une liste de réseaux Wi-Fi de confiance :

        1. Double-cliquez sur le type d'appareil **Wi-Fi** pour ouvrir la liste des réseaux Wi-Fi de confiance.

        2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

        3. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance :

            - **Nom du réseau**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.
            - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.
            - **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.
            - **Commentaires**. Plus d'informations sur le réseau Wi-Fi ajouté.

    Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

    > Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment limiter les connexions Wi-Fi dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

    La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

    La fenêtre **Contrôle des appareils** s'ouvre.

5. Cochez la case **Activer le Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

    La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

8. Double-cliquez sur le type d'appareil **Wi-Fi** pour ouvrir les propriétés des règles d'accès.

9. Sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Interdire avec des exceptions**.

10. Si vous avez sélectionné le mode **Interdire avec des exceptions**, vous devez créer une liste de réseaux Wi-Fi de confiance :

    1. Cliquez sur le bouton **Ajouter** dans le groupe **Réseaux Wi-Fi de confiance**.

    2. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance :

        - **Nom du réseau**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.
        - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.
        - **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.
        - **Commentaires**. Plus d'informations sur le réseau Wi-Fi ajouté.

    Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

    > Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

11. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment limiter les connexions Wi-Fi dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Pour les appareils **Wi-Fi**, configurez une règle d'accès :

    a. Sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Interdire avec des exceptions**.

    b. Si vous avez sélectionné le mode **Interdire avec des exceptions**, vous devez créer une liste de réseaux Wi-Fi de confiance :

        1. Double-cliquez sur le type d'appareil **Wi-Fi** pour ouvrir la liste des réseaux Wi-Fi de confiance.

        2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.

        3. Une fenêtre s'ouvre ; dans cette fenêtre, configurez le réseau Wi-Fi de confiance :

            - **Nom du réseau**. Nom ou SSID (Service Set Identifier) du réseau Wi-Fi.
            - **Type d'authentification**. Type d'authentification utilisé lors de la connexion au réseau Wi-Fi.

- **Type de chiffrement**. Type de chiffrement utilisé pour protéger le trafic du réseau Wi-Fi.
- **Commentaires**. Plus d'informations sur le réseau Wi-Fi ajouté.

Vous pouvez afficher les paramètres du réseau Wi-Fi de confiance dans les paramètres du routeur.

> Le réseau Wi-Fi est considéré de confiant si ses paramètres correspondent à tous les paramètres définis dans la règle.

7. Enregistrez vos modifications.

Par conséquent, lorsqu'un utilisateur tente de se connecter à un réseau Wi-Fi qui n'est pas répertorié comme étant de confiance, l'application bloque la connexion.

Contrôle de l'impression

Le Contrôle des appareils permet de configurer l'accès des utilisateurs aux imprimantes locales et réseau.

Contrôle de l'imprimante locale

Kaspersky Embedded Systems Security contrôle la connexion de l'imprimante locale via les bus suivants : USB, Port série, Port parallèle (LPT).

> Kaspersky Embedded Systems Security contrôle la connexion des imprimantes locales aux ports COM et LPT uniquement au niveau du bus. Autrement dit, pour empêcher la connexion des imprimantes aux ports COM et LPT, pour le type d'appareil **Imprimantes locales**, sélectionnez le mode **Dépend du bus de connexion** et interdisez la connexion des appareils aux bus COM et LPT.

Pour les imprimantes connectées en USB, l'application exerce un contrôle à deux niveaux : type d'appareil (imprimantes locales) et bus de connexion (USB).

Vous pouvez sélectionner l'un des modes d'accès suivants aux imprimantes locales via USB :

- **Autoriser**. Kaspersky Embedded Systems Security accorde l'accès complet aux imprimantes locales à tous les utilisateurs. Les utilisateurs peuvent connecter des imprimantes et imprimer des documents par les moyens fournis par le système d'exploitation.
- **Interdire**. Kaspersky Embedded Systems Security bloque la connexion des imprimantes locales. L'application n'autorise la connexion qu'à des imprimantes de confiance.
- **Dépend du bus de connexion**. Kaspersky Embedded Systems Security autorise la connexion aux imprimantes locales en fonction de l'état de la connexion au bus USB (**Autoriser** ✓ ou **Interdire** ⊘).
- **Selon les règles**. Pour contrôler l'impression, vous devez ajouter des *règles d'impression*. Dans les règles, vous pouvez sélectionner les utilisateurs ou un groupe d'utilisateurs pour lesquels vous souhaitez autoriser ou bloquer l'accès à l'impression de documents sur des imprimantes locales.

Contrôle des imprimantes réseau

Kaspersky Embedded Systems Security permet de configurer l'accès à l'impression sur les imprimantes réseau. Vous pouvez sélectionner l'un des modes d'accès suivants sur les imprimantes réseau :

- **Autoriser et ne pas enregistrer** . Kaspersky Embedded Systems Security ne contrôle pas l'impression sur les imprimantes réseau. L'application accorde l'accès à l'impression à tous les utilisateurs et n'enregistre pas les informations sur l'impression dans le journal des événements.
- **Autoriser** . Kaspersky Embedded Systems Security accorde l'accès à l'impression sur les imprimantes du réseau à tous les utilisateurs.
- **Interdire** . Kaspersky Embedded Systems Security limite l'accès aux imprimantes réseau pour tous les utilisateurs. L'application n'autorise l'accès qu'aux imprimantes de confiance.
- **Selon les règles**. Pour contrôler l'impression, vous devez ajouter des *règles d'impression*. Dans les règles, vous pouvez sélectionner les utilisateurs ou un groupe d'utilisateurs pour lesquels vous souhaitez autoriser ou bloquer l'accès à l'impression de documents sur des imprimantes réseau.

Ajout de règles d'impression pour les imprimantes

Comment ajouter des règles d'impression dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
5. Cochez la case **Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.
7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.
8. Configurez les règles d'accès à l'imprimante :

   a. Pour les types d'appareils **Imprimantes locales** et **Imprimantes réseau**, configurez les règles d'accès suivante : **Autoriser**, **Interdire**, **Autoriser et ne pas enregistrer** (uniquement pour les imprimantes réseau), **Dépend du bus de connexion** (uniquement pour les imprimantes locales) et **Selon les règles**.

   b. Si vous avez sélectionné le mode d'accès **Dépend du bus de connexion**, accédez à l'écran **Bus de connexion** et configurez les règles d'accès aux interfaces de connexion.

c. Si vous sélectionnez le mode d'accès **Selon les règles**, vous devez configurer les règles d'impression :

1. Double-cliquez sur le type d'appareil **Imprimantes locales** et **Imprimantes réseau** pour ouvrir les propriétés des règles d'accès.

2. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle d'impression. Pour ce faire, cliquez sur le bouton **Ajouter**.

   Une fenêtre s'ouvre pour ajouter une nouvelle règle d'impression.

3. Attribuez une priorité à l'*entrée de la règle*. Une entrée de règle comprend les attributs suivants : compte utilisateur, action (autoriser/bloquer) et priorité.

   Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

   Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

   Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

4. Sous **Action**, configurez l'accès de l'utilisateur à l'impression sur l'imprimante.

5. Cliquez sur **Utilisateurs et groupes** et sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

6. Cliquez sur **OK**.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment ajouter des règles d'impression dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.

5. Cochez la case **Activer le Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

8. Configurez les règles d'accès à l'imprimante :

   a. Pour les types d'appareils **Imprimantes locales** et **Imprimantes réseau**, sélectionnez un mode d'accès : **Autoriser**, **Bloquer**, **Autoriser et ne pas enregistrer** (uniquement pour les imprimantes réseau), **Dépend du bus de connexion** (uniquement pour les imprimantes locales) ou **Selon les règles**.

   Si le mode d'accès ne se trouve pas dans le menu déroulant, ouvrez les propriétés de la règle d'accès en double-cliquant sur le type d'appareil.

   b. Si vous sélectionnez le mode d'accès **Dépend du bus de connexion**, vous devez revenir à la fenêtre des paramètres généraux du module Contrôle des appareils, cliquer sur **Bus de connexion** et configurer les règles d'accès aux interfaces de connexion.

   c. Si vous devez configurer l'impression :

      1. Double-cliquez sur le type d'appareil **Imprimantes locales** ou **Imprimantes réseau** pour ouvrir les propriétés des règles d'accès.

      2. Sélectionnez le mode d'accès **Selon les règles**.

      3. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle d'impression. Pour ce faire, cliquez sur le bouton **Ajouter**.

         Une fenêtre s'ouvre pour ajouter une nouvelle règle d'impression.

      4. Attribuez une priorité à l'*entrée de la règle*. Une entrée de règle comprend les attributs suivants : compte utilisateur, action (autoriser/bloquer) et priorité.

         Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

         Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

         Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

      5. Sous **Action**, configurez l'accès de l'utilisateur à l'impression sur l'imprimante.

      6. Sous **Utilisateurs et groupes**, cliquez sur **Ajouter** et sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

      7. Cliquez sur **OK**.

9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment ajouter des règles d'impression dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Configurez les règles d'accès à l'imprimante :

   a. Pour les types d'appareils **Imprimantes locales** et **Imprimantes réseau**, configurez les règles d'accès suivante : **Autoriser**, **Interdire**, **Autoriser et ne pas enregistrer** (uniquement pour les imprimantes réseau), **Dépend du bus de connexion** (uniquement pour les imprimantes locales) et **Selon les règles**.

   b. Si vous avez sélectionné le mode d'accès **Dépend du bus de connexion**, accédez à l'écran **Bus de connexion** et configurez les règles d'accès aux interfaces de connexion.

   c. Si vous sélectionnez le mode d'accès **Selon les règles**, vous devez configurer les règles d'impression :

      1. Double-cliquez sur le type d'appareil **Imprimantes locales** et **Imprimantes réseau** pour ouvrir les propriétés des règles d'accès.

      2. Sélectionnez les utilisateurs ou groupes d'utilisateurs auxquels vous souhaitez appliquer la règle d'impression. Pour ce faire, cliquez sur le bouton **Ajouter**.

         Une fenêtre s'ouvre pour ajouter une nouvelle règle d'impression.

      3. Attribuez une priorité à l'*entrée de la règle*. Une entrée de règle comprend les attributs suivants : compte utilisateur, action (autoriser/bloquer) et priorité.

         Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

         Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

         Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

      4. Sous **Action**, configurez l'accès de l'utilisateur à l'impression sur l'imprimante.

5. Cliquez sur **Utilisateurs et groupes** et sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès à l'impression. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

6. Cliquez sur **OK**.

7. Enregistrez vos modifications.

Contrôle des appareils d'entrée (HID)

Les appareils d'entrée incluent les claviers, les souris, les boules de commande, les pavés tactiles et les autres appareils du même type. Il est possible de connecter des appareils d'entrée via les interfaces suivantes : USB, Bluetooth, port PS/2, port RS-232 (COM), port IR, etc.

Kaspersky Embedded Systems Security permet de contrôler les souris et les claviers USB et Bluetooth. Le Contrôle des appareils consigne les connexions et les déconnexions des appareils en entrée.

Lorsque des appareils Bluetooth sont connectés ou déconnectés, l'application peut créer plusieurs événements sur l'appareil. La raison en est que le système d'exploitation peut détecter un appareil Bluetooth comme plusieurs appareils de types différents. Kaspersky Embedded Systems Security gère également l'adaptateur Bluetooth via lequel l'appareil est connecté en tant qu'appareil distinct. C'est pourquoi l'application crée un événement pour chacun des appareils détectés.

Kaspersky Embedded Systems Security permet d'autoriser ou d'interdire l'utilisation d'un appareil d'entrée, ainsi que de dresser une liste des appareils de confiance.

Comment activer le Contrôle des appareils dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.

4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.

5. Cochez la case **Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.

8. Pour le type d'appareil **Bluetooth**, sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Autoriser et ne pas enregistrer**.

   Vous pouvez interdire ou autoriser tous les appareils Bluetooth, ou vous pouvez autoriser la connexion uniquement aux appareils d'entrée Bluetooth (classe HID : appareils d'interface humaine).

Vous pouvez autoriser la connexion des appareils d'entrée uniquement dans Kaspersky Security Center Web Console. Vous ne pouvez pas autoriser la connexion des appareils de saisie dans la Console d'administration (MMC) ou Kaspersky Embedded Systems Security Console.

9. Pour les types d'appareils **Claviers USB** et **Souris USB**, sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Dépend du bus de connexion**.
10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer le Contrôle des appareils dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Contrôle de l'activité locale → Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.
5. Cochez la case **Activer le Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.
7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.
8. Cliquez sur le type d'appareil **Bluetooth** pour ouvrir les propriétés de la règle d'accès.
9. Sélectionnez un mode d'accès : **Autoriser**, **Bloquer** ou **Autoriser et ne pas enregistrer**.

   Vous pouvez interdire ou autoriser tous les appareils Bluetooth, ou vous pouvez autoriser la connexion uniquement aux appareils d'entrée Bluetooth (classe HID : appareils d'interface humaine).
10. Pour les types d'appareils **Claviers USB** et **Souris USB**, sélectionnez un mode d'accès : **Autoriser**, **Bloquer** ou **Dépend du bus de connexion**.
11. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer le Contrôle des appareils dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.
2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.
3. Cochez la case **Contrôle des appareils**.
4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Pour le type d'appareil **Bluetooth**, sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Autoriser et ne pas enregistrer**.

   Vous pouvez interdire ou autoriser tous les appareils Bluetooth, ou vous pouvez autoriser la connexion uniquement aux appareils d'entrée Bluetooth (classe HID : appareils d'interface humaine).

   > Vous pouvez autoriser la connexion des appareils d'entrée uniquement dans Kaspersky Security Center Web Console. Vous ne pouvez pas autoriser la connexion des appareils de saisie dans la Console d'administration (MMC) ou Kaspersky Embedded Systems Security Console.

7. Pour les types d'appareils **Claviers USB** et **Souris USB**, sélectionnez un mode d'accès : **Autoriser**, **Interdire** ou **Dépend du bus de connexion**.

8. Enregistrez vos modifications.

Gestion de l'accès aux appareils mobiles

Kaspersky Embedded Systems Security vous permet de contrôler l'accès aux données sur les appareils mobiles fonctionnant sous Android et iOS. Les appareils mobiles appartiennent à la catégorie des appareils portables (MTP). Par conséquent, pour configurer l'accès aux données sur les appareils mobiles, vous devez modifier les paramètres d'accès relatifs aux appareils portables (MTP).

Lorsqu'un appareil portable se connecte à un ordinateur, le système d'exploitation en détermine le type. Si iTunes ou des applications similaires sont installés sur l'ordinateur Android Debug Bridge (pour en savoir plus sur l'application ADB, consultez la Base de connaissances et le site Internet de l'assistance technique Android), le système d'exploitation identifie les appareils mobiles comme des appareils ADB ou iTunes. Dans les autres cas, le système d'exploitation peut déterminer le type d'appareil mobile en tant qu'appareil portable (MTP) pour transférer des fichiers, en tant qu'appareil PTP (appareil photo) pour transférer des images ou en tant qu'autre appareil. Le type d'appareil dépend du modèle de l'appareil mobile et du mode de connexion USB sélectionné. Kaspersky Embedded Systems Security vous permet de configurer des autorisations d'accès individuelles pour les données des appareils mobiles dans les applications ADB, iTunes ou le gestionnaire de fichiers. Dans tous les autres cas, le Contrôle des appareils autorise l'accès aux appareils mobiles conformément aux règles d'accès aux appareils portables (MTP).

Accès aux appareils mobiles

Les appareils mobiles appartiennent à la catégorie des appareils portables (MTP), par conséquent, leurs paramètres sont les mêmes. Vous pouvez sélectionner l'un des modes d'accès suivants aux appareils mobiles :

- **Autoriser**. Kaspersky Embedded Systems Security accorde un accès complet aux appareils mobiles. Vous pouvez ouvrir, créer, modifier, copier ou supprimer des fichiers sur les appareils mobiles à l'aide du gestionnaire de fichiers ou des applications ADB et iTunes. Vous pouvez également charger la batterie de l'appareil en connectant l'appareil mobile à un port USB de l'ordinateur.

- **Interdire**. Kaspersky Embedded Systems Security restreint l'accès aux appareils mobiles dans le gestionnaire de fichiers et dans les applications ADB et iTunes. L'application n'autorise l'accès qu'aux appareils mobiles de confiance. Vous pouvez également charger la batterie de l'appareil en connectant l'appareil mobile à un port USB de l'ordinateur.

- **Dépend du bus de connexion**. Kaspersky Embedded Systems Security autorise la connexion aux appareils mobiles en fonction de l'état de la connexion au bus USB (**Autoriser** ou **Interdire**).

- **Selon les règles**. Kaspersky Embedded Systems Security restreint l'accès aux appareils mobiles conformément aux règles. Dans les règles, vous pouvez configurer les autorisations d'accès (lecture/écriture), sélectionner les utilisateurs ou le groupe ayant accès aux appareils mobiles et configurer une planification de l'accès aux appareils mobiles. Vous pouvez également restreindre l'accès aux données des appareils mobiles via les applications ADB et iTunes.

Configuration des règles d'accès aux appareils mobiles

Les règles d'accès pour les appareils portables (MTP), les appareils ADB et les appareils iTunes sont configurées différemment. Pour les appareils portables (MTP) et les appareils ADB, vous pouvez configurer des règles pour des utilisateurs individuels ou des groupes d'utilisateurs et créer un programme selon lequel les règles s'appliqueront. Pour les appareils iTunes, cette opération n'est pas possible. Vous pouvez uniquement autoriser ou refuser l'accès aux données via l'application iTunes pour tous les utilisateurs.

Comment configurer les règles d'accès aux appareils mobiles dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.
6. Dans le menu contextuel relatif au type d'appareil **Appareils portables (MTP)**, configurez le mode d'accès aux appareils mobiles : **Autoriser**, **Interdire** ou **Dépend du bus de connexion**.
7. Pour configurer les règles d'accès aux appareils mobiles, double-cliquez pour ouvrir la liste des règles.

8. Configurer la règle d'accès aux appareils mobiles :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

      Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils mobiles.

   b. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) et priorité.

      Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

      Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

      Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

   c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

9. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils mobiles pour les utilisateurs.

   Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

10. Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

11. Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

    Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

12. Sous **Accès via iTunes**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

    Kaspersky Embedded Systems Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.

13. Enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils mobiles dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.
5. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur le lien **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.
6. Sélectionnez le type d'appareil **Appareils portables (MTP)**.

   Cette action ouvre les droits d'accès aux appareils portables (MTP).
7. Configurez le mode d'accès aux appareils mobiles : **Autoriser**, **Interdire**, **Dépend du bus de connexion** ou **Selon les règles**.
8. Sous **Accès via iTunes**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

   Kaspersky Endpoint Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.
9. Si vous sélectionnez le mode **Selon les règles**, vous devez ajouter des règles d'accès pour les appareils. Pour ce faire, sous **Utilisateurs**, cliquez sur le bouton **Ajouter** et configurez la règle d'accès aux appareils mobiles :

   a. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) et priorité.

   Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

   Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

   Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

   b. Sous **Utilisateurs**, sélectionnez les utilisateurs ou les groupes d'utilisateurs qui auront accès aux appareils mobiles. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

c. Sous **Planification de l'accès aux appareils**, configurez une planification d'accès aux appareils mobiles pour les utilisateurs.

> Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

d. Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

e. Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

10. Enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils mobiles dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Sélectionnez l'onglet **Types d'appareils**.

La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

4. Dans le menu contextuel relatif au type d'appareil **Appareils portables (MTP)**, configurez le mode d'accès aux appareils mobiles : **Autoriser**, **Interdire** ou **Dépend du bus de connexion**.

5. Pour configurer les règles d'accès aux appareils mobiles, double-cliquez pour ouvrir la liste des règles.

6. Configurer la règle d'accès aux appareils mobiles :

a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

Cette action ouvre une fenêtre permettant d'ajouter une nouvelle règle d'accès aux appareils mobiles.

b. Dans le champ **Priorité**, définissez la priorité d'écriture de la règle. Une règle comprend les attributs suivants : compte d'utilisateur, planification, autorisations (lecture/écriture/accès ADB) et priorité.

Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

d. Cliquez sur **OK**.

7. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils mobiles pour les utilisateurs.

   Il n'est pas possible de configurer une planification d'accès distincte pour les appareils ADB. Vous pouvez configurer une planification d'accès commune pour les appareils ADB et les appareils portables (MTP).

8. Configurez les autorisations d'accès des utilisateurs aux appareils mobiles dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

9. Configurez l'accès aux données sur un appareil mobile via l'application ADB à l'aide de la case **Accès via ADB**.

   Si la case est décochée, lorsque l'appareil mobile est connecté, l'application ADB ne peut pas détecter l'appareil.

10. Sous **Accès via iTunes**, configurez l'accès aux données sur l'appareil mobile via l'application iTunes.

    Kaspersky Embedded Systems Security applique les paramètres d'accès aux appareils mobiles via l'application iTunes pour tous les utilisateurs. Il n'est pas possible de configurer une planification d'accès distincte pour les appareils iTunes.

11. Enregistrez vos modifications.

L'accès des utilisateurs aux appareils mobiles est dès lors limité conformément aux règles. Si vous avez interdit l'accès aux appareils mobiles dans les applications ADB et iTunes, lorsque vous connectez un appareil mobile, les applications ADB et iTunes ne peuvent pas le détecter.

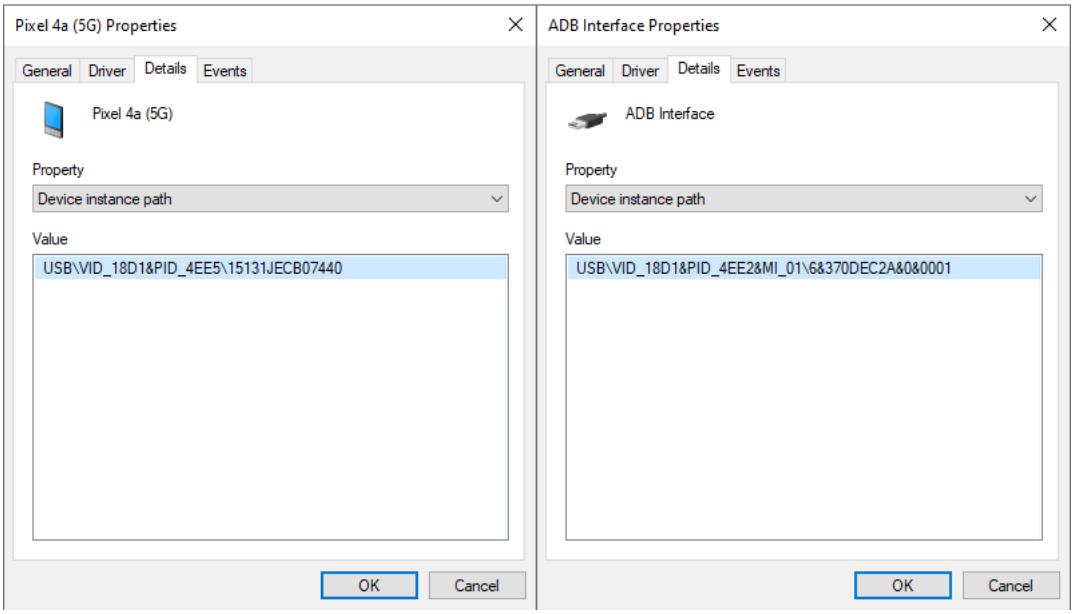
Appareils mobiles de confiance

La procédure d'ajout d'un appareil mobile de confiance est exactement la même que pour les autres types d'appareils de confiance. Vous pouvez ajouter un appareil mobile par identifiant ou par modèle d'appareil.

Pour ajouter un appareil mobile de confiance par identifiant, vous aurez besoin d'un identifiant unique (Hardware ID – HWID). Vous pouvez trouver l'identifiant dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). L'outil Device Manager vous permet de réaliser cette opération. Les identifiants des appareils portables (MTP) ainsi que des appareils ADB et iTunes sont différents même pour le même appareil mobile. L'identifiant d'un appareil portable (MTP) peut ressembler à ceci : `15131JECB07440`. L'identifiant d'un appareil ADB peut se présenter comme suit : `6&370DEC2A&0&0001`. L'ajout d'appareils par ID est pratique si vous souhaitez ajouter plusieurs appareils particuliers. Vous pouvez également utiliser des masques.

Si vous avez installé les applications ADB ou iTunes après avoir connecté l'appareil à l'ordinateur, l'identifiant unique de l'appareil peut être réinitialisé. En d'autres termes, Kaspersky Embedded Systems Security identifie cet appareil comme nouveau. S'il s'agit d'un appareil de confiance, ajoutez-le à nouveau à la liste des appareils de confiance.

Pour ajouter un appareil mobile de confiance par modèle d'appareil, vous avez besoin de son Vendor ID (VID) et de son Product ID (PID). Vous pouvez trouver les identifiants dans les propriétés de l'appareil en utilisant les outils du système d'exploitation (voir la figure ci-dessous). Modèle de saisie du VID et du PID : `VID_18D1&PID_4EE5`. L'ajout d'appareil par modèle est pratique si vous utilisez des appareils d'un certain modèle dans votre organisation. Ainsi, vous pouvez ajouter tous les appareils de ce modèle.



L'identifiant de l'appareil dans le Gestionnaire des appareils

Surveillance de l'utilisation des disques amovibles

La surveillance de l'utilisation des disques amovibles comprend :

- La surveillance des opérations exécutées sur les fichiers des disques amovibles.
- La surveillance de la connexion et de la déconnexion des disques amovibles de confiance.

  Kaspersky Embedded Systems Security permet de surveiller la connexion et la déconnexion de tous les appareils de confiance et pas seulement des disques amovibles. Vous pouvez activer l'enregistrement des événements dans le journal dans les paramètres de notification du module Contrôle des appareils. Les événements présentent le niveau de gravité *Informations*.

Comment activer la surveillance des opérations sur les fichiers sur les disques amovibles dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
5. Cochez la case **Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.
7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.
8. Sélectionnez le type d'appareil **Disques amovibles** et cliquez sur le bouton **Enregistrement des événements dans le journal**.

   Cette action ouvre la fenêtre d'enregistrement des événements.
9. Cochez la case **Activer l'enregistrement des événements**.
10. Dans le groupe **Opérations sur les fichiers**, sélectionnez les opérations que vous voulez surveiller : **Écriture**, **Suppression**.
11. Dans le groupe **Filtrer selon les formats de fichiers**, sélectionnez les formats des fichiers dont les opérations associées doivent être enregistrées par le Contrôle des appareils.
12. Sélectionnez les utilisateurs ou le groupe d'utilisateurs dont vous souhaitez surveiller l'utilisation des disques amovibles.
13. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer la surveillance des opérations sur les fichiers sur les disques amovibles dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Contrôle de l'activité locale → Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.
5. Cochez la case **Activer le Contrôle des appareils**.
6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

8. Double-cliquez sur le type d'appareil **Disques amovibles** pour ouvrir les propriétés des règles d'accès.

9. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Enregistrement des événements dans le journal**.

10. Réglez le commutateur à bascule sur **Enregistrement des événements dans le journal ACTIVÉ**.

11. Dans le groupe **Opérations sur les fichiers**, sélectionnez les opérations que vous voulez surveiller : **Écrire**, **Supprimer**.

12. Dans le groupe **Filtrer selon les formats de fichiers**, sélectionnez les formats des fichiers dont les opérations associées doivent être enregistrées par le Contrôle des appareils.

13. Sélectionnez les utilisateurs ou le groupe d'utilisateurs dont vous souhaitez surveiller l'utilisation des disques amovibles.

14. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment activer la surveillance des opérations sur les fichiers sur les disques amovibles dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Sélectionnez le type d'appareil **Disques amovibles** et cliquez sur le bouton **Enregistrement des événements dans le journal**.

   Cette action ouvre la fenêtre d'enregistrement des événements.

7. Cochez la case **Activer l'enregistrement des événements**.

8. Dans le groupe **Opérations sur les fichiers**, sélectionnez les opérations que vous voulez surveiller : **Écriture**, **Suppression**.

9. Dans le groupe **Filtrer selon les formats de fichiers**, sélectionnez les formats des fichiers dont les opérations associées doivent être enregistrées par le Contrôle des appareils.

10. Sélectionnez les utilisateurs ou le groupe d'utilisateurs dont vous souhaitez surveiller l'utilisation des disques amovibles.

11. Enregistrez vos modifications.

Par conséquent, lorsque les utilisateurs génèreront une entrée dans les fichiers situés sur les disques amovibles ou lorsqu'ils les supprimeront, Kaspersky Embedded Systems Security enregistrera les informations sur les opérations réalisées dans le journal des événements et les enverra à Kaspersky Security Center. Vous pouvez consulter les événements liés aux fichiers sur les disques amovibles, dans la Console de Kaspersky Security Center dans l'espace de travail pour l'entrée **Serveur d'administration** de l'onglet **Événements**. Pour que les événements s'affichent dans le journal local des événements de Kaspersky Embedded Systems Security, il faut cocher la case **Exécution d'une opération sur un fichier** dans les paramètres des notifications du module Contrôle des appareils.

Gestion de l'accès aux appareils Bluetooth

Kaspersky Embedded Systems Security permet de gérer l'accès aux appareils Bluetooth. Les appareils Bluetooth incluent les claviers, souris, casques, imprimantes sans fil, etc. Vous pouvez également utiliser le Bluetooth pour la communication, p. ex., avec un appareil mobile.

Lorsque des appareils Bluetooth sont connectés ou déconnectés, l'application peut créer plusieurs événements sur l'appareil. La raison en est que le système d'exploitation peut détecter un appareil Bluetooth comme plusieurs appareils de types différents. Kaspersky Embedded Systems Security gère également l'adaptateur Bluetooth via lequel l'appareil est connecté en tant qu'appareil distinct. C'est pourquoi l'application crée un événement pour chacun des appareils détectés.

Vous pouvez sélectionner l'un des modes d'accès suivants aux appareils Bluetooth :

- **Autoriser et ne pas enregistrer** . Kaspersky Embedded Systems Security permet de connecter n'importe quel appareil Bluetooth et n'enregistre pas les informations sur la connexion dans le journal des événements. Vous pouvez connecter des appareils de saisie Bluetooth (claviers, souris, etc.), envoyer des données via Bluetooth ou encore gérer d'autres appareils Bluetooth (casque, écouteurs, etc.).
- **Autoriser** . Kaspersky Embedded Systems Security permet de connecter n'importe quel appareil Bluetooth. Vous pouvez connecter des appareils de saisie Bluetooth (claviers, souris, etc.), envoyer des données via Bluetooth ou encore gérer d'autres appareils Bluetooth (casque, écouteurs, etc.).
- **Interdire** . Kaspersky Embedded Systems Security restreint l'accès aux appareils Bluetooth. Vous pouvez autoriser la connexion uniquement aux appareils d'entrée Bluetooth (la classe Appareils d'interface humaine). Ces appareils incluent les claviers, les souris, les manettes de jeu, etc.

Il n'est pas possible de créer une liste d'appareils Bluetooth de confiance. Si vous avez restreint l'accès aux appareils Bluetooth, vous ne pouvez connecter que des appareils d'entrée Bluetooth.

Vous pouvez autoriser la connexion des appareils d'entrée uniquement dans la Console de l'application ou dans Kaspersky Security Center Web Console. Vous ne pouvez pas autoriser la connexion des appareils d'entrée dans la Console d'administration de Kaspersky Security Center.

Comment configurer les règles d'accès aux appareils Bluetooth dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur **Paramètres**.

4. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

5. Dans le menu contextuel relatif au type d'appareil **Bluetooth**, configurez le mode d'accès aux appareils Bluetooth : **Autoriser**, **Interdire** ou **Autoriser et ne pas enregistrer**.

   Si vous avez bloqué l'accès aux appareils Bluetooth, vous pouvez autoriser la connexion des appareils d'entrée (claviers, souris, etc.) uniquement dans la Console de l'application ou dans Kaspersky Security Center Web Console. Vous ne pouvez pas autoriser la connexion des appareils d'entrée dans la Console d'administration de Kaspersky Security Center.

6. Enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils Bluetooth dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur **Paramètres**.

5. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur le lien **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

6. Sélectionnez le type d'appareil **Bluetooth**.

   Cette action ouvre les paramètres d'accès aux appareils Bluetooth.

7. Configurez le mode d'accès aux appareils Bluetooth : **Autoriser**, **Bloquer**, **Autoriser et ne pas enregistrer**.

8. Si vous sélectionnez le mode **Bloquer**, vous pouvez autoriser la connexion uniquement des appareils de saisie Bluetooth (claviers, souris, etc.). Pour ce faire, sous **Exclusions**, cochez la case **Appareils d'entrée (souris et claviers)**.

9. Enregistrez vos modifications.

Comment configurer les règles d'accès aux appareils Bluetooth dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur** → **Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   Le tableau énumère les règles d'accès pour tous les appareils qui sont présents dans la classification du module Contrôle des appareils.

4. Sous **Accès**, configurez le mode d'accès aux appareils Bluetooth : **Autoriser**, **Bloquer**, **Autoriser et ne pas enregistrer**.

5. Si vous sélectionnez le mode **Bloquer**, vous pouvez autoriser la connexion uniquement des appareils de saisie Bluetooth (claviers, souris, etc.). Pour ce faire, sous **Exclusions**, cochez la case **Appareils d'entrée (souris et claviers)**.

6. Enregistrez vos modifications.

Différenciation des privilèges d'accès des utilisateurs aux appareils

Vous pouvez configurer les droits d'accès des utilisateurs selon le type d'appareil ou aux appareils de confiance.

Différenciation des droits d'accès des utilisateurs selon le type d'appareil

Le Contrôle des appareils permet de configurer les privilèges d'accès des utilisateurs aux données sur les *appareils de stockage*. Pour ces appareils, vous pouvez configurer les autorisations d'écriture et de lecture. Le Contrôle des appareils prend en charge les types d'appareils de stockage suivants :

- Disques durs
- Disques amovibles
- Disquettes
- Lecteurs de CD/DVD
- Appareils portables (MTP). Les appareils portables (MTP) incluent les appareils mobiles, les appareils photo, les lecteurs multimédias, etc.

Ainsi, vous pouvez par exemple autoriser l'utilisation des supports amovibles uniquement au groupe d'administrateurs. Pour les autres types d'appareils, vous pouvez interdire ou autoriser l'accès à tous les utilisateurs. Vous pouvez également configurer les droits d'accès des utilisateurs aux imprimantes.

Comment configurer les privilèges d'accès des utilisateurs aux données des disques amovibles dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.

4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.

5. Cochez la case **Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   L'onglet **Types d'appareils** présente les règles d'accès pour tous les appareils qui sont inclus dans la classification du Contrôle des appareils.

8. Pour configurer les règles d'accès aux appareils de stockage, double-cliquez pour ouvrir la liste des règles.

9. Configurer la règle d'accès à l'appareil de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

      Cette action ouvre une fenêtre pour ajouter une nouvelle règle d'accès à l'appareil de stockage.

   b. Dans le champ **Priorité**, définissez la priorité de la *règle d'écriture*. Une règle comprend les attributs suivants : compte d'utilisateur, programme, autorisations (lecture/écriture) et priorité.

      Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

      Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

      Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

   c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

10. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

    Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

11. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

12. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment configurer les privilèges d'accès des utilisateurs aux données sur les appareils de stockage dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.

5. Cochez la case **Activer le Contrôle des appareils**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

7. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Règles d'accès pour les appareils et les réseaux Wi-Fi**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

8. Dans le groupe **Accès aux appareils de stockage**, ouvrez les propriétés de la règle d'accès à l'appareil de stockage.

9. Configurer la règle d'accès à l'appareil de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Utilisateurs**.

      Cette action ouvre une fenêtre pour ajouter une nouvelle règle d'accès à l'appareil de stockage.

   b. Dans le champ **Priorité**, définissez la priorité de la *règle d'écriture*. Une règle comprend les attributs suivants : compte d'utilisateur, programme, autorisations (lecture/écriture) et priorité.

      Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

      Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

      Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

   c. Sous **Utilisateurs**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Sous **Planification de l'accès aux appareils**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

      Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

   e. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

   f. Cliquez sur **OK**.

10. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment configurer les privilèges d'accès des utilisateurs aux données sur les appareils de stockage dans la Console de Kaspersky Embedded Systems Security

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez **Bloquer** ou **Informer**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Types d'appareils**.

   La fenêtre qui s'ouvre avec règles d'accès pour tous les appareils qui sont inclus dans la classification du module Contrôle des appareils.

6. Pour configurer les règles d'accès à l'appareil de stockage, double-cliquez pour ouvrir la liste des règles.

7. Configurer la règle d'accès à l'appareil de stockage :

   a. Cliquez sur le bouton **Ajouter** dans le groupe **Règles d'accès**.

      Cette action ouvre une fenêtre pour ajouter une nouvelle règle d'accès à l'appareil de stockage.

   b. Dans le champ **Priorité de la règle**, définissez la priorité de la *règle d'écriture*. Une règle comprend les attributs suivants : compte d'utilisateur, programme, autorisations (lecture/écriture) et priorité.

      Une règle présente une priorité particulière. Si un utilisateur a été ajouté à plusieurs groupes, Kaspersky Embedded Systems Security contrôle l'accès aux appareils en fonction de la règle présentant la priorité la plus élevée. Kaspersky Embedded Systems Security vous permet d'attribuer une priorité comprise entre 0 et 10 000. Plus la valeur est élevée, plus la priorité est élevée. Autrement dit, une entrée dont la valeur est 0 présente la priorité la plus faible.

      Par exemple, vous pouvez accorder des autorisations en lecture seule au groupe Tous et accorder des autorisations en lecture/écriture au groupe des administrateurs. Pour ce faire, attribuez une priorité de 1 au groupe des administrateurs et une priorité de 0 au groupe Tous.

      Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Autrement dit, si un utilisateur a été ajouté à plusieurs groupes et que la priorité de toutes les règles est la même, Kaspersky Embedded Systems Security contrôle l'accès à l'appareil en fonction de n'importe quelle règle de blocage existante.

   c. Sous **Règle pour les utilisateurs et les groupes**, sélectionnez des utilisateurs ou des groupes d'utilisateurs. Vous pouvez sélectionner des utilisateurs dans Active Directory ou saisir un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine.

   d. Cliquez sur **OK**.

8. Sous **Planification pour la règle d'accès sélectionnée**, configurez une planification d'accès aux appareils de stockage pour les utilisateurs.

   Par exemple, vous pouvez autoriser les utilisateurs à utiliser les appareils de stockage uniquement pendant les heures de travail.

9. Configurez les autorisations d'accès des utilisateurs aux appareils de stockage dans le gestionnaire de fichiers (**Lecture** / **Écriture**).

10. Enregistrez vos modifications.

Différenciation des privilèges d'accès des utilisateurs aux appareils de confiance

Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment. Pour pouvoir utiliser les appareils de confiance, vous pouvez accorder l'accès à un utilisateur individuel, à un groupe d'utilisateurs ou à tous les utilisateurs de l'organisation. Vous pouvez configurer les droits d'accès des utilisateurs dans les propriétés de l'appareil de confiance.

À propos du Générateur de règles pour le Contrôle des appareils

Vous pouvez générer des règles du Contrôle des appareils à l'aide de tâches et de stratégies de Kaspersky Security Center simultanément pour tous les appareils protégés et groupes d'appareils protégés du réseau de l'organisation. Pour créer une liste d'appareils de confiance, vous devez réaliser un audit des appareils externes dans votre organisation.

Pour créer une liste de règles basée sur la liste des appareils connectés à un appareil protégé donné, vous pouvez exécuter localement la tâche *Générateur de règles pour le Contrôle des appareils* à l'aide de la Console de l'application.

Vous pouvez créer des règles du Contrôle des appareils à l'aide de Kaspersky Security Center de la manière suivante :

- Avec l'aide de la tâche *Générateur de règles pour le Contrôle des appareils*.

  Selon ses paramètres, la tâche *Générateur de règles pour le Contrôle des appareils* peut collecter des informations sur tous les appareils qui ont déjà été connectés à l'ordinateur et pour lesquels des informations sont stockées dans le système d'exploitation, ou sur les appareils connectés au moment du lancement de la tâche. Sur la base des informations collectées, la tâche génère une liste de règles d'autorisation pour le module Contrôle des appareils. Vous pouvez configurer l'importation automatique des règles générées dans la liste des règles du module Contrôle des appareils ou importer manuellement les règles générées.

  Ce scénario peut être utilisé, par exemple, si vous devez créer rapidement des règles d'autorisation pour les appareils de confiance que vous avez utilisés par le passé avant la première exécution du module Contrôle des appareils.

  Comment exécuter une tâche Générateur de règles pour le Contrôle des appareils dans la Console d'administration de Kaspersky Security Center

  1. Ouvrez la Console d'administration de Kaspersky Security Center.
  2. Dans l'arborescence de la console, sélectionnez **Tâches**.
  3. Sélectionnez la tâche *Générateur de règles pour le Contrôle des appareils* et ouvrez les propriétés de la tâche d'un double-clic.

     Si nécessaire, créez une nouvelle tâche.

4. Dans la section **Mode**, sélectionnez le mode de la tâche :

   - **Prendre en compte les données du système concernant tous les appareils externes qui ont été connectés**.

     L'application obtient des informations sur tous les appareils connectés à l'ordinateur à partir de la mémoire du système d'exploitation.

   - **Ne prendre en compte que les appareils externes actuellement connectés**.

     L'application obtient des informations sur les appareils connectés au lancement de la tâche.

5. Saisissez le chemin d'accès à l'enregistrement du fichier de données.

6. Si vous exécutez la tâche sur plusieurs ordinateurs, nous vous recommandons de cocher la case **Ajouter les informations concernant l'appareil protégé au nom du fichier**.

7. Enregistrez vos modifications.

8. Exécutez la tâche.

Comment lancer une tâche Générateur de règles pour le Contrôle des appareils dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Sélectionnez la tâche *Générateur de règles pour le Contrôle des appareils* et ouvrez les propriétés de la tâche d'un double-clic.

   Si nécessaire, créez une nouvelle tâche.

3. Dans la section **Mode**, sélectionnez le mode de la tâche :

   - **Tenir compte des données du système sur tous les appareils externes connectés à un moment donné**.

     L'application obtient des informations sur tous les appareils connectés à l'ordinateur à partir de la mémoire du système d'exploitation.

   - **Tenir compte uniquement des appareils externes connectés actuellement**.

     L'application obtient des informations sur les appareils connectés au lancement de la tâche.

4. Saisissez le chemin d'accès à l'enregistrement du fichier de données.

5. Si vous exécutez la tâche sur plusieurs ordinateurs, nous vous recommandons de cocher la case **Ajouter les informations concernant l'appareil protégé au nom du fichier**.

6. Enregistrez vos modifications.

7. Exécutez la tâche.

Comment lancer une tâche Générateur de règles pour le Contrôle des appareils dans la Web Console

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Génération automatique de règles → Générateur de règles pour le Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Générateur de règles pour le Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Générateur de règles pour le Contrôle des appareils** s'ouvre.

3. Dans la section **Mode**, sélectionnez le mode de la tâche :

   - **Prendre en compte les données du système concernant tous les appareils externes qui ont été connectés**.

     L'application obtient des informations sur tous les appareils connectés à l'ordinateur à partir de la mémoire du système d'exploitation.

   - **Ne prendre en compte que les appareils externes actuellement connectés**.

     L'application obtient des informations sur les appareils connectés au lancement de la tâche.

4. Dans la section **Après l'achèvement de la tâche**, sélectionnez les actions de l'application une fois que la tâche est terminée :

   - **Ajouter des règles d'autorisation à la liste des règles du Contrôle des appareils**. La liste des règles de contrôle des appareils est disponible dans les paramètres du module Contrôle des appareils.

     Si cette case est sélectionnée, l'application ajoute les règles générées par la tâche à la liste des règles du Contrôle des appareils en fonction du principe sélectionné pour l'ajout de règles.

     Si la case est décochée, l'application n'ajoute pas les règles d'autorisation créées à la liste Règles du Contrôle des appareils. L'application exporte les règles uniquement dans un fichier.

   - **Principe d'ajout**. Méthode utilisée pour ajouter les nouvelles règles d'autorisation à la liste des règles du Contrôle des appareils :

     - **Ajouter aux règles existantes**. L'application ajoute une règle à la liste des règles existantes. Dans ce cas, l'application duplique les règles identiques.

     - **Remplacer les règles existantes**. L'application ajoute de nouvelles règles au lieu des règles existantes.

     - **Fusionner avec les règles existantes**. L'application ajoute une règle à la liste des règles existantes. Dans ce cas, l'application fusionne les règles identiques.

   - **Exporter les règles d'autorisation vers un fichier**. L'application exporte les règles d'autorisation dans le fichier indiqué dans le champ ci-dessous. Vous pouvez ensuite importer le fichier dans les paramètres de l'application sur d'autres ordinateurs pour y diffuser les règles d'autorisation. Le fichier peut également être utilisé pour sauvegarder les règles d'autorisation.

   - **Ajouter les détails de l'appareil protégé au nom du fichier**. En plus de la date et de l'heure, l'application ajoute le nom de l'ordinateur au nom du fichier exporté. Cette option est pratique si vous rassemblez des règles d'autorisation provenant de plusieurs ordinateurs.

5. Enregistrez vos modifications.

Par conséquent, Kaspersky Embedded Systems Security effectue un audit des appareils externes et enregistre les informations dans le registre de Kaspersky Security Center. La liste des appareils externes est disponible lors de l'ajout d'appareils de confiance.

La tâche *Générateur de règles pour le Contrôle des appareils* ne collecte pas d'informations sur les imprimantes réseau et les réseaux Wi-Fi connectés aux appareils. Pour les appareils de ces types, vous devez créer les règles manuellement.

- Sur la base du rapport d'événements généré dans Kaspersky Security Center pour le module Contrôle des appareils, en mode **Informer**.

  Dans ce scénario, Kaspersky Embedded Systems Security ne bloque pas l'accès aux appareils. Lorsque le module Contrôle des appareils fonctionne en mode **Informer**, l'application autorise l'utilisation de tous les appareils et consigne les événements de connexion et de déconnexion des appareils externes.

  Comment activer Contrôle des appareils en mode Informer dans la Console d'administration de Kaspersky Security Center

  1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
  2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
  3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.
  4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.
  5. Cochez la case **Contrôle des appareils**.
  6. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez **Informer**.
  7. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

  Comment activer Contrôle des appareils en mode Informer dans Kaspersky Security Center Web Console

  1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
  2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

     La fenêtre des propriétés de la stratégie s'ouvre.
  3. Sélectionnez l'onglet **Paramètres de l'application**.
  4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

     La fenêtre **Contrôle des appareils** s'ouvre.
  5. Cochez la case **Activer le Contrôle des appareils**.
  6. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez **Informer**.
  7. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

  Comment activer Contrôle des appareils en mode Informer dans la Console de l'application

  1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur** → **Contrôle des appareils**.
  2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

     La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Cochez la case **Contrôle des appareils**.

4. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez **Informer**.

5. Enregistrez vos modifications.

Pendant l'exécution du module, tous les scénarios possibles pour les appareils protégés et les groupes d'appareils protégés doivent être exécutés. Ensuite, vous pouvez importer les informations du rapport d'événements de Kaspersky Security Center dans un fichier TXT et, après avoir examiné le rapport, ajouter des appareils de confiance.

Ce scénario est recommandé si le réseau de l'entreprise compte un grand nombre d'appareils protégés de types différents, chacun doté d'un ensemble différent d'appareils externes.

Ajout d'appareils de confiance

Les *Appareils de confiance* sont les appareils que les utilisateurs définis dans les paramètres de l'appareil de confiance peuvent accéder librement à tout moment.

Pour pouvoir utiliser les appareils de confiance, vous pouvez accorder l'accès à un utilisateur individuel, à un groupe d'utilisateurs ou à tous les utilisateurs de l'organisation.

Par exemple, si votre organisation n'autorise pas l'utilisation de disques amovibles, mais que les administrateurs utilisent de tels disques dans le cadre de leur travail, vous pouvez autoriser l'utilisation des disques amovibles uniquement pour le groupe d'administrateurs. Pour ce faire, ajoutez un disque amovible à la liste de confiance et configurez les privilèges d'accès des utilisateurs.

Il n'est pas recommandé d'ajouter plus de 1000 appareils de confiance, car cela peut entraîner une instabilité du système.

Comment ajouter un appareil de confiance dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.

4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.

5. Sous les **Paramètres de surveillance des appareils**, sélectionnez l'onglet **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.

6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'appareils de confiance pour tous les ordinateurs de l'organisation.

   Les listes des appareils de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les appareils de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultés. La modification ou la suppression d'appareils de confiance de la stratégie parent n'est pas possible.

7. Cliquez sur le bouton **Ajouter** et sélectionnez une méthode pour ajouter un appareil à la liste des appareils de confiance.

   - **Générer des règles en fonction des appareils connectés**.
   - **Générer des règles en fonction des données du système**.
   - **Générer des règles basées sur le registre de Kaspersky Security Center**.

   Si la liste des appareils est vide, vous devez réaliser un audit des appareils externes. Pour ce faire, exécutez la tâche *Générateur de règles pour le Contrôle des appareils*.

   > Kaspersky Embedded Systems Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.

8. Cliquez sur **Ajouter des règles pour les appareils sélectionnés**.
9. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment ajouter un appareil de confiance dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Contrôle de l'activité locale** → **Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.
5. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.
6. Cochez la case **Regrouper les valeurs après l'héritage** si vous souhaitez créer une liste commune d'appareils de confiance pour tous les ordinateurs de l'organisation.

   Les listes des appareils de confiance des stratégies parent et enfant sont fusionnées. Pour fusionner des listes, l'héritage des paramètres de la stratégie parent doit être activé. Les appareils de confiance de la stratégie parent apparaissent dans les stratégies enfant et peuvent uniquement être consultés. La modification ou la suppression d'appareils de confiance de la stratégie parent n'est pas possible.
7. Cliquez sur **À partir du registre KSC**.

   Si la liste des appareils est vide, vous devez réaliser un audit des appareils externes. Pour ce faire, exécutez la tâche *Générateur de règles pour le Contrôle des appareils*.

   > Kaspersky Embedded Systems Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.

8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas.

Comment ajouter un appareil de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.
2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.
3. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.
4. Cliquez sur le bouton **Ajouter** et sélectionnez une méthode pour ajouter un appareil à la liste des appareils de confiance.

   - **Générer des règles en fonction des appareils connectés**.
   - **Générer des règles en fonction des données du système**.
   - **Générer des règles basées sur le registre de Kaspersky Security Center**.

   Si la liste des appareils est vide, vous devez réaliser un audit des appareils externes. Pour ce faire, exécutez la tâche *Générateur de règles pour le Contrôle des appareils*.

   > Kaspersky Embedded Systems Security ne prend pas en charge l'ajout d'appareils du type **Disquettes** à la liste de confiance.
5. Cliquez sur **Ajouter des règles pour les appareils sélectionnés**.
6. Enregistrez vos modifications.

Exportation et importation de la liste des appareils de confiance

Pour distribuer la liste des appareils de confiance aux autres ordinateurs de votre organisation, vous pouvez utiliser la procédure d'exportation/importation. Vous pouvez exporter la liste des appareils de confiance dans un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'appareils du même type. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des appareils de confiance ou pour procéder à la migration de la liste vers un autre serveur.

> Kaspersky Embedded Systems Security permet d'importer la liste des appareils de confiance depuis Kaspersky Endpoint Security for Windows. Le format de fichier XML pour ces applications est le même.

Comment exporter et importer une liste d'appareils de confiance dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Contrôle de l'activité locale**.

4. Dans la section **Contrôle des appareils**, cliquez sur **Paramètres**.

5. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.

6. Pour exporter une liste d'appareils de confiance, procédez comme suit :

   a. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

   b. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

      1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

      2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

   c. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

      Kaspersky Embedded Systems Security exporte la liste des appareils de confiance dans le fichier XML.

7. Pour importer une liste d'appareils de confiance, procédez comme suit :

   a. Cliquez sur **Ajouter → Importer les règles à partir d'un fichier XML** sélectionnez le mode d'importation : ajouter ou remplacer.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des appareils de confiance.

      En mode Fusionner, l'application vérifie les listes d'appareils de confiance et supprime les entrées en double. En mode Ajouter, l'application ajoute des entrées à la liste des applications de confiance sans rechercher des doublons.

   b. Ouvrez le fichier.

      Kaspersky Embedded Systems Security importe les appareils de confiance selon le mode sélectionné.

8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment exporter et importer une liste d'appareils de confiance dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Contrôle de l'activité locale → Contrôle des appareils** et cliquez sur le bouton **Configurer**.

   La fenêtre **Contrôle des appareils** s'ouvre.

5. Dans le groupe **Paramètres du contrôle des appareils**, cliquez sur **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.

6. Pour exporter une liste d'appareils de confiance, procédez comme suit :

   a. Sélectionnez les appareils de confiance que vous souhaitez exporter.

   b. Cliquez sur le bouton **Exporter**, puis sélectionnez le mode d'exportation : exportez toute la liste des appareils de confiance, ou uniquement une sélection d'appareils de confiance.

   c. Enregistrez le fichier.

      Kaspersky Embedded Systems Security exporte la liste des adresses de ressources Internet dans un fichier XML.

7. Pour importer une liste d'appareils de confiance, procédez comme suit :

   a. Cliquez sur le bouton **Importer** et sélectionnez le mode d'importation : ajouter ou remplacer.

   b. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des ressources Internet.

   c. Ouvrez le fichier.

      Kaspersky Embedded Systems Security importe les appareils de confiance selon le mode sélectionné.

8. Enregistrez vos modifications. Pour appliquer la stratégie sur les ordinateurs, fermez les cadenas .

Comment exporter et importer une liste d'appareils de confiance dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Contrôle des appareils**.

2. Dans le panneau des résultats du nœud **Contrôle des appareils**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle des appareils** s'ouvre.

3. Sous les **Paramètres du Contrôle des appareils**, sélectionnez l'onglet **Appareils de confiance**.

   Cette action permet d'exporter une liste d'appareils de confiance.

4. Pour exporter une liste d'appareils de confiance, procédez comme suit :

   a. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

   b. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

      1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

      2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

   c. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

      Kaspersky Embedded Systems Security exporte la liste des appareils de confiance dans le fichier XML.

5. Pour importer une liste d'appareils de confiance, procédez comme suit :

   a. Cliquez sur **Ajouter → Importer les règles à partir d'un fichier XML** sélectionnez le mode d'importation : ajouter ou remplacer.

Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des ressources Internet.

En mode Fusionner, l'application vérifie les listes d'appareils de confiance et supprime les entrées en double. En mode Ajouter, l'application ajoute des entrées à la liste des applications de confiance sans rechercher des doublons.

b. Ouvrez le fichier.

Kaspersky Embedded Systems Security importe les appareils de confiance selon le mode sélectionné.

6. Enregistrez vos modifications.

Pare-feu

Le module Pare-feu peut fonctionner dans les modes suivants :

- **Observer l'état du pare-feu Windows**. Ce mode est destiné à assurer une transition en douceur entre la logique de la tâche Gestion du pare-feu dans la version 3.4 et les versions antérieures et le Pare-feu complet dans la version 4.0 et les versions antérieures de l'application. Lorsque vous mettez à jour la version 3.4 et toute version antérieure de l'application, les règles de la tâche Gestion du pare-feu intégrée au pare-feu Windows sont conservées. Cependant, le module Pare-feu n'interagit plus avec le pare-feu Windows, mais se contente de surveiller le filtrage du trafic par le pare-feu Windows et d'enregistrer les événements correspondants dans le journal des opérations du module. Vous pouvez ensuite créer des règles de pare-feu et/ou importer des règles de pare-feu Windows et faire passer le mode de fonctionnement du pare-feu à **Informer**.

- **Informer**. L'application contrôle uniquement le fonctionnement des règles du Pare-feu et enregistre les événements correspondants dans le journal des opérations du module. Le mode est conçu pour tester les règles de pare-feu. Vous pouvez évaluer leur applicabilité à l'aide du journal des opérations du pare-feu. Ensuite, si nécessaire, vous pouvez modifier les règles de pare-feu et faire passer le mode de fonctionnement du pare-feu à **Bloquer**.

- **Bloquer**. L'application filtre le trafic réseau conformément aux paramètres du module et enregistre les événements correspondants dans le journal des opérations du module.

À propos des règles du pare-feu

Si le mode **Bloquer** est sélectionné, le module Pare-feu filtre le trafic réseau à l'aide des règles de pare-feu.

Les règles de pare-feu pour les applications contrôlent les connexions réseau pour des applications spécifiées. Le critère de déclenchement de ces règles est le chemin d'accès à un fichier d'application exécutable.

Les règles de port du pare-feu contrôlent les connexions réseau pour les ports et protocoles (TCP/UDP) indiqués. Les critères de déclenchement de ces règles sont le type de protocole et le port ou la plage de ports.

Les règles pour les ports impliquent une plus grande zone d'action que les règles pour les applications. En autorisant les connexions sur la base de règles pour les ports, vous abaissez le niveau de sécurité de l'ordinateur protégé.

Configuration du pare-feu

Cette section fournit des instructions sur la configuration des paramètres généraux du module Pare-feu, ainsi que sur la création et la configuration des règles du Pare-feu.

Configuration des paramètres généraux du pare-feu

Configuration des paramètres généraux du module Pare-feu dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Paramètres** dans la sous-section **Pare-feu**.

   La fenêtre **Pare-feu** s'ouvre.
4. Sous l'onglet **Général**, dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Observer l'état du pare-feu Windows**. Ce mode est destiné à assurer une transition en douceur entre la logique de la tâche Gestion du pare-feu dans la version 3.4 et les versions antérieures et le Pare-feu complet dans la version 4.0 et les versions antérieures de l'application. Lorsque vous mettez à jour la version 3.4 et toute version antérieure de l'application, les règles de la tâche Gestion du pare-feu intégrée au pare-feu Windows sont conservées. Cependant, le module Pare-feu n'interagit plus avec le pare-feu Windows, mais se contente de surveiller le filtrage du trafic par le pare-feu Windows et d'enregistrer les événements correspondants dans le journal des opérations du module. Vous pouvez ensuite créer des règles de pare-feu et/ou importer des règles de pare-feu Windows et faire passer le mode de fonctionnement du pare-feu à **Informer**.
   - **Informer**. L'application contrôle uniquement le fonctionnement des règles du Pare-feu et enregistre les événements correspondants dans le journal des opérations du module. Le mode est conçu pour tester les règles de pare-feu. Vous pouvez évaluer leur applicabilité à l'aide du journal des opérations du pare-feu. Ensuite, si nécessaire, vous pouvez modifier les règles de pare-feu et faire passer le mode de fonctionnement du pare-feu à **Bloquer**.
   - **Bloquer**. L'application filtre le trafic réseau conformément aux paramètres du module et enregistre les événements correspondants dans le journal des opérations du module.
5. Dans le groupe **Connexions entrantes**, configurez les paramètres des connexions réseau entrantes :

   - La liste déroulante **Action à effectuer pour les connexions entrantes** permet d'indiquer l'action que l'application exécute pour toutes les connexions réseau entrantes, sauf indication contraire dans les règles du Pare-feu pour les connexions entrantes.
   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions entrantes.

     Les règles de pare-feu pour les connexions entrantes remplissent le rôle d'exclusions. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Bloquer** dans la liste déroulante **Action à effectuer pour les connexions entrantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

6. Dans le groupe **Connexions sortantes**, configurez les paramètres des connexions réseau sortantes :

   - La liste déroulante **Action à effectuer pour les connexions sortantes** permet d'indiquer l'action que l'application exécutera pour toutes les connexions réseau sortantes, sauf indication contraire dans les règles du Pare-feu pour les connexions sortantes.

   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions sortantes.

     Les règles de pare-feu pour les connexions sortantes remplissent le rôle d'exclusion. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Autoriser** dans la liste déroulante **Action à effectuer pour les connexions sortantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

7. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Configuration des paramètres généraux du module Pare-feu dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configurer** dans la sous-section **Pare-feu**.

   La fenêtre **Pare-feu** s'ouvre.

5. Réglez le commutateur à bascule sur **Pare-feu ACTIVÉ**.

6. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Observer l'état du pare-feu Windows**. Ce mode est destiné à assurer une transition en douceur entre la logique de la tâche Gestion du pare-feu dans la version 3.4 et les versions antérieures et le Pare-feu complet dans la version 4.0 et les versions antérieures de l'application. Lorsque vous mettez à jour la version 3.4 et toute version antérieure de l'application, les règles de la tâche Gestion du pare-feu intégrée au pare-feu Windows sont conservées. Cependant, le module Pare-feu n'interagit plus avec le pare-feu Windows, mais se contente de surveiller le filtrage du trafic par le pare-feu Windows et d'enregistrer les événements correspondants dans le journal des opérations du module. Vous pouvez ensuite créer des règles de pare-feu et/ou importer des règles de pare-feu Windows et faire passer le mode de fonctionnement du pare-feu à **Informer**.

   - **Informer**. L'application contrôle uniquement le fonctionnement des règles du Pare-feu et enregistre les événements correspondants dans le journal des opérations du module. Le mode est conçu pour tester les règles de pare-feu. Vous pouvez évaluer leur applicabilité à l'aide du journal des opérations du pare-feu. Ensuite, si nécessaire, vous pouvez modifier les règles de pare-feu et faire passer le mode de fonctionnement du pare-feu à **Bloquer**.

   - **Bloquer**. L'application filtre le trafic réseau conformément aux paramètres du module et enregistre les événements correspondants dans le journal des opérations du module.

7. Dans le groupe **Connexions entrantes**, configurez les paramètres des connexions réseau entrantes :

   - La liste déroulante **Action à effectuer pour les connexions entrantes** permet d'indiquer l'action que l'application exécute pour toutes les connexions réseau entrantes, sauf indication contraire dans les règles du Pare-feu pour les connexions entrantes.

   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions entrantes.

     Les règles de pare-feu pour les connexions entrantes remplissent le rôle d'exclusions. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Bloquer** dans la liste déroulante **Action à effectuer pour les connexions entrantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

8. Dans le groupe **Connexions sortantes**, configurez les paramètres des connexions réseau sortantes :

   - La liste déroulante **Action à effectuer pour les connexions sortantes** permet d'indiquer l'action que l'application exécutera pour toutes les connexions réseau sortantes, sauf indication contraire dans les règles du Pare-feu pour les connexions sortantes.

   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions sortantes.

     Les règles de pare-feu pour les connexions sortantes remplissent le rôle d'exclusion. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Autoriser** dans la liste déroulante **Action à effectuer pour les connexions sortantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

9. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Configuration des paramètres généraux du module Pare-feu dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur** → **Pare-feu**.

2. Dans le panneau des résultats du nœud **Pare-feu**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Pare-feu** s'ouvre.

3. Cochez la case **Pare-feu**.

4. Dans le groupe **Mode de fonctionnement des règles de blocage**, sélectionnez le mode de fonctionnement du module :

   - **Observer l'état du pare-feu Windows**. Ce mode est destiné à assurer une transition en douceur entre la logique de la tâche Gestion du pare-feu dans la version 3.4 et les versions antérieures et le Pare-feu complet dans la version 4.0 et les versions antérieures de l'application. Lorsque vous mettez à jour la version 3.4 et toute version antérieure de l'application, les règles de la tâche Gestion du pare-feu intégrée au pare-feu Windows sont conservées. Cependant, le module Pare-feu n'interagit plus avec le pare-feu Windows, mais se contente de surveiller le filtrage du trafic par le pare-feu Windows et d'enregistrer les événements correspondants dans le journal des opérations du module. Vous pouvez ensuite créer des règles de pare-feu et/ou importer des règles de pare-feu Windows et faire passer le mode de fonctionnement du pare-feu à **Informer**.

   - **Informer**. L'application contrôle uniquement le fonctionnement des règles du Pare-feu et enregistre les événements correspondants dans le journal des opérations du module. Le mode est conçu pour tester les règles de pare-feu. Vous pouvez évaluer leur applicabilité à l'aide du journal des opérations du pare-feu. Ensuite, si nécessaire, vous pouvez modifier les règles de pare-feu et faire passer le mode de fonctionnement du pare-feu à **Bloquer**.

   - **Bloquer**. L'application filtre le trafic réseau conformément aux paramètres du module et enregistre les événements correspondants dans le journal des opérations du module.

5. Dans le groupe **Connexions entrantes**, configurez les paramètres des connexions réseau entrantes :

   - La liste déroulante **Action à effectuer pour les connexions entrantes** permet d'indiquer l'action que l'application exécute pour toutes les connexions réseau entrantes, sauf indication contraire dans les règles du Pare-feu pour les connexions entrantes.

   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions entrantes.

     Les règles de pare-feu pour les connexions entrantes remplissent le rôle d'exclusions. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Bloquer** dans la liste déroulante **Action à effectuer pour les connexions entrantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

6. Dans le groupe **Connexions sortantes**, configurez les paramètres des connexions réseau sortantes :

   - La liste déroulante **Action à effectuer pour les connexions sortantes** permet d'indiquer l'action que l'application exécutera pour toutes les connexions réseau sortantes, sauf indication contraire dans les règles du Pare-feu pour les connexions sortantes.

   - Si nécessaire, ajoutez les Règles de pare-feu pour les connexions sortantes.

     Les règles de pare-feu pour les connexions sortantes remplissent le rôle d'exclusion. Par exemple, si vous configurez une règle d'autorisation pour les connexions réseau entrantes et que vous sélectionnez **Autoriser** dans la liste déroulante **Action à effectuer pour les connexions sortantes**, l'application autorise les connexions réseau entrantes qui correspondent aux critères de la règle.

7. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Création et configuration des règles du Pare-feu

Création et configuration des règles du pare-feu dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Paramètres** dans la sous-section **Pare-feu**.
   La fenêtre **Pare-feu** s'ouvre.
4. Cliquez sur le bouton **Liste des règles** dans le groupe **Connexions entrantes**.
   La fenêtre **Règles pour les connexions entrantes** s'ouvre.
5. **Créer et configurer des règles du Pare-feu pour les connexions entrantes**.
   1. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.
      La fenêtre **Règle pour une application** s'ouvre.
   2. Configurez les paramètres de la règle :
      a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      > Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau entrantes.

      b. Dans la liste **Action**, sélectionnez l'une des options suivantes :
      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour l'application.
      - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour l'application.

      c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.
      d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.
      e. Dans le champ **Chemin d'accès à l'application**, manuellement ou à l'aide du bouton **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.
      f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes à partir des adresses réseau indiquées, conformément aux paramètres de la règle.

> Seul le format IPv4 est pris en charge pour les adresses IP.

h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

i. Cliquez sur le bouton **OK** pour enregistrer la règle.

3. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règles pour les ports** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

   - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour les ports.
   - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour les ports.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

   e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes à partir des adresses réseau indiquées, conformément aux paramètres de la règle.

   > Seul le format IPv4 est pris en charge pour les adresses IP.

   f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   g. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions entrantes**.

6. Cliquez sur le bouton **Liste des règles** dans le groupe **Connexions sortantes**.

   La fenêtre **Règles pour les connexions sortantes** s'ouvre.

7. **Créer et configurer des règles du Pare-feu pour les connexions sortantes**.

   1. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Règle pour une application** s'ouvre.

2. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau sortantes.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau sortantes pour l'application.
      - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour l'application.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

   e. Dans le champ **Chemin d'accès à l'application**, manuellement ou à l'aide du bouton **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.

   f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

   g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

      Seul le format IPv4 est pris en charge pour les adresses IP.

   h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   i. Cliquez sur le bouton **OK** pour enregistrer la règle.

3. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règles pour les ports** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option a été sélectionnée, l'application autorise les connexions réseau sortantes pour les ports.
      - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour les ports.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

> Seul le format IPv4 est pris en charge pour les adresses IP.

f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

g. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions sortantes**.

8. Si vous souhaitez importer ou exporter des règles personnalisées à partir d'un fichier XML, utilisez les boutons **Importer** ou **Exporter** dans le groupe **Importation et exportation de règles**.

9. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Création et configuration des règles du pare-feu dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configurer** dans la sous-section **Pare-feu**.

   La fenêtre **Pare-feu** s'ouvre.

5. Réglez le commutateur à bascule sur **Pare-feu ACTIVÉ**.

6. Cliquez sur le bouton **Configurer** dans le groupe **Connexions entrantes**.

   La fenêtre **Règles pour les connexions entrantes** s'ouvre.

7. **Créer et configurer des règles du Pare-feu pour les connexions entrantes**.

   1. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Règle pour les ports** s'ouvre.

2. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour les ports.
      - **Refuser**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour les ports.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports locaux** et **Ports distants**, indiquez un port ou une plage de ports.

   e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes aux adresses réseau indiquées, conformément aux paramètres de la règle.

      Seul le format IPv4 est pris en charge pour les adresses IP.

   f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   g. Cliquez sur le bouton **OK** pour enregistrer la règle.

3. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle pour les applications** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau entrantes.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour l'application.
      - **Refuser**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour l'application.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports locaux** et **Ports distants**, indiquez un port ou une plage de ports.

   e. Dans le champ **Chemin d'accès à l'application**, indiquez manuellement le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.

f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes à partir des adresses réseau indiquées, conformément aux paramètres de la règle.

> Seul le format IPv4 est pris en charge pour les adresses IP.

h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

i. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions entrantes**.

8. Cliquez sur le bouton **Configurer** dans le groupe **Connexions sortantes**.

La fenêtre **Règles pour les connexions sortantes** s'ouvre.

9. **Créer et configurer des règles du Pare-feu pour les connexions sortantes**.

1. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

La fenêtre **Règle pour les ports** s'ouvre.

2. Configurez les paramètres de la règle :

a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

- **Autoriser**. Si cette option a été sélectionnée, l'application autorise les connexions réseau sortantes pour les ports.
- **Refuser**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour les ports.

c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

d. Dans les groupes **Ports locaux** et **Ports distants**, indiquez un port ou une plage de ports.

e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

> Seul le format IPv4 est pris en charge pour les adresses IP.

f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

g. Cliquez sur le bouton **OK** pour enregistrer la règle.

3. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.

La fenêtre **Règle pour les applications** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   > Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau sortantes.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

   - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau sortantes pour l'application.
   - **Refuser**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour l'application.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports locaux** et **Ports distants**, indiquez un port ou une plage de ports.

   e. Dans le champ **Chemin d'accès à l'application**, indiquez manuellement le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.

   f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

   g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

   > Seul le format IPv4 est pris en charge pour les adresses IP.

   h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   i. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions sortantes**.

10. Si vous souhaitez importer ou exporter des règles personnalisées à partir d'un fichier XML, utilisez les boutons **Importation de règles** ou **Exportation de règles** dans le groupe **Importation et exportation de règles**.

11. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Création et configuration de règles de pare-feu dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Pare-feu**.

2. Dans le panneau des résultats du nœud **Pare-feu**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Pare-feu** s'ouvre.

3. Cliquez sur le bouton **Liste des règles** dans le groupe **Connexions entrantes**.

   La fenêtre **Règles pour les connexions entrantes** s'ouvre.

4. **Créer et configurer des règles du Pare-feu pour les connexions entrantes**.

   1. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Règle pour une application** s'ouvre.

   2. Configurez les paramètres de la règle :

      a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      > Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau entrantes.

      b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour l'application.
      - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour l'application.

      c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

      d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

      e. Dans le champ **Chemin d'accès à l'application**, manuellement ou à l'aide du bouton **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.

      f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

      g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes à partir des adresses réseau indiquées, conformément aux paramètres de la règle.

      > Seul le format IPv4 est pris en charge pour les adresses IP.

      h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

      i. Cliquez sur le bouton **OK** pour enregistrer la règle.

   3. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Règles pour les ports** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

   - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau entrantes pour les ports.
   - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau entrantes pour les ports.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

   e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions entrantes à partir des adresses réseau indiquées, conformément aux paramètres de la règle.

   > Seul le format IPv4 est pris en charge pour les adresses IP.

   f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   g. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions entrantes**.

5. Cliquez sur le bouton **Liste des règles** dans le groupe **Connexions sortantes**.

   La fenêtre **Règles pour les connexions sortantes** s'ouvre.

6. **Créer et configurer des règles du Pare-feu pour les connexions sortantes**.

   1. Sous l'onglet **Applications**, cliquez sur le bouton **Ajouter**.

      La fenêtre **Règle pour une application** s'ouvre.

   2. Configurez les paramètres de la règle :

      a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

      > Le nom de la règle, quelle que soit la casse des caractères, ne doit pas correspondre aux noms réservés All, ICMPv4 et ICMPv6 ; il doit être unique dans la liste de toutes les règles pour les connexions réseau sortantes.

      b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

      - **Autoriser**. Si cette option est sélectionnée, l'application autorise les connexions réseau sortantes pour l'application.
      - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour l'application.

c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

e. Dans le champ **Chemin d'accès à l'application**, manuellement ou à l'aide du bouton **Parcourir**, indiquez le chemin d'accès au fichier exécutable de l'application pour laquelle vous configurez la règle.

f. Dans le champ **Nom du service**, indiquez si nécessaire le nom du service auquel la règle sera appliquée.

g. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

> Seul le format IPv4 est pris en charge pour les adresses IP.

h. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

i. Cliquez sur le bouton **OK** pour enregistrer la règle.

3. Sous l'onglet **Ports**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Règles pour les ports** s'ouvre.

4. Configurez les paramètres de la règle :

   a. Dans le champ **Nom de la règle**, saisissez le nom de la règle.

   b. Dans la liste **Action**, sélectionnez l'une des options suivantes :

   - **Autoriser**. Si cette option a été sélectionnée, l'application autorise les connexions réseau sortantes pour les ports.
   - **Bloquer**. Si cette option est sélectionnée, l'application bloque les connexions réseau sortantes pour les ports.

   c. Cochez la case **Protocole** pour sélectionner le type de protocole pour lequel l'application contrôle les connexions réseau entrantes.

   d. Dans les groupes **Ports** et **Ports**, indiquez un port ou une plage de ports.

   e. Dans le champ **Zone d'application de la règle**, indiquez les adresses réseau. L'application surveille les connexions sortantes vers les adresses réseau indiquées, conformément aux paramètres de la règle.

   > Seul le format IPv4 est pris en charge pour les adresses IP.

   f. Dans le groupe **Adaptateurs réseau**, spécifiez la liste des adaptateurs réseau.

   g. Cliquez sur le bouton **OK** pour enregistrer la règle.

5. Cliquez sur le bouton **OK** dans la fenêtre **Règles pour les connexions sortantes**.

7. Si vous souhaitez importer ou exporter des règles personnalisées à partir d'un fichier XML, utilisez les boutons **Importer** ou **Exporter** dans le groupe **Importation et exportation de règles**.

8. Pour importer les règles du Pare-feu Windows, cliquez sur **Importer les règles du pare-feu Windows**.

   Sur les ordinateurs Windows 11 24H2, l'application peut ignorer certaines règles du pare-feu Windows. En raison des particularités de cette version du système d'exploitation, Kaspersky Embedded Systems Security peut ne pas reconnaître les paramètres de certaines règles pour les paquets d'application.

9. Enregistrez vos modifications.

Kaspersky Embedded Systems Security applique les nouveaux paramètres. La date et l'heure de modification des paramètres sont enregistrées dans le journal d'audit système.

Activation et désactivation des règles du pare-feu

Activation et désactivation des règles du pare-feu dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Paramètres** dans la sous-section **Pare-feu**.

   La fenêtre **Pare-feu** s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Liste des règles** dans la section **Connexions entrantes** ou **Connexions sortantes**, en fonction du type de règle dont vous souhaitez modifier l'état.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications** ou **Ports**.

   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. Pour supprimer des règles de la liste, sélectionnez-les et cliquez sur **Supprimer**.
7. Enregistrez vos modifications.

Activation et désactivation des règles du pare-feu dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Dans la section **Contrôle de l'activité réseau**, cliquez sur le bouton **Configurer** dans la sous-section **Pare-feu**.

   La fenêtre **Pare-feu** s'ouvre.

5. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Configurer** dans la section **Connexions entrantes** ou **Connexions sortantes**, en fonction du type de règle dont vous souhaitez modifier l'état.

6. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Ports** ou **Applications**.

   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.

7. Pour supprimer des règles de la liste, sélectionnez-les et cliquez sur **Supprimer**.

8. Enregistrez vos modifications.

Activation et désactivation des règles du pare-feu dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Contrôle de l'ordinateur → Pare-feu**.

2. Dans le panneau des résultats du nœud **Pare-feu**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Pare-feu** s'ouvre.

3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Liste des règles** dans la section **Connexions entrantes** ou **Connexions sortantes**, en fonction du type de règle dont vous souhaitez modifier l'état.

4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Applications** ou **Ports**.

   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.

5. Pour supprimer des règles de la liste, sélectionnez-les et cliquez sur **Supprimer**.

6. Enregistrez vos modifications.

Protection BadUSB

Le module Protection BadUSB n'est pas installé par défaut. Vous pouvez ajouter un module pendant l'installation de l'application ou modifier l'ensemble des modules après l'installation de l'application.

Certains virus modifient l'application interne des appareils USB afin que le système d'exploitation considère l'appareil USB comme un clavier. Par conséquent, le virus peut exécuter des commandes sous votre compte d'utilisateur, par exemple, pour télécharger des logiciels malveillants.

Le module Protection BadUSB permet d'empêcher la connexion d'appareils USB infectés qui imitent un clavier.

Quand un appareil USB est connecté à l'ordinateur et que le système d'exploitation le reconnait comme étant un clavier, l'application génère un code numérique et invite l'utilisateur à le saisir à partir de ce clavier ou à l'aide d'un clavier numérique, si ce dernier est disponible. C'est ce qu'on appelle l'autorisation du clavier.

Si le code est correctement saisi, l'application enregistre les paramètres d'identification, à savoir le VID/PID du clavier et le numéro du port auquel il est connecté, dans la liste des claviers autorisés. Il ne sera pas nécessaire d'autoriser à nouveau le clavier lors de la prochaine connexion ou suite au redémarrage du système d'exploitation.

Par contre, si vous connectez un clavier autorisé à un autre port USB, l'application sollicitera à nouveau l'autorisation.

Si le code numérique n'est pas saisi correctement, l'application crée un autre code. Vous pouvez configurer le nombre de tentatives de saisie du code numérique. En cas de plusieurs saisies erronées du code numérique ou si la fenêtre d'autorisation de clavier est fermée, l'application bloque la saisie depuis ce clavier. Si la durée de blocage de l'appareil USB arrive à échéance ou si le système d'exploitation redémarre, l'application proposera à nouveau d'autoriser le clavier.

L'application autorise l'utilisation du clavier autorisé et bloque tout clavier qui n'a pas réussi l'autorisation.

Les appareils USB définis par le système d'exploitation comme des claviers et connectés à l'ordinateur avant l'installation du module Protection BadUSB sont considérés comme autorisés après son installation.

Comment activer et configurer le module Protection BadUSB dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Contrôle de l'activité locale**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Protection BadUSB**.
   La fenêtre **Protection BadUSB** s'ouvre.
5. Utilisez la case **Protection BadUSB** pour activer ou désactiver le module.

6. Configurez les paramètres suivants dans la section **Autorisation des appareils USB** :

   - **Nombre maximal de tentatives d'autorisation des appareils USB**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Embedded Systems Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez de cinq tentatives pour saisir le code d'autorisation.

   - **Délai d'attente lorsque le nombre maximal de tentatives est atteint (min.)**. Durée de blocage de l'appareil USB après le nombre défini de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).

7. Configurez les paramètres suivants dans la section **Autorisation de l'appareil USB lors de la connexion** :

   - **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB**. Si la case est cochée, l'application autorise l'utilisation d'un clavier virtuel pour autoriser les appareils USB à partir desquels la saisie du code d'autorisation est impossible (par exemple, les lecteurs de code-barres).

   - **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB**. Si la case est cochée, l'application n'affiche pas le code-barres dans la notification d'autorisation du lecteur de codes-barres.

8. Fermez les cadenas pour appliquer la stratégie aux ordinateurs.

9. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer et configurer le module Protection BadUSB dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Contrôle de l'activité locale**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Protection BadUSB**.

   La fenêtre **Protection BadUSB** s'ouvre.

6. Utilisez le commutateur **Protection BadUSB** pour activer ou désactiver le module.

7. Activez ou désactivez le commutateur **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB ACTIVÉ** pour autoriser ou bloquer l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB à partir desquels la saisie du code d'autorisation est impossible (par exemple, les lecteurs de code-barres).

8. Activez ou désactivez le commutateur **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB ACTIVÉ** pour autoriser ou bloquer l'affichage d'un code-barres dans la notification d'autorisation du lecteur de code-barres.

9. Configurez les paramètres suivants dans la section **Autorisation des appareils USB** :

    - **Nombre maximal de tentatives d'autorisation des appareils USB (1-10)**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Embedded Systems Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez de cinq tentatives pour saisir le code d'autorisation.

    - **Délai d'attente lorsque le nombre maximal de tentatives est atteint en minutes (1-180)**. Durée de blocage de l'appareil USB après le nombre défini de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).

10. Fermez les cadenas pour appliquer la stratégie aux ordinateurs.

11. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment activer et configurer le module Protection BadUSB dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Contrôle de l'ordinateur → Protection BadUSB**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

    La fenêtre **Protection BadUSB** s'ouvre.

3. Utilisez la case **Protection BadUSB** pour activer ou désactiver le module.

4. Configurez les paramètres suivants dans la section **Autorisation des appareils USB** :

    - **Nombre maximal de tentatives d'autorisation des appareils USB**. Blocage automatique de l'appareil USB si le code d'autorisation est saisi incorrectement le nombre de fois défini. Les valeurs valides sont de 1 à 10. Par exemple, si vous autorisez cinq tentatives de saisie du code d'autorisation, l'application bloque l'appareil USB après la cinquième tentative infructueuse. Kaspersky Embedded Systems Security affiche la durée de blocage de l'appareil USB. Une fois ce délai écoulé, vous disposez de cinq tentatives pour saisir le code d'autorisation.

    - **Délai d'attente lorsque le nombre maximal de tentatives est atteint (min.)**. Durée de blocage de l'appareil USB après le nombre défini de tentatives infructueuses de saisie du code d'autorisation. Les valeurs valides sont de 1 à 180 (minutes).

5. Configurez les paramètres suivants dans la section **Autorisation de l'appareil USB lors de la connexion** :

    - **Interdire l'utilisation d'un clavier virtuel pour l'autorisation des appareils USB**. Si la case est cochée, l'application autorise l'utilisation d'un clavier virtuel pour autoriser les appareils USB à partir desquels la saisie du code d'autorisation est impossible (par exemple, les lecteurs de code-barres).

    - **Interdire l'utilisation d'un code-barres pour l'autorisation des appareils USB**. Si la case est cochée, l'application n'affiche pas le code-barres dans la notification d'autorisation du lecteur de codes-barres.

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

Contrôle de l'intégrité du système

Kaspersky Embedded Systems Security 4.0 inclut désormais le module Contrôle de l'intégrité du système au lieu du module de Contrôle de l'intégrité des fichiers. Le Contrôle de l'intégrité du système inclut toutes les fonctionnalités du Contrôle de l'intégrité des fichiers et permet également de surveiller les modifications apportées au registre et la connexion d'appareils externes.

Le Contrôle de l'intégrité du système surveille les modifications du système d'exploitation qui peuvent être le signe d'une atteinte à la sécurité de l'ordinateur. En cas de détection de telles modifications, Kaspersky Embedded Systems Security génère les événements correspondants et en informe l'administrateur. Le Contrôle de l'intégrité du système peut fonctionner en mode temps réel et peut également effectuer des vérifications de l'intégrité du système sur demande.

Contrôle de l'intégrité du système en temps réel

En mode temps réel, le Contrôle de l'intégrité du système suit les modifications apportées aux objets que vous avez inclus dans le champ d'application du module (la zone de surveillance). Le Contrôle de l'intégrité du système permet également de bloquer en temps réel l'accès non autorisé à ces objets.

Vérification de l'intégrité du système sur demande

La Vérification de l'intégrité du système à la demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Pour exécuter la tâche **Contrôle de l'intégrité du système par rapport à une référence**, vous devez configurer la zone d'application du module (la zone de surveillance) et créer une référence. Une référence est un état enregistré des objets dans le système, que l'application utilise comme référence lors de la comparaison avec l'état actuel. Une référence est créée lors du premier lancement de la tâche.

Migration des paramètres du Contrôle de l'intégrité des fichiers

Lorsque vous mettez à jour Kaspersky Embedded Systems Security version 3.4 ou antérieure vers la version 4.1, les paramètres du Contrôle de l'intégrité des fichiers et de l'accès au registre sont migrés automatiquement. Dans le cadre de la migration, l'application déplace les règles de surveillance vers le Contrôle de l'intégrité du système.

À propos des règles du Contrôle de l'intégrité du système

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une *règle du Contrôle de l'intégrité du système* est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers ou au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers ou dans le registre à l'intérieur de la *zone de surveillance* spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système.

Contrôle de l'intégrité du système permet de surveiller les objets suivants :

- Fichiers
- Registre
- Appareils externes

Considérations particulières liées à la surveillance des fichiers

Le Contrôle de l'intégrité du système surveille les modifications dans les fichiers et les dossiers, ainsi que les fichiers ajoutés ou supprimés de la zone de surveillance. Ces changements peuvent indiquer une faille de sécurité informatique. Il est conseillé d'ajouter des objets rarement modifiés ou des objets auxquels seul l'administrateur a accès. Cette mesure permettra de réduire le nombre d'événements du Contrôle de l'intégrité du système.

Kaspersky Embedded Systems Security surveille les modifications des fichiers et des dossiers uniquement sur les disques connectés au moment où le Contrôle de l'intégrité du système en temps réel a commencé à fonctionner. Si un disque n'était pas connecté lorsque le Contrôle de l'intégrité du système en temps réel a commencé à fonctionner, l'application ne surveille pas les modifications des fichiers et des dossiers sur ce disque même si les fichiers et les dossiers sont ajoutés à la zone de surveillance.

L'application génère l'événement Création d'un objet lorsqu'une des actions suivantes est enregistrée : création d'un fichier, augmentation de la taille d'un fichier, réécriture des données d'un fichier ou troncature d'un fichier. En conséquence, si l'événement Création d'un objet est généré pour un fichier lors de l'application des règles de blocage du Contrôle du lancement des applications, cela peut résulter soit d'une création de fichier interdite, soit d'une modification de fichier interdite, y compris des opérations comme l'augmentation de la taille du fichier, la réécriture des données et la troncature.

Considérations particulières liées à la surveillance du registre

Contrôle de l'intégrité du système surveille le registre. Ces changements peuvent indiquer une faille de sécurité informatique.

Le Contrôle de l'intégrité du système surveille les clés racine suivantes du registre :

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`

- HKEY_USERS
- HKEY_CURRENT_CONFIG

Le Contrôle de l'intégrité du système ne prend pas en charge la clé HKEY_CURRENT_USER. Vous pouvez spécifier une clé sous HKEY_USERS en tant que HKEY_USERS\<user profile ID>\<key>.

Considérations particulières liées à la surveillance des appareils externes

Le Contrôle de l'intégrité du système surveille la connexion et la déconnexion des appareils externes. Ceci est nécessaire afin de protéger l'ordinateur contre les menaces de sécurité pouvant résulter de l'échange de fichiers avec de tels appareils. Le Contrôle de l'intégrité du système ne surveille pas l'accès aux appareils externes et ne bloque pas l'échange de fichiers. Vous pouvez configurer l'accès aux appareils à l'aide d'un autre module d'application, à savoir le Contrôle des appareils.

Lors de l'exécution de la tâche *Contrôle de l'intégrité du système par rapport à une référence*, l'application ignore la reconnexion des appareils externes si ceux-ci présentent la même lettre de lecteur dans le système d'exploitation. Pour être journalisés, les appareils reconnectés doivent avoir des lettres de lecteur différentes.

Le Contrôle de l'intégrité du système surveille la connexion des types d'appareils externes suivants :

- Disque amovible (y compris les clés USB)
- Disque dur
- Adaptateur réseau externe
- Disque CD/DVD/Blu-ray
- Scanner/caméra

Contrôle de l'intégrité du système en temps réel

Le Contrôle de l'intégrité du système permet de suivre en temps réel les modifications du système d'exploitation. Vous pouvez suivre les modifications susceptibles d'indiquer des atteintes à la sécurité sur l'ordinateur. Le module permet de bloquer ces modifications ou de consigner simplement les événements liés aux modifications.

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une règle du Contrôle de l'intégrité du système est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers et au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers et dans le registre à l'intérieur de la zone de surveillance spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système.

Comment activer et configurer le Contrôle de l'intégrité du système en temps réel dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Diagnostic du système**.
4. Dans la section **Contrôle de l'intégrité du système**, cliquez sur **Paramètres**.
5. Cochez la case **Contrôle de l'intégrité du système**.
6. Configurez le Contrôle de l'intégrité des fichiers :
   a. Cochez la case **Surveiller les fichiers** sous l'onglet **Fichiers**.
   b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour le Contrôle de l'intégrité des fichiers :
      - **Bloquer**. Dans ce mode, l'application exécute des actions sur les fichiers conformément aux règles du Contrôle de l'intégrité des fichiers et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.
      - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles du Contrôle de l'intégrité des fichiers uniquement dans le journal du Contrôle de l'intégrité du système.
   c. Ajoutez manuellement les règles du Contrôle de l'intégrité des fichiers à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Contrôle de l'intégrité des fichiers sont décrits dans le tableau suivant.
   d. Dans la liste des règles du Contrôle de l'intégrité des fichiers, cochez les cases pour conserver les règles nécessaires activées.
7. Configurez la Surveillance d'accès au registre :
   a. Cochez la case **Surveiller le registre** sous l'onglet **Registre**.
   b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour la Surveillance d'accès au registre :
      - **Bloquer**. Dans ce mode, l'application bloque les actions avec le registre conformément aux règles de la Surveillance d'accès au registre et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.
      - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles de la Surveillance d'accès au registre uniquement dans le journal du Contrôle de l'intégrité du système.
   c. Ajoutez manuellement les règles de la Surveillance d'accès au registre à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Moniteur d'accès au registre sont décrits dans le tableau suivant.
   d. Dans la liste des règles de la Surveillance d'accès au registre, cochez les cases pour conserver les règles nécessaires activées.

8. Configurez la surveillance des appareils externes :

    a. Cochez la case **Surveiller les appareils** sous l'onglet **Appareils**.

    b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif*, *Avertissement*, *Critique*.

    Après l'application des paramètres de surveillance des appareils externes, l'application garde en mémoire les connexions actuelles des appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant dans le journal du Contrôle de l'intégrité du système.

9. Enregistrez vos modifications.

Comment activer et configurer le Contrôle de l'intégrité du système en temps réel dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

    La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Diagnostic du système → Contrôle de l'intégrité du système** et cliquez sur le bouton **Configurer**.

5. Cochez la case **Contrôle de l'intégrité du système**.

6. Configurez le Contrôle de l'intégrité des fichiers :

    a. Cochez la case **Surveiller les fichiers** sous l'onglet **Fichiers**.

    b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour le Contrôle de l'intégrité des fichiers :

    - **Bloquer**. Dans ce mode, l'application exécute des actions sur les fichiers conformément aux règles du Contrôle de l'intégrité des fichiers et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.

    - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles du Contrôle de l'intégrité des fichiers uniquement dans le journal du Contrôle de l'intégrité du système.

    c. Ajoutez manuellement les règles du Contrôle de l'intégrité des fichiers à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Contrôle de l'intégrité des fichiers sont décrits dans le tableau suivant.

    d. Dans la liste des règles du Contrôle de l'intégrité des fichiers, cochez les cases dans la colonne **État** pour laisser activées les règles dont vous avez besoin.

7. Configurez la Surveillance d'accès au registre :

    a. Cochez la case **Surveiller le registre** sous l'onglet **Registre**.

    b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour la Surveillance d'accès au registre :

    - **Bloquer**. Dans ce mode, l'application bloque les actions avec le registre conformément aux règles de la Surveillance d'accès au registre et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.

    - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles de la Surveillance d'accès au registre uniquement dans le journal du Contrôle de l'intégrité du système.

    c. Ajoutez manuellement les règles de la Surveillance d'accès au registre à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Moniteur d'accès au registre sont décrits dans le tableau suivant.

    d. Dans la liste des règles de la Surveillance d'accès au registre, cochez les cases dans la colonne **État** pour laisser activées les règles dont vous avez besoin.

8. Configurez la surveillance des appareils externes :

    a. Cochez la case **Surveiller les appareils** sous l'onglet **Appareils**.

    b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif*, *Avertissement*, *Critique*.

    Le Contrôle de l'intégrité du système enregistre la connexion actuelle d'appareils externes. Après l'activation du module dans les paramètres de l'application, l'application commence à surveiller les connexions et les déconnexions d'appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant.

9. Enregistrez vos modifications.

Comment activer et configurer le Contrôle de l'intégrité du système en temps réel dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Diagnostic du système → Contrôle de l'intégrité du système**.

2. Dans le panneau des résultats du nœud **Contrôle de l'intégrité du système**, cliquez sur **Propriétés**.

    La fenêtre **Propriétés : Contrôle de l'intégrité du système** s'ouvre.

3. Cochez la case **Contrôle de l'intégrité du système**.

4. Configurez le Contrôle de l'intégrité des fichiers :

   a. Cochez la case **Surveiller les fichiers** sous l'onglet **Fichiers**.

   b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour le Contrôle de l'intégrité des fichiers :

      - **Bloquer**. Dans ce mode, l'application exécute des actions sur les fichiers conformément aux règles du Contrôle de l'intégrité des fichiers et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.

      - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles du Contrôle de l'intégrité des fichiers uniquement dans le journal du Contrôle de l'intégrité du système.

   c. Ajoutez manuellement les règles du Contrôle de l'intégrité des fichiers à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Contrôle de l'intégrité des fichiers sont décrits dans le tableau suivant.

   d. Dans la liste des règles du Contrôle de l'intégrité des fichiers, cochez les cases pour conserver les règles nécessaires activées.

5. Configurez la Surveillance d'accès au registre :

   a. Cochez la case **Surveiller le registre** sous l'onglet **Registre**.

   b. Sous **Mode de fonctionnement des règles de blocage**, sélectionnez un mode pour la Surveillance d'accès au registre :

      - **Bloquer**. Dans ce mode, l'application bloque les actions avec le registre conformément aux règles de la Surveillance d'accès au registre et génère les événements correspondants dans le journal du Contrôle de l'intégrité du système.

      - **Informer**. Dans ce mode, l'application génère des événements sur le déclenchement des règles de la Surveillance d'accès au registre uniquement dans le journal du Contrôle de l'intégrité du système.

   c. Ajoutez manuellement les règles de la Surveillance d'accès au registre à l'aide du bouton **Ajouter** ou en les important à partir d'un fichier XML. Les paramètres de la règle du Moniteur d'accès au registre sont décrits dans le tableau suivant.

   d. Dans la liste des règles de la Surveillance d'accès au registre, cochez les cases pour conserver les règles nécessaires activées.

6. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils** sous l'onglet **Appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informations*, *Avertissement*, *Critique*.

      Après l'application des paramètres de surveillance des appareils externes, l'application garde en mémoire les connexions actuelles des appareils externes. Par la suite, lors de la connexion ou de la déconnexion d'un appareil externe, l'application génère un événement correspondant dans le journal du Contrôle de l'intégrité du système.

7. Enregistrez vos modifications.

Paramètres des règles du Contrôle de l'intégrité du système

Paramètre	Description
Contrôler les opérations sur les fichiers dans la zone	La zone d'action que vous souhaitez pour le Contrôle de l'intégrité des fichiers. Ce champ est obligatoire. Utilisez des masques : Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque : Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers. Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide. Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
Objets surveillés	Vous pouvez spécifier ici le nom ou la valeur d'une clé de registre. Utilisez des masques : Kaspersky Embedded Systems Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque :
Opérations sur les fichiers	• **Détecter**. L'application autorise les actions sur les fichiers dans la zone de surveillance. • **Détecter et bloquer**. Les actions de l'application dépendent du mode sélectionné du Contrôle de l'intégrité des fichiers. Si vous avez sélectionné le mode *Bloquer*, le Contrôle de l'intégrité du système bloque les actions avec les fichiers provenant de la zone de surveillance. Si vous avez sélectionné le mode *Informer*, le Contrôle de l'intégrité du système autorise les actions avec les fichiers provenant de la zone de surveillance.
Utilisateurs et/ou groupes d'utilisateurs de confiance	Un utilisateur de confiance est un utilisateur qui est autorisé à exécuter des actions avec les fichiers et les clés de registre dans la zone de surveillance. Si Kaspersky Embedded Systems Security détecte une action effectuée par un utilisateur de confiance, le Contrôle de l'intégrité du système génère un événement Informatif. Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement.
Marqueurs d'opérations sur les fichiers/Actions	Marqueurs caractérisant l'action avec les fichiers ou les clés de registre que l'application va surveiller.
Détecter les opérations sur les fichiers en fonction de tous les marqueurs reconnus/Détecter les opérations sur le registre en fonction de tous les marqueurs reconnus	Par défaut, Kaspersky Embedded Systems Security détecte tous les marqueurs d'opération de fichier / registre.
Détecter les opérations sur les fichiers en fonction des marqueurs suivants/Détecter les opérations sur le registre en fonction des marqueurs suivants	Dans la liste des opérations disponibles sur les fichiers / registre, cochez les cases en regard des opérations que vous souhaitez surveiller.
Si possible, calculer une somme de contrôle après une opération sur un fichier. La somme de contrôle sera indiquée dans le journal des tâches	Si la case est cochée, Kaspersky Embedded Systems Security calcule la somme de contrôle du fichier modifié si une opération avec au moins un marqueur sélectionné a été détectée. Si l'opération sur le fichier est détectée par plusieurs marqueurs, seule la somme de contrôle du fichier final après toutes les modifications est calculée. Si la case est décochée, Kaspersky Embedded Systems Security ne calcule pas la somme de contrôle pour les fichiers modifiés. Aucune somme de contrôle n'est calculée dans les cas suivants : • si le fichier est devenu inaccessible (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. Par défaut, la case est décochée.
Algorithme de calcul de la somme de contrôle	Choisissez l'un des algorithmes de calcul de la somme de contrôle dans la liste déroulante : • Hash MD5 • Hash SHA256

Paramètre	Description
Exclusions	Sous l'onglet **Exclusions**, vous pouvez ajouter des objets que vous souhaitez exclure de la zone de surveillance : • Pour une règle du Contrôle de l'intégrité des fichiers, vous pouvez spécifier une liste de dossiers. • Pour une règle de la Surveillance de l'accès au registre, vous pouvez spécifier des clés ou des valeurs de registre. Utilisez des masques : **Fichiers** Liste des fichiers et des dossiers surveillés par le module. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque : Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers. Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide. Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères. **Registre** Kaspersky Embedded Systems Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque : les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.
Niveau de gravité de l'événement	Kaspersky Embedded Systems Security enregistre les événements de modification de fichier chaque fois qu'un fichier ou une clé de registre de la zone de surveillance est modifié. Les niveaux de gravité d'événement suivants sont disponibles : **Informatif**, **Avertissement**, **Critique**.

Vérification de l'intégrité du système sur demande

La Vérification de l'intégrité du système sur demande est une tâche que vous pouvez exécuter manuellement ou de manière planifiée. Lors de l'exécution de la tâche *Contrôle de l'intégrité du système par rapport à une référence*, l'application compare l'état actuel des objets inclus dans la zone de surveillance avec leur état *de référence*. Une référence est créée lors du premier lancement de la tâche.

Pour que le Contrôle de l'intégrité du système fonctionne, vous devez ajouter au moins une règle. Une règle du Contrôle de l'intégrité du système est un ensemble de critères qui définissent les conditions d'accès des utilisateurs aux fichiers et au registre. Le Contrôle de l'intégrité du système détecte les modifications dans les fichiers et dans le registre à l'intérieur de la zone de surveillance spécifiée. La zone de surveillance est l'un des critères d'une règle du Contrôle de l'intégrité du système.

Configuration de la zone de surveillance pour la tâche Contrôle de l'intégrité du système par rapport à une référence

Par défaut, la zone de surveillance de la tâche *Contrôle de l'intégrité du système par rapport à une référence* est identique à la zone de surveillance du Contrôle de l'intégrité du système. Vous pouvez configurer une autre zone de surveillance pour la tâche.

Le Contrôle de l'intégrité du système ne prend pas en charge l'importation des clés `HKEY_CURRENT_USER` et `HKEY_CURRENT_CONFIG` pour la tâche *Vérification de l'intégrité du système*. Si la zone de surveillance de la tâche contient ces clés, l'application génère l'événement *La zone de surveillance inclut des objets incorrects*.

Comment configurer une autre zone de surveillance pour la tâche Contrôle de l'intégrité du système par rapport à une référence dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.
2. Sélectionnez la tâche nécessaire *Contrôle de l'intégrité du système par rapport à une référence* et ouvrez les propriétés de la tâche d'un double-clic.
3. Dans la fenêtre qui s'ouvre, sélectionnez **Paramètres**.
4. Configurez la surveillance des fichiers :
    a. Cochez la case **Surveiller les fichiers** sous l'onglet **Fichiers**.
    b. Sélectionnez des règles dans la liste en cochant les cases.
    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.
    d. Vous pouvez également importer des règles depuis une autre source.
5. Configurez la surveillance des registres :
    a. Cochez la case **Surveiller le registre** sous l'onglet **Registre**.
    b. Sélectionnez des règles dans la liste en cochant les cases.
    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.
    d. Vous pouvez également importer des règles depuis une autre source.

6. Configurez la surveillance des appareils externes :

    a. Cochez la case **Surveiller les appareils** sous l'onglet **Appareils**.

    b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif*, *Avertissement*, *Critique*.

    La tâche Contrôle de l'intégrité du système par rapport à une référence enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche, l'application ne surveille pas la déconnexion des appareils externes.

7. Enregistrez vos modifications.

Comment configurer une autre zone de surveillance pour la tâche Contrôle de l'intégrité du système par rapport à une référence dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

2. Sélectionnez la tâche nécessaire *Contrôle de l'intégrité du système par rapport à une référence* et ouvrez les propriétés de la tâche d'un double-clic.

3. Dans la fenêtre qui s'ouvre, sélectionnez **Paramètres de l'application**.

4. Configurez la surveillance des fichiers :

    a. Cochez la case **Surveiller les fichiers**.

    b. Sélectionnez des règles dans la liste en cochant les cases.

    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.

    d. Vous pouvez également importer des règles depuis une autre source.

5. Configurez la surveillance des registres :

    a. Cochez la case **Surveiller le registre**.

    b. Sélectionnez des règles dans la liste en cochant les cases.

    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.

    d. Vous pouvez également importer des règles depuis une autre source.

6. Configurez la surveillance des appareils externes :

    a. Cochez la case **Surveiller les appareils**.

    b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informatif*, *Avertissement*, *Critique*.

    La tâche *Contrôle de l'intégrité du système par rapport à une référence* enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche, l'application ne surveille pas la déconnexion des appareils externes.

7. Enregistrez vos modifications.

Comment configurer une autre zone de surveillance pour la tâche Contrôle de l'intégrité du système par rapport à une référence dans la Console de l'application

Les propriétés de la tâche **Contrôle de l'intégrité du système par rapport à une référence** sont modifiables dans la Console de Kaspersky Embedded Systems Security si la tâche a été créée localement ou si la case **Autoriser l'utilisation des tâches locales** est cochée dans la section des propriétés de la stratégie **Paramètres de l'application → Exécuter les tâches du système local**.

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Diagnostic du système → Contrôle de l'intégrité du système par rapport à une référence**.

2. Dans le panneau des résultats du nœud **Contrôle de l'intégrité du système par rapport à une référence**, cliquez sur **Propriétés**.

    La fenêtre **Propriétés : Contrôle de l'intégrité du système par rapport à une référence** s'ouvre.

3. Configurez la surveillance des fichiers :

    a. Cochez la case **Surveiller les fichiers** sous l'onglet **Fichiers**.

    b. Sélectionnez des règles dans la liste en cochant les cases.

    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.

    d. Vous pouvez également importer des règles depuis une autre source.

4. Configurez la surveillance des registres :

    a. Cochez la case **Surveiller le registre** sous l'onglet **Registre**.

    b. Sélectionnez des règles dans la liste en cochant les cases.

    c. Si nécessaire, ajoutez une nouvelle règle en cliquant sur le bouton **Ajouter**. Les paramètres des règles du Contrôle de l'intégrité du système par rapport à une référence sont décrits dans le tableau suivant.

    d. Vous pouvez également importer des règles depuis une autre source.

5. Configurez la surveillance des appareils externes :

   a. Cochez la case **Surveiller les appareils** sous l'onglet **Appareils**.

   b. Dans la liste déroulante **Niveau de gravité de l'événement**, sélectionnez le niveau d'importance des événements de surveillance des appareils externes : *Informations*, *Avertissement*, *Critique*.

      La tâche Contrôle de l'intégrité du système par rapport à une référence enregistre les informations relatives aux appareils externes connectés au moment de la création de la référence. Par la suite, lors de la connexion d'un appareil externe, l'application génère un événement correspondant. Lors de l'exécution de la tâche, l'application ne surveille pas la déconnexion des appareils externes.

6. Enregistrez vos modifications.

Paramètres d'une règle de la tâche Contrôle de l'intégrité du système par rapport à une référence

Paramètre	Description
Contrôler les opérations sur les fichiers dans la zone	La zone d'action que vous souhaitez pour le Contrôle de l'intégrité des fichiers. Ce champ est obligatoire. Utilisez des masques : Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque : Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers. Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide. Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères \ et / (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères.
Objets surveillés	Vous pouvez spécifier ici le nom ou la valeur d'une clé de registre. Utilisez des masques : Kaspersky Embedded Systems Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque :
Exclusions	Sous l'onglet **Exclusions**, vous pouvez ajouter des objets que vous souhaitez exclure de la zone de surveillance : • Pour une règle du Contrôle de l'intégrité des fichiers, vous pouvez spécifier une liste de dossiers. • Pour une règle de la Surveillance de l'accès au registre, vous pouvez spécifier des clés ou des valeurs de registre. Utilisez des masques : **Fichiers** Liste des fichiers et des dossiers surveillés par le module. Kaspersky Embedded Systems Security prend en charge les variables d'environnement ainsi que les caractères `*` et `?` lors de la saisie d'un masque : Le caractère `*` remplace n'importe quelle combinaison de caractères, y compris l'absence de caractères, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\*\*.txt` inclura tous les chemins vers les fichiers avec l'extension TXT situés dans des dossiers sur le lecteur C:, mais pas dans des sous-dossiers. Deux caractères `*` qui se suivent remplacent n'importe quelle combinaison de caractères, y compris des espaces, dans le nom du fichier ou de dossier, y compris les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\**\*.txt` inclura tous les chemins d'accès aux fichiers avec l'extension TXT situés dans le dossier joint nommé `Folder`, sauf pour le `Folder` lui-même. Le masque doit comprendre au moins un niveau d'imbrication. Le masque `C:\**\*.txt` n'est pas un masque valide. Le caractère `?` remplace n'importe quel caractère unique, sauf les caractères `\` et `/` (séparateurs des noms de fichier et de dossier dans les chemins d'accès aux fichiers et aux dossiers). Par exemple, le masque `C:\Folder\???.txt` inclura les chemins d'accès à tous les fichiers résidant dans le dossier nommé `Folder` qui ont l'extension TXT et un nom composé de trois caractères. **Registre** Kaspersky Embedded Systems Security prend en charge les caractères `*` et `?` lors de la saisie d'un masque : les entrées d'exclusion ont une priorité plus élevée que les entrées de la zone de surveillance.
Niveau de gravité de l'événement	Kaspersky Embedded Systems Security enregistre les événements de modification de fichier chaque fois qu'un fichier ou une clé de registre de la zone de surveillance est modifié. Les niveaux de gravité d'événement suivants sont disponibles : **Informatif**, **Avertissement**, **Critique**.

Lancement de la tâche Contrôle de l'intégrité du système par rapport à une référence

La tâche **Contrôle de l'intégrité du système par rapport à une référence** permet de vérifier si des fichiers ou des clés de registre ont été modifiés et de contrôler la connexion d'appareils externes. Pour vérifier si des fichiers ont été modifiés, vous pouvez exécuter la tâche **Contrôle de l'intégrité du système par rapport à une référence** dans les modes suivants :

- **Analyse complète**. Dans ce mode, l'application vérifie tous les attributs et tous les hachages des fichiers.
- **Analyse rapide**. Dans ce mode, l'application vérifie uniquement les attributs des fichiers.

Le mode d'exécution de la tâche n'influence pas la vérification du registre ou des appareils externes.

Comment exécuter une tâche Contrôle de l'intégrité du système par rapport à une référence dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Nouvelle tâche**.

   L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

3. Sélectionnez **Kaspersky Embedded Systems Security → Contrôle de l'intégrité du système par rapport à une référence**. Sélectionnez un mode de Contrôle de l'intégrité du système :

   - **Analyse complète**. Dans ce mode, l'application vérifie tous les attributs et tous les hachages des fichiers.
   - **Analyse rapide**. Dans ce mode, l'application vérifie uniquement les attributs des fichiers.

4. Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

   - Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – les appareils non distribués. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
   - Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.
   - Indiquez la sélection d'appareils pour lesquels vous souhaitez exécuter la tâche.
   - Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.

5. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Embedded Systems Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

6. Configurer une planification pour la tâche, par exemple, manuellement ou un certain jour de la semaine.

7. Saisissez un nom pour la tâche.

8. Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Comment lancer une tâche Contrôle de l'intégrité du système par rapport à une référence dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

   L'Assistant de création de tâche démarre.

3. Configurez les paramètres de la tâche :

   a. Dans la liste déroulante **Application**, sélectionnez Kaspersky Embedded Systems Security.

   b. Dans la liste déroulante **Type de tâche**, choisissez **Contrôle de l'intégrité du système par rapport à une référence**.

   c. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Contrôle hebdomadaire de l'intégrité du système*.

4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

5. Sélectionnez les appareils conformément à l'option choisie de la zone d'action de la tâche. Passez à l'étape suivante.

6. Sélectionnez l'algorithme de calcul de la somme de contrôle.

7. Sélectionnez un compte pour exécuter la tâche. Par défaut, Kaspersky Embedded Systems Security lance la tâche sous les privilèges d'un compte d'utilisateur local.

8. Quittez l'Assistant.

   La nouvelle tâche apparaît dans la liste des tâches.

9. Cliquez sur la nouvelle tâche.

   La fenêtre des propriétés de la tâche s'ouvre.

10. Sélectionnez l'onglet **Paramètres de l'application**.

11. Sélectionnez un mode de Vérification de l'intégrité du système :

    - **Analyse complète**. Dans ce mode, l'application vérifie tous les attributs et tous les hachages des fichiers.
    - **Analyse rapide**. Dans ce mode, l'application vérifie uniquement les attributs des fichiers.

12. Enregistrez vos modifications.

13. Cochez la case en regard de la tâche.

14. Cliquez sur **Démarrer**.

Exportation et importation des règles du Contrôle de l'intégrité du système

Vous pouvez exporter la liste des règles du Contrôle de l'intégrité du système vers un fichier XML. Vous pouvez ensuite modifier le fichier pour, par exemple, ajouter un grand nombre d'enregistrements du même type. Vous pouvez utiliser la fonction d'exportation/importation pour sauvegarder la liste des règles du Contrôle de l'intégrité du système ou pour procéder à la migration de la liste vers un autre serveur.

Le Contrôle de l'intégrité du système ne prend pas en charge l'importation des clés `HKEY_CURRENT_USER` et `HKEY_CURRENT_CONFIG` pour la tâche *Vérification de l'intégrité du système*. Si la zone de surveillance de la tâche contient ces clés, l'application génère l'événement *La zone de surveillance inclut des objets incorrects*.

Comment exporter et importer une liste de règles du Contrôle de l'intégrité du système dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Diagnostic du système**.
4. Dans la section **Contrôle de l'intégrité du système**, cliquez sur **Paramètres**.
5. Selon les règles que vous souhaitez exporter ou importer, accédez à l'onglet **Fichiers** ou à l'onglet **Registre**.
6. Pour exporter une liste de règles de fichiers et de règles de Registre :
   a. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.
   b. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :
      1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.
      2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.
   c. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

      Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.
7. Pour importer un fichier/les règles du registre, procédez comme suit :
   a. Cliquez sur **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.

b. Ouvrez le fichier.

Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

8. Enregistrez vos modifications.

Comment exporter et importer une liste du Contrôle de l'intégrité du système dans Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Diagnostic du système → Contrôle de l'intégrité du système** et cliquez sur le bouton **Configurer**.

   La fenêtre **Paramètres du contrôle de l'intégrité du système** s'ouvre.
5. Pour exporter un fichier/les règles du registre, procédez comme suit :

   a. Sous l'onglet **Fichier** ou **Registre**, sélectionnez les règles que vous souhaitez exporter.

   b. Cliquez sur le bouton **Exporter**. Une fenêtre s'ouvre ; dans cette fenêtre, indiquez si vous souhaitez exporter les règles sélectionnées ou toutes les règles, puis cliquez sur **Exporter**.

   Si vous n'avez sélectionné aucune règle, Kaspersky Embedded Systems Security exportera toutes les règles.
6. Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.
7. Pour importer un fichier/les règles du registre, procédez comme suit :

   a. Sous l'onglet **Fichier** ou **Registre**, cliquez sur le bouton **Importer depuis la version antérieure** si vous souhaitez importer les règles depuis un fichier XML créé dans la version 3.4 ou dans une version antérieure de l'application.

   Si vous importez des règles depuis un fichier XML créé dans la version 4.0 ou une version ultérieure, cliquez sur **Importer**.

   b. Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

   c. Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.

   d. Cliquez sur **Importer**.
8. Enregistrez vos modifications.

Comment exporter et importer une liste du Contrôle de l'intégrité du système dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Diagnostic du système → Contrôle de l'intégrité du système**.
2. Dans le panneau des résultats du nœud **Contrôle de l'intégrité du système**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Contrôle de l'intégrité du système** s'ouvre.

3. Selon les règles que vous souhaitez exporter ou importer, accédez à l'onglet **Fichiers** ou à l'onglet **Registre**.

4. Pour exporter une liste de règles de fichiers et de règles de Registre :

   a. Si vous souhaitez exporter la liste entière, cliquez sur le bouton et sélectionnez **Exporter**.

   b. Si vous souhaitez exporter uniquement une partie de la liste, procédez comme suit :

      1. Sélectionnez les éléments de la liste à exporter à l'aide des touches **CTRL** ou **MAJ**. Pour sélectionner tous les éléments, appuyez sur **CTRL+A**.

      2. Cliquez sur le bouton et sélectionnez **Exporter la sélection**.

   c. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier XML vers lequel vous souhaitez effectuer l'exportation, puis sélectionnez le dossier dans lequel enregistrer le fichier. Cliquez sur le bouton **Enregistrer**.

      Kaspersky Embedded Systems Security exporte la liste des règles dans un fichier XML.

5. Pour importer un fichier/les règles du registre, procédez comme suit :

   a. Cliquez sur **Importer**.

      Dans la fenêtre qui s'ouvre, sélectionnez le fichier XML à partir duquel vous souhaitez importer la liste des règles.

   b. Ouvrez le fichier.

      Si l'ordinateur dispose déjà d'une liste de règles, Kaspersky Embedded Systems Security propose de supprimer la liste existante ou d'y ajouter les entrées du fichier XML.

6. Enregistrez vos modifications.

Affichage des rapports du Contrôle de l'intégrité du système

Pour analyser les performances des règles du Contrôle de l'intégrité du système, vous pouvez consulter les rapports et les événements générés par l'application. Kaspersky Embedded Systems Security génère les rapports suivants concernant le module :

- Rapport sur les ordinateurs sur lesquels les règles de surveillance ont été appliquées le plus grand nombre de fois

- Rapport sur les règles de surveillance les plus fréquemment appliquées

  Pour générer un rapport sur les règles de surveillance les plus fréquemment déclenchées, l'application enregistre les événements suivants :

  - *Un changement du fichier ou du dossier a été détecté*
  - *Statistiques uniquement : opération sur les fichiers interdite dans la zone de contrôle*
  - *Opération sur un fichier autorisée dans une zone contrôlée par un utilisateur de confiance*
  - *Opération sur les fichiers non contrôlée dans la zone contrôlée*.

Pour configurer la durée de conservation de ces événements, dans la section **Configuration de l'événement** de la stratégie, indiquez la durée de l'événement général Contrôle de l'intégrité du système : *Un changement du fichier ou du dossier a été détecté*.

Par défaut, un rapport est créé pour les 30 jours précédents, en incluant la date de création du rapport.

Comment consulter les rapports du Contrôle de l'intégrité du système dans la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans le nœud **Serveur d'administration** de l'arborescence de la Console de l'administration, choisissez l'onglet **Rapports**.
3. Cliquez sur **Nouveau modèle de rapport**.

   L'Assistant de création du modèle du rapport démarre.
4. Suivez les instructions de l'Assistant de création du modèle de rapport. À l'étape **Sélection du type de modèle de rapport**, sélectionnez un rapport du Contrôle de l'intégrité du système (la section **Autres**) :

   - **Top 10 des appareils dont les règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système sont le plus souvent déclenchées**.
   - **Top 10 des règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système qui ont été le plus souvent déclenchées sur les appareils**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau sous l'onglet **Rapports**.
5. Ouvrez le rapport d'un double-clic.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Comment consulter les rapports du Contrôle de l'intégrité du système dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Surveillance → Rapports**.
2. Cliquez sur **Ajouter**.

   L'Assistant de création du modèle du rapport démarre.
3. Sous **Modèle**, dans la section **Autres**, sélectionnez un rapport du Contrôle de l'intégrité du système :

   - **Top 10 des appareils dont les règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système sont le plus souvent déclenchées**.
   - **Top 10 des règles du Contrôle de l'intégrité des fichiers/Contrôle de l'intégrité du système qui ont été le plus souvent déclenchées sur les appareils**.

   Quand l'Assistant de création du modèle de rapport est terminé, le nouveau modèle de rapport apparaît dans le tableau.
4. Sélectionnez et exécutez le rapport.

Le processus de création du rapport est lancé. Le rapport s'ouvre dans une nouvelle fenêtre.

Pour consulter les événements générés par l'application, vous pouvez également utiliser les sélections d'événements dans la console de Kaspersky Security Center.

Inspection des journaux

L'inspection des journaux surveille l'intégrité de l'environnement protégé en fonction de l'analyse du journal des événements Windows. Lorsque l'application détecte des signes de comportement atypique dans le système, elle en informe l'administrateur, car ce comportement peut indiquer une tentative de cyberattaque.

Kaspersky Embedded Systems Security analyse les journaux d'événements Windows et détecte les violations conformément aux règles. Le module inclut des règles prédéfinies. Les règles prédéfinies sont alimentées par une analyse heuristique. Vous pouvez également ajouter vos propres règles (règles personnalisées). Lorsqu'une règle se déclenche, l'application crée un événement avec l'état *Critique*.

Si vous souhaitez utiliser l'inspection des journaux, assurez-vous que la stratégie d'audit de sécurité est configurée et que le système enregistre les événements pertinents (pour plus de détails, consultez le site du Support Technique Microsoft).

Paramètre	Description
Règles prédéfinies	Liste des règles d'Inspection des journaux. Les règles prédéfinies incluent des modèles d'activité anormale sur l'ordinateur protégé. Une activité anormale peut signifier une tentative d'attaque.
Règles personnalisées	Liste des règles d'Inspection des journaux ajoutées par l'utilisateur. Vous pouvez définir vos propres critères de déclenchement de règle d'inspection des journaux. Pour ce faire, vous devez entrer un ID d'événement et sélectionner une source d'événement. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Vous pouvez également spécifier le journal d'une application tierce.

Ajout des règles personnalisées

Vous pouvez définir vos propres critères de déclenchement de règle d'inspection des journaux. Pour ce faire, vous devez entrer un ID d'événement et sélectionner une source d'événement. Vous pouvez rechercher l'ID d'événement sur le site du Support Technique de Microsoft. Vous pouvez sélectionner une source d'événement parmi les journaux standards : *Application*, *Security* et *System*. Vous pouvez également spécifier le journal d'une application tierce. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal *Windows PowerShell*).

L'application ne vérifie pas si le journal spécifié est bien présent dans le journal d'événements Windows. S'il y a une erreur dans le nom du journal, l'application ne surveille pas les événements de ce journal.

La liste des règles personnalisées comprend déjà plusieurs règles créées par les experts de Kaspersky.

Comment ajouter des règles personnalisées dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Diagnostic du système**.
4. Dans la section **Inspection des journaux**, cliquez sur **Paramètres**.

5. Cochez la case **Inspection des journaux**.

6. Sous l'onglet **Règles personnalisées**, cochez la case **Appliquer des règles personnalisées pour l'inspection des journaux**.

7. Cochez les cases en regard des règles personnalisées que vous souhaitez activer.

8. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.

9. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :

   - **Nom de la règle**.
   - **Nom du journal**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.
   - **Source**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal Windows PowerShell).
   - **Identificateurs des événements**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

10. Enregistrez vos modifications.

Comment ajouter des règles personnalisées dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Diagnostic du système** → **Inspection des journaux** et cliquez sur le bouton **Configurer**.

5. Cochez la case **Activer l'inspection des journaux**.

6. Sous l'onglet **Règles personnalisées**, cochez la case **Appliquer des règles personnalisées pour l'inspection des journaux**.

7. Configurez les règles personnalisées à l'aide des commutateurs :

8. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.

9. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :

   - **Nom de la règle**.
   - **Nom du journal d'événements Windows**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.

- **Source**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal Windows PowerShell).

- **Identifiant de l'événement**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

10. Enregistrez vos modifications.

Ajout d'une règle personnalisée dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Diagnostic du système → Inspection des journaux**.

2. Dans le panneau des résultats du nœud **Inspection des journaux**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Inspection des journaux** s'ouvre.

3. Cochez la case **Inspection des journaux**.

4. Sous l'onglet **Règles personnalisées**, cochez la case **Appliquer des règles personnalisées pour l'inspection des journaux**.

5. Cochez les cases en regard des règles personnalisées que vous souhaitez activer.

6. Si nécessaire, cliquez **Ajouter** pour créer vos propres règles personnalisées.

7. Cela ouvre une fenêtre ; dans cette fenêtre, configurez la règle personnalisée :

   - **Nom de la règle**.

   - **Nom du journal**. Journaux d'événements Windows. Les journaux suivants sont disponibles : *Application*, *Security*, *System*.

   - **Source**. Journaux d'application tiers. Vous pouvez connaître le nom du journal des applications tierces à l'aide de l'outil Observateur d'événements. Les journaux des applications tierces sont conservés dans le dossier Journaux des applications et des services (par exemple, le journal Windows PowerShell).

   - **Identificateurs des événements**. IDs d'événement dans le journal d'événements Windows. Vous pouvez rechercher l'ID d'événement dans la documentation technique de Microsoft.

8. Enregistrez vos modifications.

Par conséquent, lorsque la règle se déclenche, Kaspersky Embedded Systems Security crée un événement *Critique*.

Configuration des règles prédéfinies

Les règles prédéfinies incluent des modèles d'activité anormale sur l'ordinateur protégé. Une activité anormale peut signifier une tentative d'attaque. Les règles prédéfinies sont alimentées par une analyse heuristique. Sept règles prédéfinies sont disponibles pour l'inspection des journaux. Vous pouvez activer ou désactiver n'importe quelle règle. Les règles prédéfinies ne peuvent pas être supprimées.

Vous pouvez configurer les critères de déclenchement des règles qui surveillent les événements pour les opérations suivantes :

- Détection des attaques brute-force contre les mots de passe
- Traitement de la connexion au réseau

Comment configurer des règles prédéfinies dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Diagnostic du système**.
4. Dans la section **Inspection des journaux**, cliquez sur **Paramètres**.
5. Cochez la case **Inspection des journaux**.
6. Sous l'onglet **Règles prédéfinies**, cochez la case **Appliquer des règles prédéfinies pour l'inspection des journaux**.
7. Cochez ou décochez les cases pour configurer des règles prédéfinies :
   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.
   - **Certains comportements indiquent une possible violation du journal des événements Windows**.
   - **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
   - **Connexion inhabituelle utilisant des identifiants explicites**.
   - **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.
   - **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.
8. Si nécessaire ; configurez la règle **Certains comportements indiquent une possible attaque par force brute dans le système** :
   a. Cliquez sur le bouton **Paramètres** à côté de la règle.
   b. Dans la fenêtre qui s'ouvre, indiquez le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle se déclenche.
   c. Cliquez sur le bouton **OK**.
9. Si vous avez sélectionné la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**, vous devez configurer ses paramètres :
   a. Cliquez sur le bouton **Paramètres** à côté de la règle.
   b. Dans la fenêtre qui s'ouvre, dans le groupe **Détection des connexions au réseau**, spécifiez le début et la fin de l'intervalle de temps.

Kaspersky Embedded Systems Security considère les tentatives de connexion effectuées pendant l'intervalle défini comme une activité anormale.

Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.

c. Créez la liste des utilisateurs de confiance et des adresses IP de confiance (IPv4 et IPv6).

Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Kaspersky Embedded Systems Security ne surveille pas les tentatives de connexion de ces utilisateurs et ordinateurs.

> L'exclusion d'ordinateurs de confiance par adresse IP ne fonctionne pas dans l'application fonctionnant sous Windows XP.

d. Cliquez sur **OK**.

10. Enregistrez vos modifications.

Comment configurer des règles prédéfinies dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Diagnostic du système → Inspection des journaux** et cliquez sur le bouton **Configurer**.
5. Cochez la case **Activer l'inspection des journaux**.
6. Sous l'onglet **Règles prédéfinies**, cochez la case **Appliquer des règles prédéfinies pour l'inspection des journaux**.
7. Configurez les règles prédéfinies à l'aide des commutateurs :

   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.
   - **Certains comportements indiquent une possible violation du journal des événements Windows**.
   - **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
   - **Connexion inhabituelle utilisant des identifiants explicites**.
   - **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.
   - **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.

8. Sous l'onglet **Élargi**, configurez les paramètres de la tâche suivants :

   - Le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle **Certains comportements indiquent une possible attaque par force brute dans le système** se déclenche.

   - Pour que la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau** se déclenche, spécifiez les valeurs de début et de fin de l'intervalle de temps pendant lequel l'application considère toutes les tentatives de connexion comme une activité anormale.

     Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.

9. Créez la liste des utilisateurs de confiance et des adresses IP de confiance (IPv4 et Ipv6) sous les onglets correspondants.

   Vous pouvez sélectionner des utilisateurs dans la liste des comptes ou saisir un nom d'utilisateur local manuellement.

   L'exclusion d'ordinateurs de confiance par adresse IP ne fonctionne pas dans l'application fonctionnant sous Windows XP.

10. Enregistrez vos modifications.

Configuration des règles prédéfinies dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Diagnostic du système → Inspection des journaux**.

2. Dans le panneau des résultats du nœud **Inspection des journaux**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Inspection des journaux** s'ouvre.

3. Cochez la case **Inspection des journaux**.

4. Sous l'onglet **Règles prédéfinies**, cochez la case **Appliquer des règles prédéfinies pour l'inspection des journaux**.

5. Cochez ou décochez les cases pour configurer des règles prédéfinies :

   - **Certains comportements indiquent une possible attaque par force brute dans le système**.
   - **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**.
   - **Certains comportements indiquent une possible violation du journal des événements Windows**.
   - **Des actions inhabituelles ont été détectées au nom d'un nouveau service installé**.
   - **Connexion inhabituelle utilisant des identifiants explicites**.
   - **Certains comportements indiquent une possible attaque Kerberos forged PAC (MS14-068) dans le système**.
   - **Des modifications suspectes ont été détectées dans le groupe privilégié intégré « Administrateurs »**.

6. Si nécessaire ; configurez la règle **Certains comportements indiquent une possible attaque par force brute dans le système** :

   a. Cliquez sur le bouton **Paramètres** à côté de la règle.

   b. Dans la fenêtre qui s'ouvre, indiquez le nombre de tentatives et un délai dans lequel les tentatives de saisie d'un mot de passe doivent être effectuées pour que la règle se déclenche.

   c. Cliquez sur le bouton **OK**.

7. Si vous avez sélectionné la règle **Une activité inhabituelle a été détectée lors d'une session de connexion au réseau**, vous devez configurer ses paramètres :

   a. Cliquez sur le bouton **Paramètres** à côté de la règle.

   b. Dans la fenêtre qui s'ouvre, dans le groupe **Détection des connexions au réseau**, spécifiez le début et la fin de l'intervalle de temps.

   Kaspersky Embedded Systems Security considère les tentatives de connexion effectuées pendant l'intervalle défini comme une activité anormale.

   Par défaut, l'intervalle n'est pas défini, et l'application ne surveille pas les tentatives de connexion. Pour que l'application surveille en permanence les tentatives de connexion, réglez l'intervalle sur 00h00 - 23h59. Le début et la fin de l'intervalle ne doivent pas coïncider. Si elles sont identiques, l'application ne surveille pas les tentatives de connexion.

   c. Créez la liste des utilisateurs de confiance et des adresses IP de confiance (IPv4 et IPv6).

   Vous pouvez sélectionner des utilisateurs dans Active Directory, dans la liste des comptes dans Kaspersky Security Center ou en saisissant un nom d'utilisateur local manuellement. Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Créer la liste d'utilisateurs à partir d'Active Directory. Kaspersky Embedded Systems Security ne surveille pas les tentatives de connexion de ces utilisateurs et ordinateurs.

   > L'exclusion d'ordinateurs de confiance par adresse IP ne fonctionne pas dans l'application fonctionnant sous Windows XP.

   d. Cliquez sur **OK**.

8. Enregistrez vos modifications.

Par conséquent, lorsque la règle se déclenche, Kaspersky Embedded Systems Security crée un événement *Critique*.

Analyse à la demande

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

À propos des tâches d'analyse à la demande

Kaspersky Embedded Systems Security recherche des virus et autres menaces informatique dans la zone indiquée. Kaspersky Embedded Systems Security analyse les fichiers, la mémoire vive de l'appareil protégé et les objets de démarrage.

Kaspersky Embedded Systems Security propose les tâches Analyse à la demande suivantes :

- La tâche *Analyse 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 et zones d'amorce des disques durs et des disques amovibles, mémoire système et mémoire du processus. Kaspersky Embedded Systems Security applique les paramètres de sécurité qui correspondent au niveau **Inform**. Vous pouvez modifier les paramètres la tâche *Analyse des zones critiques*.

- La tâche *Vérification de l'intégrité de l'application* est exécutée quotidiennement. Elle permet de vérifier si les modules de Kaspersky Embedded Systems Security ont été endommagés ou modifiés. Le dossier d'installation de l'application est analysé. Les statistiques de l'exécution de la tâche indique le nombre de modules analysés et le nombre de modules endommagés. Les paramètres de la tâche sont définis par défaut et ne sont pas modifiables. Les paramètres de la planification du lancement de la tâche peuvent être modifiés.

- La tâche *Analyse des disques amovibles* analyse tous les fichiers que vous exécutez ou copiez, même si le fichier se trouve sur un disque amovible. Pour empêcher la propagation de virus et autres logiciels malveillants, vous pouvez configurer des analyses automatiques des lecteurs amovibles lorsqu'ils sont connectés à l'ordinateur.

- La tâche *Analyse complète* est exécutée chaque semaine. La tâche assure une analyse approfondie de l'appareil protégé, y compris du stockage de la Sauvegarde du système, des secteurs d'amorçage et des bases de données de messagerie.

Vous pouvez également créer des tâches d'analyse à la demande définie par l'utilisateur, par exemple, une tâche pour l'analyse des dossiers partagés sur l'appareil protégé.

Kaspersky Embedded Systems Security peut exécuter simultanément plusieurs tâches d'analyse à la demande.

À propos de la zone d'analyse de la tâche et des paramètres de sécurité

Dans la console de l'application, la zone d'analyse de la tâche d'analyse à la demande sélectionnée se présente sous la forme d'une liste de ressources de fichiers de l'appareil protégé que Kaspersky Embedded Systems Security peut contrôler.

Les éléments ou les nœuds sont présentés sous forme de liste des ressources de fichiers de l'appareil protégé de la manière suivante :

☑ Nœud repris dans la zone d'analyse.

☐ Nœud exclu de la zone d'analyse.

Paramètres de sécurité

Dans la tâche à la demande sélectionnée, vous pouvez modifier les valeurs des paramètres de sécurité par défaut de la même manière pour toute la zone de protection ou d'analyse ou avec des variations pour différents nœuds ou éléments dans la liste des ressources de fichiers de l'appareil.

Si le même objet est inclus dans plusieurs entrées de la zone de protection et si ces entrées ont des niveaux de sécurité différents, la dernière règle de la liste a la priorité. Prenons l'exemple d'une zone de protection qui inclut deux entrées : **Tous les disques durs** (niveau de sécurité **Inform**) et `*\Users\*\Downloads\*` (niveau de sécurité **Custom**). L'application analyse les disques durs conformément au niveau Informer, à l'exception du dossier `Downloads`. L'application analyse le dossier `Downloads` selon les paramètres définis manuellement, car cette entrée est la dernière de la liste de la zone de protection.

Les paramètres de sécurité configurés pour le nœud principal sélectionné sont appliqués automatiquement à tous les nœuds enfant. Les paramètres de sécurité du nœud parent ne sont pas appliqués aux nœuds enfants configurés séparément.

Vous pouvez configurer les paramètres de la zone d'analyse ou de la zone de protection sélectionnée de l'une des manières suivantes :

- Sélectionner un des trois niveaux de sécurité prédéfinis (**Performance maximale**, **Recommandé** ou **Protection maximale**) ;
- Modifier manuellement les paramètres de sécurité pour les nœuds sélectionnés dans la liste des ressources fichier de l'appareil protégé (le niveau de sécurité prend alors la valeur **Personnalisé**).

Zones d'analyse prédéfinies

La liste des ressources fichier de l'appareil protégé s'affiche dans le panneau de détails de l'entrée de la tâche d'analyse à la demande sélectionnée dans la fenêtre **Zone d'analyse**.

La liste des ressources fichiers affiche les entrées auxquelles vous avez accès en lecture conformément aux paramètres de sécurité configurés de Microsoft Windows.

Kaspersky Embedded Systems Security propose les zones d'analyse prédéfinies suivantes :

- **Tous les disques durs**. Kaspersky Embedded Systems Security analyse les objets des disques durs d'un appareil protégé. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques durs ainsi que des disques, des répertoires ou des fichiers individuels.

- **Tous les disques amovibles**. Kaspersky Embedded Systems Security analyse les fichiers sur les appareils externes tels que les lecteurs de disques compacts ou les disques amovibles. Vous pouvez inclure ou exclure de la zone d'analyse tous les disques amovibles ainsi que des disques, des répertoires ou des fichiers individuels.

- **Tous les disques réseau**. Vous pouvez ajouter à la zone d'analyse des répertoires de réseau ou des fichiers en indiquant leur chemin d'accès au format UNC (Universal Naming Convention). Le compte utilisateur exploité pour lancer la tâche doit jouir des privilèges d'accès aux dossiers réseau ou aux fichiers ajoutés. Par défaut, les tâches d'analyse à la demande sont exécutées sous le compte système.

  Les disques réseau connectés ne sont pas non plus repris dans l'arborescence des ressources fichier de l'appareil protégé. Pour inclure les objets d'un disque réseau dans la zone d'analyse, indiquez le chemin d'accès au répertoire correspondant à ce disque réseau au format UNC (Universal Naming Convention).

- **Mémoire du noyau**. Kaspersky Embedded Systems Security analyse les fichiers exécutables et les modules des processus exécutés dans le système d'exploitation au moment de l'analyse.

- **Processus exécutés et objets de démarrage automatique**. Kaspersky Embedded Systems Security analyse les objets auxquels les clés du registre et les fichiers de configuration font référence, par exemple WIN.INI ou SYSTEM.INI, ainsi que les modules de l'application qui sont lancés automatiquement au démarrage de l'appareil protégé.

- **Secteurs d'amorçage**. Kaspersky Embedded Systems Security analyse les secteurs d'amorçage des disques durs et des supports amovibles.

- **Sauvegarde système**. Kaspersky Embedded Systems Security analyse le contenu du dossier Informations sur le volume système.

  Dans Kaspersky Embedded Systems Security 4.1, la messagerie est exclue du champ d'application de l'analyse. Si vous utilisez une version antérieure du plug-in d'administration, l'application exclut les emails de la portée de l'analyse, même si la stratégie les inclut.

Les zones d'analyse standard s'affichent par défaut dans l'arborescence des ressources de fichiers réseau. Elles peuvent être ajoutées à la liste des ressources de fichier réseau lorsqu'elle est créée 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 des zones critiques* :
  - **Tous les disques durs** (à l'exception des dossiers Windows).
  - **Tous les disques amovibles**.
  - **Mémoire du noyau**.
  - **Processus exécutés et objets de démarrage automatique**.

- Tâche *Analyse à la demande* :
  - **Tous les disques durs** (à l'exception des dossiers Windows).
  - **Tous les disques amovibles**.
  - **Mémoire du noyau**.
  - **Processus exécutés et objets de démarrage automatique**.
- Tâche *Analyse complète* :
  - **Tous les disques durs** (à l'exception des dossiers Windows).
  - **Tous les disques amovibles**.
  - **Mémoire du noyau**.
  - **Processus exécutés et objets de démarrage automatique**.
  - **Sauvegarde système**.
  - **Secteurs d'amorçage**.

Analyse des fichiers dans le stockage en ligne

À propos des fichiers cloud

Kaspersky Embedded Systems Security peut interagir avec les fichiers sur le cloud Microsoft OneDrive. L'application prend en charge la nouvelle fonctionnalité OneDrive Files On-Demand.

> Kaspersky Embedded Systems Security ne prend pas en charge d'autres stockages en ligne.

OneDrive Files On-Demand permet d'accéder à tous les fichiers de OneDrive sans avoir à les télécharger tous et à utiliser de l'espace de stockage sur votre appareil. Vous pouvez télécharger des fichiers sur votre disque dur lorsque vous en avez besoin.

Lorsque la fonction OneDrive Files On-Demand est activée, des icônes d'état apparaissent en regard de chaque fichier dans la colonne **État** de l'Explorateur de fichiers. Chaque fichier peut prendre un des états suivants :

Cette icône d'état indique que le fichier est *uniquement disponible en ligne*. Les fichiers uniquement disponibles en ligne ne sont pas stockés sur le disque dur. Vous ne pouvez pas les ouvrir lorsque votre appareil n'est pas connecté à Internet.

Cette icône d'état indique qu'un fichier est *disponible en local*. Ce cas se produit lorsque vous ouvrez un fichier uniquement disponible en ligne et qu'il se télécharge sur votre appareil. Vous pouvez ouvrir un fichier disponible en local à tout moment même sans accès Internet. Pour gagner de l'espace, vous pouvez redéfinir l'état du fichier sur uniquement en ligne.

Cette icône d'état indique qu'un fichier est *stocké sur le disque dur et toujours disponible*.

Analyse des fichiers de stockage dans le cloud

Kaspersky Embedded Systems Security analyse uniquement les fichiers du cloud lorsqu'ils sont stockés localement sur un appareil protégé. Ces fichiers OneDrive ont les états et . Les fichiers sont ignorés pendant l'analyse car ils ne sont pas physiquement situés sur l'appareil protégé.

Kaspersky Embedded Systems Security ne télécharge pas automatiquement les fichiers du Cloud lors de l'analyse, même s'ils figurent dan la zone d'analyse.

Les fichiers du Cloud sont traités par plusieurs tâches de Kaspersky Embedded Systems Security dans différents scénario en fonction du type de tâche :

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone de protection du module Protection des fichiers en temps réel. Un fichier est analysé quand l'utilisateur y accède. Si l'utilisateur accède à un fichier , celui-ci est téléchargé, devient disponible en local et a désormais l'état . Cela permet au fichier d'être traité par le module Protection des fichiers en temps réel.

- Analyse des fichiers cloud en temps réel : vous pouvez ajouter des dossiers contenant des fichiers cloud à la zone d'analyse de la tâche Analyse à la demande. La tâche analyse les fichiers avec les états et . Si des fichiers sont trouvés dans la zone, ils seront ignorés pendant l'analyse et un événement d'information sera enregistré dans le journal d'exécution de la tâche. Il indiquera que le fichier analysé n'est qu'une marque de réservation pour un fichier cloud et n'existe pas sur un disque local.

- Création et utilisation de règles du Contrôle du lancement des applications : vous pouvez créer des règles d'autorisation et d'interdiction pour les fichiers et à l'aide de la tâche *Générateur de règles pour le Contrôle du lancement des applications*. Le module Contrôle du lancement des applications applique le principe Interdire par défaut et des règles créées pour traiter et interdire les fichiers cloud.

  Le module Contrôle du lancement des applications bloque le lancement de tous les fichiers dans le Cloud, peu importe leur état. Les fichiers ne sont pas inclus dans la zone de génération de règles par l'application car ils ne sont pas physiquement stockés sur votre disque dur. Vu que les règles d'autorisation ne peuvent être créées pour ces fichiers. Par conséquent, ils sont soumis au principe Interdiction par défaut.

Lorsqu'une menace est détectée sur un fichier cloud OneDrive, l'application exécute l'action spécifiée dans les paramètres de la tâche effectuant l'analyse. Ainsi, le fichier peut être supprimé, désinfecté, placé en quarantaine ou sauvegardé.

Les modifications apportées aux fichiers locaux sont synchronisées avec les copies stockées sur OneDrive conformément aux principes exposés dans la documentation Microsoft OneDrive correspondante.

À propos des niveaux de sécurité prédéfinis

Le paramètre de sécurité **Utiliser l'analyse heuristique** n'est pas inclus dans les paramètres des niveaux de sécurité prédéfinis. La modification de ce paramètre ne changera pas le niveau de sécurité par défaut que vous avez sélectionné.

Vous pouvez appliquer l'un des quatre niveaux de sécurité prédéfinis à un nœud sélectionné dans l'arborescence des ressources de fichiers de l'appareil : **Performance maximale**, **Recommandé**, **Protection maximale** ou **Informer**. Chacun de ces niveaux de sécurité possède sa propre sélection de paramètres de sécurité prédéfinie (cf. tableau ci-dessous).

Performance maximale

Le niveau de sécurité **Performance maximale** est recommandé si votre réseau a adopté des mesures de sécurité pour l'appareil protégé additionnelles comme des pare-feux ou des stratégies de sécurité existantes, en plus de l'installation de Kaspersky Embedded Systems Security sur les appareils protégés et les postes de travail.

Recommandé

Le niveau de sécurité **Recommandé** offre le meilleur équilibre entre la protection et l'impact sur les performances des appareils protégés. Les experts de Kaspersky recommandent ce niveau pour protéger les appareils sur la majorité des réseaux d'entreprise. Le niveau de sécurité **Recommandé** est sélectionné par défaut.

Protection maximale

Le niveau de sécurité **Protection maximale** est recommandé si le réseau de votre organisation requiert un niveau de sécurité élevé pour les appareils.

Informer

Le niveau de sécurité **Informer** est recommandé si le réseau de votre organisation comporte un grand nombre d'ordinateurs potentiellement infectés et si leur blocage est susceptible de perturber considérablement le fonctionnement de votre organisation.

Niveaux de sécurité prédéfinis et valeurs des paramètres correspondants

Options	Niveau de sécurité			
	Performance maximale	Recommandé	Protection maximale	Informer
Object types	Objets analysés en fonction du format	Tous les objets	Tous les objets	Tous les objets
Scan only new and modified files	Activée	Désactivée	Désactivée	Désactivée
Action to perform on infected and other objects	Désinfecter. Supprimer si la désinfection échoue	Exécuter l'action recommandée par les experts de Kaspersky	Désinfecter. Supprimer si la désinfection échoue	Informer

Options	Niveau de sécurité			
	Performance maximale	Recommandé	Protection maximale	Informer
Scan of compound files	Analyser les paquets de distribution et les fichiers au format Microsoft Office	Analyser toutes les archives, les paquets de distribution et les fichiers au format Microsoft Office	Analyser toutes les archives, les paquets de distribution et les fichiers au format Microsoft Office	Analyser toutes les archives, les paquets de distribution et les fichiers au format Microsoft Office
Les objets système critiques sont les fichiers nécessaires au fonctionnement du système d'exploitation et de Kaspersky Embedded Systems Security. Vous ne pouvez pas supprimer ces fichiers. Il est impossible d'arrêter les processus associés à ces objets.				
Appliquer l'action aux types d'objets sélectionnés	Par défaut, tous les types d'objets sont analysés.	Par défaut, tous les types d'objets sont analysés.	Par défaut, tous les types d'objets sont analysés.	Par défaut, tous les types d'objets sont analysés.
Entirely remove the compound file that cannot be modified by the application in case of embedded object detection	non	non	non	non
Exclure les fichiers	non	non	non	non
Do not detect objects by type	non	non	non	non
Stop scanning if it takes longer than (sec)	60 s	non	non	non
Do not scan compound objects larger than (MB)	8 Mo	non	non	non
Utiliser la technologie iSwift	Oui	Oui	Oui	Oui
Utiliser la technologie iChecker	Oui	Oui	Oui	Oui

Analyse des disques amovibles

Vous pouvez configurer l'analyse des disques amovibles connectés via USB à l'appareil protégé.

Kaspersky Embedded Systems Security lance l'analyse des disques amovibles lorsque ces derniers sont enregistrés dans le système d'exploitation en tant que appareil externe USB. L'application n'analyse pas le disque amovible si le module Contrôle des appareils a bloqué la connexion de ce dernier.

Kaspersky Embedded Systems Security autorise l'accès aux disques amovibles durant l'analyse.

Les résultats de l'analyse de chaque disque amovible peuvent être consultés dans le journal d'exécution de la tâche Analyse à la demande créée lors de la connexion du disque amovible.

Vous pouvez modifier les valeurs des paramètres du module Analyse des disques amovibles (cf. tableau ci-dessous).

Paramètres d'analyse des disques amovibles

Paramètre	Valeur par défaut	Description
Analyser les disques amovibles lors d'une connexion via USB	Non cochée	Vous pouvez activer ou désactiver l'analyse des disques amovibles lorsqu'ils sont connectés à l'appareil protégé via USB.
Analyser le disque amovible si sa taille ne dépasse pas (Mo)	4096 Mo	Vous pouvez réduire la plage de déclenchement du module en indiquant le volume de données maximum sur le disque amovible. Kaspersky Embedded Systems Security ne lance pas l'analyse du disque amovible si le volume des données qu'il contient est supérieur à la valeur indiquée.
Analyser avec le niveau de sécurité	Protection maximale	Vous pouvez configurer les paramètres des tâches d'analyse à la demande créées en choisissant un de trois niveaux de sécurité suivants : • **Protection maximale** • **Recommandé** • **Performance maximale** • **Informer**. L'algorithme des actions à effectuer lors de la détection d'objets infectés, probablement infectés et autres, ainsi que d'autres paramètres d'analyse pour chaque niveau de sécurité correspondent aux niveaux de sécurité préétablis dans les tâches d'analyse à la demande.

Paramètres par défaut de la tâche d'analyse à la demande

Par défaut, les tâches d'analyse à la demande possèdent les paramètres décrits dans le tableau ci-dessous. Vous pouvez configurer les tâches d'analyse à la demande locales du système et définies par l'utilisateur.

Paramètres par défaut de la tâche d'analyse à la demande

Paramètre	Valeur par défaut	Description
Zone d'analyse	S'applique aux tâches locales du système et définies par l'utilisateur : • **Analyse des zones critiques** : tout l'appareil protégé, à l'exception des dossiers partagés et de certains fichiers du système d'exploitation ; • **Analyse à la demande** (tâches définies par l'utilisateur) : tout l'appareil protégé. • **Analyse complète** : analyse minutieuse de l'appareil protégé.	Vous pouvez modifier la zone d'analyse. La zone d'analyse ne peut pas être configurée pour les tâches du système local **Analyse des disques amovibles** et **Vérification de l'intégrité de l'application**.
Paramètres de sécurité	Identique pour toute la zone d'analyse ; correspond au niveau de sécurité **Recommandé**.	Pour les nœuds sélectionnés dans la liste des ressources de fichiers de l'appareil protégé, vous pouvez exécuter les actions suivantes : • Sélectionner un autre niveau de sécurité prédéfini ; • Modifier manuellement les paramètres de sécurité.
Utiliser l'analyse heuristique	Appliqué avec le niveau d'analyse **Moyen** pour les tâches *Analyse des zones critiques*, *Analyse à la demande* et *Analyse complète*.	Vous pouvez activer ou désactiver l'application de l'analyse heuristique et régler le niveau de l'analyse.
Paramètres pour lancer une tâche avec des autorisations spécifiques	La tâche est lancée sous les autorisations du compte système.	Vous pouvez modifier les paramètres de lancement sous des autorisations spécifiques pour toutes les tâches d'analyse à la demande système ou définies par l'utilisateur, sauf pour la tâche *Vérification de l'intégrité de l'application*.
Exécuter la tâche en arrière-plan	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.
Considérer la tâche comme une Analyse des zones critiques	Appliqué pour les tâches *Analyse à la demande*, *Analyse des zones critiques* et *Analyse complète*.	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.

Paramètre	Valeur par défaut	Description
Ne pas exécuter plusieurs tâches d'analyse en même temps	Pas appliqué	Vous pouvez définir la priorité d'exécution des tâches d'analyse à la demande.
Planification du lancement de la tâche	Appliqué pour les tâches du système local : *Analyse des zones critiques*, *Vérification de l'intégrité de l'application* et *Analyse complète* – **Chaque mois**.	Vous pouvez configurer les paramètres du lancement programmé de la tâche.

Gestion des tâches d'analyse à la demande

Cette section décrit la création et la configuration de la tâche Analyse à la demande sur l'appareil protégé.

Création d'une tâche d'analyse à la demande

Création d'une tâche d'analyse à la demande dans la Console d'administration de Kaspersky Security Center

1. Lancez l'Assistant de nouvelle tâche.
2. Dans la fenêtre **Sélectionnez le type de tâche**, sélectionnez **Analyse à la demande** et cliquez sur **Suivant**.
3. Dans la fenêtre **Zone d'analyse**, définissez la zone d'analyse.

   La zone d'analyse reprend par défaut les secteurs critiques de l'appareil protégé. Les zones d'analyse sont accompagnées de l'icône ☑ dans le tableau. Les zones d'analyse exclues sont accompagnées de l'icône ☐ dans le tableau. Vous pouvez modifier la zone d'analyse, y inclure des zones distinctes prédéfinies, des disques, des dossiers, des objets de réseaux et des fichiers et définir les paramètres particuliers de la protection pour chaque zone ajoutée.

   - Pour exclure une zone de l'analyse, sélectionnez l'élément de la liste correspondant et cliquez sur **Supprimer**.
   - Pour inclure une zone d'analyse, un disque, un dossier, un objet réseau ou un fichier prédéfini dans la zone d'analyse :
     a. Cliquez sur **Ajouter**.
     b. Dans la fenêtre **Sélection de la zone d'analyse**, sélectionnez la zone d'analyse prédéfinie dans la liste et cliquez sur **OK**.
   - Pour exclure des sous-dossiers ou des fichiers de la zone d'analyse, procédez comme suit :
     a. Sélectionnez un dossier (ou un disque) ajouté dans la fenêtre **Zone d'analyse**.
     b. Cliquez sur **Modifier**.
     c. Décochez la case **Inclure les sous-dossiers**.

- Pour modifier les paramètres de sécurité de la zone d'analyse :

  a. Sélectionnez la zone d'analyse dont vous souhaitez modifier les paramètres, puis cliquez sur **Configurer**.

  b. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'un des niveaux de sécurité prédéfinis ou cliquez sur le bouton **Paramètres** pour configurer manuellement les paramètres de sécurité.

  Les paramètres de sécurité sont configurés de la même manière que pour la tâche Protection des fichiers en temps réel.

4. Configurer l'analyseur heuristique et l'intégration avec d'autres modules :

   - Configurez l'utilisation de l'analyse heuristique.
   - Cochez la case **Exécuter la tâche en arrière-plan** si vous souhaitez attribuer une priorité *Faible* au processus de travail dans lequel la tâche sera exécutée.

     Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

   - Cochez la case **Considérer la tâche comme une Analyse des zones critiques** si vous souhaitez utiliser la tâche comme une tâche *Analyse des zones critiques*.
   - Cochez la case **Ne pas exécuter plusieurs tâches d'analyse en même temps** pour optimiser la charge sur l'ordinateur.

5. Dans la fenêtre **Sélectionnez les appareils auxquels la tâche sera affectée**, spécifiez la liste des appareils et cliquez sur **Suivant**.

6. Dans la fenêtre **Sélection du compte utilisateur pour exécuter la tâche**, spécifiez un compte et cliquez sur **Suivant**.

7. Dans la fenêtre **Planifier la tâche**, configurez la planification de la tâche et cliquez sur **Suivant**.

8. Saisissez un nom pour la tâche.

   Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants : " * < > & \ : |

9. La fenêtre **Fin de la création de la tâche** s'ouvre. Cliquez sur le bouton **Terminer** pour terminer la création de la tâche.

Une nouvelle tâche *Analyse à la demande* est créée pour un appareil protégé ou un groupe d'appareils protégés sélectionnés.

Création d'une tâche Analyse à la demande dans Kaspersky Security Center Web Console

1. Lancez l'Assistant de nouvelle tâche.

2. Dans la fenêtre **Nouvelle tâche**, dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.

3. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**, puis cliquez sur **Suivant**.

4. Sélectionnez la zone d'action de la tâche et cliquez sur **Suivant**.

5. Dans la fenêtre **Sélection du compte utilisateur pour exécuter la tâche**, spécifiez un compte et cliquez sur **Suivant**.

6. Saisissez un nom pour la tâche.

   Le nom de la tâche ne doit pas compter plus de 100 caractères et ne peut contenir les caractères suivants : " * < > & \ : |

7. La fenêtre **Fin de la création de la tâche** s'ouvre. Cliquez sur le bouton **Terminé** pour terminer la création de la tâche.

Une nouvelle tâche *Analyse à la demande* est créée pour un appareil protégé ou un groupe d'appareils protégés sélectionnés.

Création d'une tâche d'analyse à la demande via la Console de l'application

Vous pouvez créer des tâches définies par l'utilisateur pour un seul appareil protégé dans le nœud **Analyse à la demande**.

Pour créer et configurer une tâche d'analyse à la demande :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Analyse à la demande**.

2. Choisissez l'option **Créer une tâche**.

   La fenêtre **Créer une tâche** s'ouvre.

3. Saisissez le nom de la tâche, puis cliquez sur **OK**.

La tâche *Analyse à la demande* pour un appareil protégé distinct est créée.

Exécution d'une tâche d'analyse à la demande en arrière-plan

Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité de base *Moyenne* (Normal).

Vous pouvez attribuer la priorité *Faible* au processus dans lequel la tâche *Analyse à la demande* va être exécutée. La réduction de la priorité du processus allonge la durée d'exécution des tâches et peut également avoir un effet positif sur les performances des processus d'autres applications actives.

Dans un processus de faible priorité, il est possible d'exécuter plusieurs tâches en arrière-plan.

Pour modifier la priorité de la tâche *Analyse à la demande* existante, cochez ou décochez la case **Exécuter la tâche en arrière-plan** dans les paramètres de la tâche.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à une tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Enregistrement de l'exécution d'une analyse rapide

Par défaut, l'état de la protection de l'appareil apparaît dans le panneau des résultats du nœud **Kaspersky Embedded Systems Security** et il est actualisé chaque semaine après la fin de la tâche *Analyse des zones critiques*.

L'heure de l'actualisation de l'état de la protection de l'appareil est liée à la planification de la tâche d'analyse à la demande où la case **Considérer la tâche comme une Analyse des zones critiques** est cochée dans les paramètres.

Configuration de la zone d'analyse dans la tâche Analyse à la demande

Si vous modifiez la zone d'analyse dans les tâches *Analyse au démarrage du système d'exploitation* et *Analyse des zones critiques*, vous pourrez rétablir la zone d'analyse par défaut pour ces tâches en exécutant la réparation de Kaspersky Embedded Systems Security à l'aide de l'Assistant d'installation.

Configuration de la zone d'analyse pour la tâche Analyse à la demande dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client requis.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Passez à la section **Tâches**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de la tâche **Analyse à la demande**.
6. Sélectionnez la section **Zone d'analyse**.
7. Pour ajouter des zones à la zone d'analyse, cochez les cases en regard de celles-ci.
8. Si vous souhaitez ajouter une zone d'analyse qui ne figure pas dans la liste, procédez comme suit :
    a. Cliquez sur **Ajouter**.
    b. Dans la fenêtre qui s'ouvre, sélectionnez une zone, un disque distinct, un dossier ou un emplacement réseau.
    c. Si vous souhaitez inclure des sous-dossiers dans la zone d'analyse, cochez la case **Inclure les sous-dossiers**.
9. Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.
10. Pour modifier une zone d'analyse, sélectionnez-la dans la liste et cliquez sur **Modifier**.

11. Pour masquer une zone d'analyse ajoutée précédemment à la liste des ressources de fichiers réseau, sélectionnez la zone d'analyse et cliquez sur **Supprimer**.

    La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.

12. Cliquez sur le bouton **OK**.

La fenêtre Configuration de la zone d'analyse s'ouvre. Les paramètres de la tâche définis seront enregistrés.

Configuration de la zone d'analyse pour la tâche Analyse à la demande dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Ressources (Appareils)**.
2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez configurer la tâche.
3. Sélectionnez la section **Tâches**.
4. Une fenêtre s'ouvre. Dans cette fenêtre, double-cliquez pour ouvrir les propriétés de la tâche **Analyse à la demande**.
5. Sélectionnez l'onglet **Paramètres de l'application**.
6. Pour ajouter des zones à la zone d'analyse, activez les commutateurs en regard de celles-ci.
7. Si vous souhaitez ajouter une zone d'analyse qui ne figure pas dans la liste, procédez comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans la fenêtre qui s'ouvre, sélectionnez une zone, un disque distinct, un dossier ou un emplacement réseau.
   c. Si vous souhaitez inclure des sous-dossiers dans la zone d'analyse, cochez la case **Sous-dossiers**.
8. Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.
9. Pour modifier une zone d'analyse, sélectionnez-la dans la liste et cliquez sur **Modifier la zone**.
10. Pour masquer une zone d'analyse ajoutée précédemment à la liste des ressources de fichiers réseau, sélectionnez la zone d'analyse et cliquez sur **Supprimer**.

    La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.

11. Cliquez sur **Enregistrer**.

La fenêtre Configuration de la zone d'analyse s'ouvre. Les paramètres de la tâche définis seront enregistrés.

Configuration de la zone d'analyse de la tâche Analyse à la demande dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.

3. Dans le panneau des résultats du nœud sélectionné, cliquez sur le lien **Configurer la zone de protection**.
4. Dans la fenêtre qui s'ouvre, pour ajouter des zones à l'analyse, cochez les cases en regard de celles-ci.
5. Si vous souhaitez ajouter une zone d'analyse qui ne figure pas dans la liste, procédez comme suit :
   a. Cliquez sur **Ajouter**.
   b. Dans la fenêtre qui s'ouvre, sélectionnez une zone, un disque distinct, un dossier ou un emplacement réseau.
   c. Si vous souhaitez inclure des sous-dossiers dans la zone d'analyse, cochez la case **Inclure les sous-dossiers**.
6. Pour exclure certaines entrées de la zone d'analyse, décochez les cases à côté des noms de ces entrées.
7. Pour modifier une zone d'analyse, sélectionnez-la dans la liste et cliquez sur **Modifier la zone**.
8. Pour masquer une zone d'analyse ajoutée précédemment à la liste des ressources de fichiers réseau, sélectionnez la zone d'analyse et cliquez sur **Supprimer**.

   La zone d'analyse est exclue de la zone d'application de la tâche d'analyse à la demande lors de sa suppression de la liste des ressources de fichier réseau.

9. Cliquez sur **OK**.

La fenêtre Configuration de la zone d'analyse s'ouvre. Les paramètres de la tâche définis seront enregistrés.

Configuration des paramètres de la tâche d'analyse à la demande

Comment configurer la tâche Analyse à la demande dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client requis.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Passez à la section **Tâches**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de la tâche **Analyse à la demande**.
6. Sélectionnez la section **Options**.
7. Cochez ou décochez la case **Utiliser l'analyse heuristique**.
8. Si nécessaire, modifiez le niveau d'analyse.

9. Cochez la case **Exécuter la tâche en arrière-plan** si vous souhaitez attribuer une priorité *Faible* au processus de travail dans lequel la tâche sera exécutée.

   Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

10. Cochez la case **Considérer la tâche comme une Analyse des zones critiques** si vous souhaitez utiliser la tâche comme une tâche *Analyse des zones critiques*.

11. Cochez la case **Ne pas exécuter plusieurs tâches d'analyse en même temps** pour optimiser la charge sur l'ordinateur.

12. Enregistrez vos modifications.

Comment configurer la tâche Analyse à la demande dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.

2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez configurer la tâche.

3. Sélectionnez la section **Tâches**.

4. Une fenêtre s'ouvre. Dans cette fenêtre, double-cliquez pour ouvrir les propriétés de la tâche **Analyse à la demande**.

5. Sélectionnez la section **Paramètres de l'application**.

6. Passez à la section **Paramètres**.

7. Cochez ou décochez la case **Utiliser l'analyse heuristique**.

8. Si nécessaire, sélectionnez le niveau d'analyse dans la liste déroulante **Niveau de l'analyse**.

9. Cochez la case **Exécuter uniquement lorsque l'ordinateur est inactif** si vous souhaitez attribuer une priorité *Faible* au processus de travail dans lequel la tâche sera exécutée.

   Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

10. Cochez la case **Considérer la tâche comme une Analyse des zones critiques** si vous souhaitez utiliser la tâche comme une tâche *Analyse des zones critiques*.

11. Cochez la case **Ne pas exécuter plusieurs tâches d'analyse en même temps** pour optimiser la charge sur l'ordinateur.

12. Enregistrez vos modifications.

Comment configurer la tâche Analyse à la demande dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.

2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.

3. Dans le panneau des résultats du nœud sélectionné, cliquez sur **Propriétés**.
4. Sélectionnez l'onglet **Paramètres de la tâche**.
5. Cochez ou décochez la case **Utiliser l'analyse heuristique**.
6. Si nécessaire, modifiez le niveau d'analyse.
7. Cochez la case **Exécuter la tâche en arrière-plan** si vous souhaitez attribuer une priorité *Faible* au processus de travail dans lequel la tâche sera exécutée.

   Par défaut, les processus dans lesquels les tâches de Kaspersky Embedded Systems Security sont exécutées ont la priorité *Moyenne* (Normale).

8. Cochez la case **Considérer la tâche comme une Analyse des zones critiques** si vous souhaitez utiliser la tâche comme une tâche *Analyse des zones critiques*.
9. Cochez la case **Ne pas exécuter plusieurs tâches d'analyse en même temps** pour optimiser la charge sur l'ordinateur.
10. Enregistrez vos modifications.

Configuration de l'analyse des disques amovibles

Configuration de l'Analyse des disques amovibles dans la Console d'administration de Kaspersky Security Center

1. Développez le nœud **Appareils administrés** dans la Console d'administration de Kaspersky Security Center.
2. Sélectionnez le groupe d'administration pour lequel vous souhaitez configurer la tâche.
3. Sélectionnez l'onglet **Stratégies**.
4. Double-cliquez sur le nom de la stratégie que vous souhaitez configurer.

   Dans la fenêtre des propriétés de la stratégie, accédez à la section **Complémentaire**.

5. Cliquez sur **Paramètres** dans la sous-section **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.

6. Exécutez les actions suivantes :

   - Cochez la case **Analyser les disques amovibles lors d'une 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 le disque amovible si sa taille ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité et les paramètres que vous souhaitez pour les tâches d'analyse des disques amovibles.

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

Les paramètres définis seront enregistrés et appliqués.

Configuration de l'analyse des disques amovibles dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Complémentaire**.
5. Cliquez sur **Configurer** sous l'onglet **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.
6. Exécutez les actions suivantes :

   - Cochez la case **Analyser les disques amovibles lors d'une 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 le disque amovible si sa taille ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité et les paramètres que vous souhaitez pour les tâches d'analyse des disques amovibles.
7. Cliquez sur le bouton **OK**.

Les paramètres définis seront enregistrés et appliqués.

Configuration de l'analyse des disques amovibles dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, ouvrez le menu contextuel du nœud **Kaspersky Embedded Systems Security** et sélectionnez **Analyse des disques amovibles**.

   La fenêtre **Analyse des disques amovibles** s'ouvre.
2. Exécutez les actions suivantes :

   - Cochez la case **Analyser les disques amovibles lors d'une 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 le disque amovible si sa taille ne dépasse pas (Mo)** et définissez le seuil maximal dans le champ à droite.
   - Dans la liste déroulante **Analyser avec le niveau de sécurité**, choisissez le niveau de sécurité et les paramètres que vous souhaitez pour les tâches d'analyse des disques amovibles.
3. Cliquez sur **OK**.

Sélection des niveaux de sécurité prédéfinis dans les tâches d'analyse à la demande

Pour un nœud sélectionné dans la liste des ressources de fichiers de l'appareil protégé, vous pouvez appliquer un des niveaux de sécurité prédéfinis suivants : **Performance maximale**, **Recommandé** et **Protection maximale**.

Sélectionner l'un des niveaux de sécurité prédéfinis dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client requis.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Passez à la section **Tâches**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de la tâche **Analyse à la demande**.
6. Sélectionnez la section **Zone d'analyse**.
7. Dans la liste de l'appareil protégé, sélectionnez un élément repris dans la zone d'analyse afin de définir un niveau de sécurité prédéfini.
8. Cliquez sur **Configurer**.
9. Une fenêtre s'ouvre ; dans cette fenêtre, sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité à appliquer.
10. Cliquez sur **OK**.
11. Cliquez sur le bouton **OK** dans la fenêtre **Propriétés : Analyse à la demande**.

Les paramètres configurés de la tâche seront enregistrés et appliqués immédiatement à une tâche en cours. Si la tâche n'est pas exécutée, les modifications des paramètres seront appliquées au prochain lancement de la tâche.

Sélectionner l'un des niveaux de sécurité prédéfinis dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.
3. Dans le panneau des résultats du nœud sélectionné, cliquez sur **Configurer la zone de protection**.
4. Dans la liste des ressources de fichiers réseau de l'appareil protégé, sélectionnez le nœud ou l'élément pour lequel vous souhaitez définir le niveau de sécurité prédéfini.
5. Assurez-vous que le nœud ou l'élément sélectionné se trouve dans la zone d'analyse.
6. Cliquez sur **Configurer**.

7. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez le niveau de sécurité de votre choix.

   La fenêtre reprend la liste des paramètres de sécurité correspondant au niveau de sécurité sélectionné.

8. Cliquez sur **OK**.

Les paramètres de la tâche sont enregistrés et appliqués immédiatement à la tâche en cours. Si la tâche n'est pas exécutée, les paramètres modifiés sont appliqués au prochain lancement de la tâche.

Configuration manuelle des paramètres de sécurité

Par défaut, les tâches d'analyse à la demande appliquent les mêmes paramètres de sécurité à toute la zone d'analyse.

Ces paramètres correspondent au niveau de sécurité prédéfini **Recommandé**.

Vous pouvez modifier les valeurs des paramètres de sécurité par défaut de manière identique pour toute la zone d'analyse ou avec des variations pour différents éléments dans les entrées de l'arborescence ou la liste des ressources de fichiers de l'appareil protégé.

Gestion manuelle des paramètres de sécurité dans la Console d'administration de Kaspersky Security Center

1. Dans le dossier **Appareils administrés** de l'arborescence de la Console d'administration, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client requis.
2. Dans l'espace de travail, sélectionnez l'onglet **Appareils**.
3. Ouvrez les propriétés de l'ordinateur d'un double clic.
4. Passez à la section **Tâches**.
5. Double-cliquez pour ouvrir la fenêtre des propriétés de la tâche **Analyse à la demande**.
6. Sélectionnez la section **Zone d'analyse**.
7. Dans la liste des appareils administrés, sélectionnez un élément inclus dans la zone d'analyse pour gérer les paramètres de sécurité.
8. Cliquez sur **Configurer**.
9. Une fenêtre s'ouvre ; dans cette fenêtre, sous l'onglet **Niveau de sécurité**, sélectionnez le niveau de sécurité à appliquer.
10. Sélectionnez la ressource dont vous souhaitez configurer les paramètres de sécurité.
11. Cliquez sur **Configurer**.
12. Dans la fenêtre qui s'ouvre, sélectionnez le niveau de sécurité requis et cliquez sur **Paramètres**.

13. Sous l'onglet **Général**, spécifiez les paramètres suivants :

- Objets qui doivent être inclus dans 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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
  - **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
  - **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.
- Dans le groupe **Optimisation**, cochez ou décochez la case **Protéger uniquement les nouveaux fichiers et les fichiers modifiés**.
- Dans la section **Analyse des fichiers composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
  - **Analyser les archives**
  - **Analyser les paquets de distribution**
  - **Analyser les fichiers aux formats Microsoft Office**
  - **Analyser les fichiers au format de messagerie**

14. Sous l'onglet **Actions**, spécifiez les paramètres suivants :

- Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
  - **Désinfecter**
  - **Disinfect. Delete if disinfection fails**
  - **Supprimer**
  - **Recommandé**
  - **Informer**
- Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
  a. Cochez ou décochez la case **Appliquer l'action aux types d'objets sélectionnés**.
  b. Cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.
- Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case **Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré**.

15. Sous l'onglet **Optimisation**, spécifiez les paramètres suivants :

    - Dans le bloc **Exclusions** :

        - Cochez ou décochez la case **Exclure les fichiers**.

        - Cochez ou décochez la case **Ne pas détecter les objets par type**.
          Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.

    - Dans le bloc **Paramètres avancés** :

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

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

        - **Utiliser la technologie iSwift**

        - **Utiliser la technologie iChecker**

16. Enregistrez les nouveaux paramètres de sécurité.

Gestion manuelle des paramètres de sécurité dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.

2. Cliquez sur le nom de l'ordinateur sur lequel vous souhaitez configurer la tâche.

3. Sélectionnez la section **Tâches**.

4. Une fenêtre s'ouvre. Dans cette fenêtre, double-cliquez pour ouvrir les propriétés de la tâche **Analyse à la demande**.

5. Sélectionnez la section **Paramètres de l'application**.

6. Passez à la section **Zone d'analyse**.

7. Dans la liste de ressources des fichiers réseau de l'appareil protégé, sélectionnez un élément dont vous souhaitez gérer les paramètres de sécurité. Assurez-vous que l'élément sélectionné se trouve dans la zone d'analyse.

8. Cliquez sur **Modifier**.

9. Sélectionnez un mode de protection des objets dans la liste déroulante :

    - **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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.

- **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.

- **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.

10. Cochez ou décochez la case **Protéger uniquement les nouveaux fichiers et les fichiers modifiés** et indiquez si vous souhaitez inclure les Sous-dossiers dans l'analyse.

11. Gérez les paramètres de protection des objets composés :

    - **Analyser les archives**
    - **Analyser les paquets de distribution**
    - **Analyser les fichiers aux formats Microsoft Office**
    - **Analyser les fichiers au format de messagerie**

12. Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :

    - **Désinfecter**
    - **Disinfect. Delete if disinfection fails**
    - **Supprimer**
    - **Recommandé**
    - **Informer**

13. Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :

    a. Cochez ou décochez la case **Appliquer l'action aux types d'objets sélectionnés**.

    b. Cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.

14. Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case **Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré**.

15. Dans le bloc **Exclusions** :

    - Cochez ou décochez la case **Exclure les fichiers**.
    - Cochez ou décochez la case **Ne pas détecter les objets par type**.

16. Dans le bloc **Ajouter une clé** :

    - **Arrêter l'analyse si elle dure plus de (s.)**
    - **Ne pas analyser les objets composés de plus de (Mo)**

- Utiliser la technologie iSwift
- Utiliser la technologie iChecker

17. Enregistrez les nouveaux paramètres de sécurité.

Gestion manuelle des paramètres de sécurité dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez le nœud enfant qui correspond à la tâche d'analyse à la demande que vous souhaitez configurer.
3. Dans le panneau des résultats du nœud sélectionné, cliquez sur **Configurer la zone de protection**.
4. Dans la liste de ressources des fichiers réseau de l'appareil protégé, sélectionnez un élément dont vous souhaitez gérer les paramètres de sécurité.
5. Assurez-vous que l'élément sélectionné se trouve dans la zone d'analyse.
6. Cliquez sur **Configurer**.
7. Dans la fenêtre qui s'ouvre, sélectionnez le niveau de sécurité requis et cliquez sur **Paramètres**.
8. Sous l'onglet **Général**, spécifiez les paramètres suivants :
   - Objets qui doivent être inclus dans 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. Kaspersky compile la liste des formats. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés par la liste des extensions spécifiées dans les bases antivirus**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. Kaspersky compile la liste des extensions. Elle figure dans les bases de données de Kaspersky Embedded Systems Security.
     - **Objets analysés en fonction de la liste d'extensions indiquée**. Kaspersky Embedded Systems Security analyse uniquement les fichiers infectables sur la base de l'extension du fichier. La liste des extensions est définie manuellement par l'utilisateur.
   - Dans le groupe **Optimisation**, cochez ou décochez la case Protéger uniquement les nouveaux fichiers et les fichiers modifiés.
   - Dans la section **Analyse des fichiers composés**, indiquez les objets composés que vous souhaitez inclure dans la zone d'analyse :
     - Analyser les archives
     - Analyser les paquets de distribution
     - Analyser les fichiers aux formats Microsoft Office
     - Analyser les fichiers au format de messagerie

9. Sous l'onglet **Actions**, spécifiez les paramètres suivants :

   - Sélectionnez l'action à exécuter sur les objets infectés et autres détectés :
     - **Désinfecter**
     - **Disinfect. Delete if disinfection fails**
     - **Supprimer**
     - **Recommandé**
     - **Informer**
   - Configurez les actions à réaliser sur les objets en fonction du type d'objet à détecter :
     a. Cochez ou décochez la case **Appliquer l'action aux types d'objets sélectionnés**.
     b. Cliquez sur **Paramètres** et sélectionnez les types d'objets à détecter.
   - Configurez les actions à exécuter sur les fichiers composés qui ne peuvent pas être modifiés : cochez ou décochez la case **Supprimer entièrement le fichier composé qui ne peut être modifié par l'application en cas de détection d'un objet intégré**.

10. Sous l'onglet **Optimisation**, spécifiez les paramètres suivants :

    - Dans le bloc **Exclusions** :
      - Cochez ou décochez la case **Exclure les fichiers**.
      - Cochez ou décochez la case **Ne pas détecter les objets par type**.

      Cliquez sur le bouton **Modifier** de chaque paramètre pour ajouter des exclusions.
    - Dans le bloc **Paramètres avancés** :
      - **Arrêter l'analyse si elle dure plus de (s.)**
      - **Ne pas analyser les objets composés de plus de (Mo)**
      - **Utiliser la technologie iSwift**
      - **Utiliser la technologie iChecker**

11. Enregistrez les nouveaux paramètres de sécurité.

Statistiques des tâches d'analyse à la demande

Pendant l'exécution de la tâche *Analyse à la demande*, vous pouvez consulter des informations détaillées sur le nombre que Kaspersky Embedded Systems Security a traité depuis son lancement.

Ces informations seront accessibles même si vous arrêtez la tâche. Les statistiques de la tâche figurent dans le journal d'exécution de la tâche.

Pour afficher les statistiques de la tâche Analyse à la demande :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Analyse à la demande**.
2. Sélectionnez la tâche d'analyse à la demande dont vous souhaitez consulter les statistiques.

Le volet résultats du nœud sélectionné reprend les statistiques de la tâche dans la section **Statistiques**.

Les informations relatives aux objets que Kaspersky Embedded Systems Security a traités depuis son lancement sont reprises dans le tableau ci-dessous.

Statistiques des tâches d'analyse à la demande

Champ	Description
Détecté	Nombre d'objets détectés par Kaspersky Embedded Systems Security. Par exemple, si Kaspersky Embedded Systems Security a découvert une objet malveillant dans cinq fichiers, la valeur de ce champ augmentera d'une unité.
Objets infectés et autres objets	Nombre d'objets que Kaspersky Embedded Systems Security a détectés et classés comme infectés ou nombre de fichiers de logiciels légitimes trouvés qui n'ont pas été exclus de la zone d'analyse et qui ont été considérés comme des logiciels légitimes que des intrus peuvent utiliser pour endommager votre appareil ou vos données personnelles.
Objets non désinfectés	Nombre d'objets que Kaspersky Embedded Systems Security n'a pas pu désinfecter pour les raisons suivantes : • L'objet détecté appartient à un type d'objet qui ne peut être désinfecté. • une erreur s'est produite lors de la désinfection.
Objets désinfectés	Nombre d'objets désinfectés par Kaspersky Embedded Systems Security.
Objets supprimés	Nombre d'objets supprimés avec succès par Kaspersky Embedded Systems Security.
Objet non analysé	Nombre d'objets de la zone de protection que Kaspersky Embedded Systems Security n'a pas pu analyser car, par exemple, l'accès à l'objet était bloqué par une autre application.
Archives	Nombre d'archives analysées par Kaspersky Embedded Systems Security.
Objets compactés	Nombre d'objets compactés analysés par Kaspersky Embedded Systems Security.
Objets protégés par un 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 corrompus	Nombre d'objets que Kaspersky Embedded Systems Security a ignorés à cause de leur format endommagé.
Erreurs de traitement	Nombre d'objets dont le traitement a entraîné une erreur de tâche.
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.
L'objet n'a pas été traité	Nombre d'objets qui n'ont pas été 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 des tâches** dans la section **Gestion** du volet résultats.

Nous recommandons le traitement manuel des événements enregistrés sous l'onglet **Événements** du journal d'exécution de la tâche à la fin de la tâche.

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

Cette section contient des informations sur les tâches de mise à jour et sur l'annulation des mises à jour de Kaspersky Embedded Systems Security, ainsi que des instructions de configuration des tâches.

Les fonctionnalités des mise à jour (y compris la fourniture de mises à jour des signatures antivirus et des bases de code) peuvent ne pas être disponibles dans le logiciel aux États-Unis.

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

La mise à jour des bases de données et des modules de l'application Kaspersky Embedded Systems Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres programmes présentant une menace apparaissent dans le monde. Les bases de Kaspersky Embedded Systems Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter les menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

Pour une mise à jour régulière, il faut une licence valide de l'application. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

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

Vous pouvez télécharger les mises à jour sur chaque appareil protégé ou utiliser un appareil protégé comme intermédiaire. Les mises à jour y seront copiées, puis distribuées sur les appareils protégés. Si vous gérez la sécurité des appareils de votre organisation de manière centralisée à l'aide de Kaspersky Security Center, vous pouvez utiliser le Serveur d'administration comme proxy pour le téléchargement des mises à jour.

Si le téléchargement des mises à jour est interrompu ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des dernières mises à jour des bases de données installées. En cas d'endommagement des bases de données de Kaspersky Embedded Systems Security, il est possible de revenir manuellement aux mises à jour antérieures.

Lors de la mise à jour, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Les bases de Kaspersky Embedded Systems Security. La protection de l'ordinateur est garantie par l'utilisation de bases de données qui contiennent les signatures des virus et autres programmes présentant une menace ainsi que les informations sur les moyens de lutter contre elles. Ces informations sont utilisées par les modules de la protection pour rechercher sur votre ordinateur les objets dangereux et les neutraliser. Ces bases sont enrichies régulièrement avec les définitions des menaces qui apparaissent et les moyens de lutter contre celles-ci. Pour cette raison, il est recommandé d'actualiser régulièrement les bases.

  En plus des bases de Kaspersky Embedded Systems Security, la mise à jour concerne également les pilotes réseau qui assurent l'interception du trafic réseau par les modules de la protection.

- Modules de l'application. Les mises à jour des modules de l'application permettent de supprimer les vulnérabilités de Kaspersky Embedded Systems Security, ajoutent de nouvelles fonctionnalités ou améliorent les fonctionnalités existantes.

Pendant la mise à jour, les bases et les modules de l'application installés sur votre ordinateur sont comparés à la dernière version stockée à la source des mises à jour. Si les bases et les modules de l'application actuels diffèrent de la dernière version, la partie manquante sera installée sur l'ordinateur.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Les informations concernant l'état actuel des bases de données de Kaspersky Embedded Systems Security sont affichées dans la fenêtre principale de l'application ou dans l'infobulle que vous voyez lorsque vous passez le curseur sur l'icône de l'application dans la zone de notification.

Les informations sur les résultats de la mise à jour et sur tous les événements qui se produisent pendant l'exécution de la tâche de mise à jour sont enregistrées dans le journal des tâches de mise à jour.

À propos des tâches de mise à jour

Kaspersky Embedded Systems Security comporte deux tâches de mise à jour : *Mise à jour* et *Annulation de la mise à jour*.

Mise à jour

Par défaut, Kaspersky Embedded Systems Security copie les bases et, le cas échéant, les modules de l'application depuis la source des mises à jour sur l'appareil protégé et les utilise directement dans les modules de protection. Les tâches Analyse à la demande utiliseront les bases de l'application mises à jour à leur prochaine exécution.

Vous pouvez configurer les paramètres la tâche *Mise à jour*. 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.

Par défaut, la tâche *Mise à jour* est configurée en mode **Manuellement**. Vous ne pouvez pas suspendre et reprendre une tâche de mise à jour.

Annulation de la mise à jour

La tâche amène Kaspersky Embedded Systems Security à rétablir les bases de données et les modules de l'application précédents.

La tâche *Annulation de la mise à jour* est désactivée par défaut.

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

Le choix de la source des mises à jour dans la tâche *Mise à jour* dépend du schéma de mise à jour des bases de données et des modules logiciels utilisés dans l'organisation.

Vous pouvez mettre à jour les bases et les modules de Kaspersky Embedded Systems Security sur les appareils protégés selon les schémas suivants :

- Télécharger les mises à jour directement depuis Internet sur chaque appareil protégé (schéma 1).
- Télécharger les mises à jour depuis Internet sur un appareil intermédiaire et les diffuser sur les appareils protégés au départ de cet appareil.

  Tout appareil sur lequel les applications suivantes sont installées peut servir d'intermédiaire :

  - Kaspersky Embedded Systems Security (schéma 2).
  - Serveur d'administration de Kaspersky Security Center (schéma 3).

  > La mise à jour via un appareil intermédiaire non seulement réduit le trafic Internet, mais offre également une sécurité supplémentaire à l'appareil protégé réseau.

- Télécharger les mises à jour des bases de données sur chaque appareil protégé via un disque amovible sécurisé (schéma 4).

Les schémas de mise à jour sont décrits ci-après.

Schéma 1. Mises à jour des bases de données et des modules directement via Internet

Pour configurer les mises à jour de Kaspersky Embedded Systems Security directement via Internet :

dans les paramètres des tâches *Mise à jour*, désignez les ordinateurs de mise à jour de Kaspersky en tant que sources des mises à jour.

En guise de source des mises à jour, vous pouvez indiquer d'autres serveurs HTTPS ou HTTP qui contiennent un dossier de mise à jour.

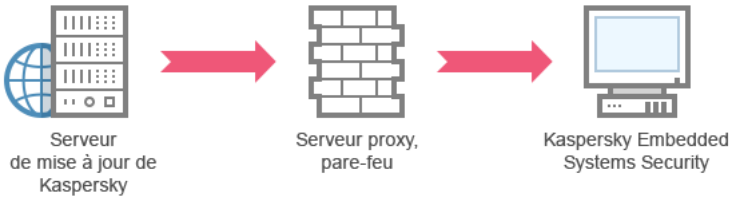


Schéma 1 : Mise à jour des bases de données et des modules directement à partir d'Internet

Schéma 2. Mise à jour des bases de données et des modules via un des appareils protégés

Pour configurer la réception des mises à jour de Kaspersky Embedded Systems Security via l'un des appareils protégés :

1. Copiez les mises à jour sur l'appareil protégé sélectionné.
   - Sur l'appareil protégé sélectionné, configurez les paramètres de la tâche *Mise à jour* :
     a. En guise de source des mises à jour, sélectionnez le serveur de mise à jour de Kaspersky.
     b. Désignez le dossier partagé en guise de dossier d'enregistrement des mises à jour.
2. Diffusez les mises à jour sur les autres appareils protégés :
   - Configurez la tâche *Mise à jour* sur chacun des appareils protégés.
     En guise de source des mises à jour, saisissez le répertoire de l'appareil intermédiaire dans lequel vous avez copié les mises à jour.

Kaspersky Embedded Systems Security récupérera les mises à jour via un des appareils protégés.

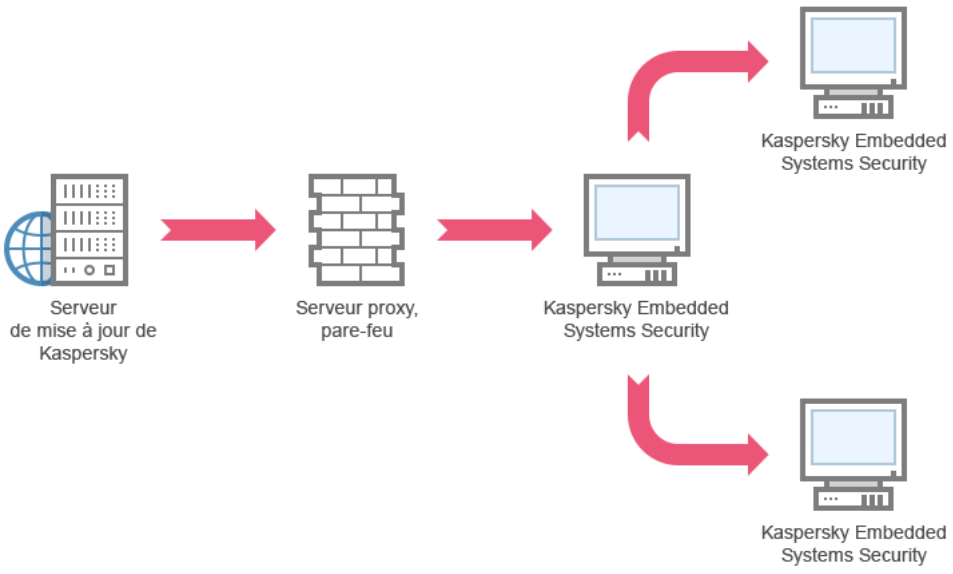


Schéma 2 : Mise à jour des bases et des modules via l'un des appareils protégés

Schéma 3. Mise à jour des bases de données et des modules via le Serveur d'administration de Kaspersky Security Center

Si vous utilisez Kaspersky Security Center pour gérer la protection antivirus des appareils de manière centralisée, vous pouvez télécharger les mises à jour via le Serveur d'administration de Kaspersky Security Center installé sur votre réseau local.

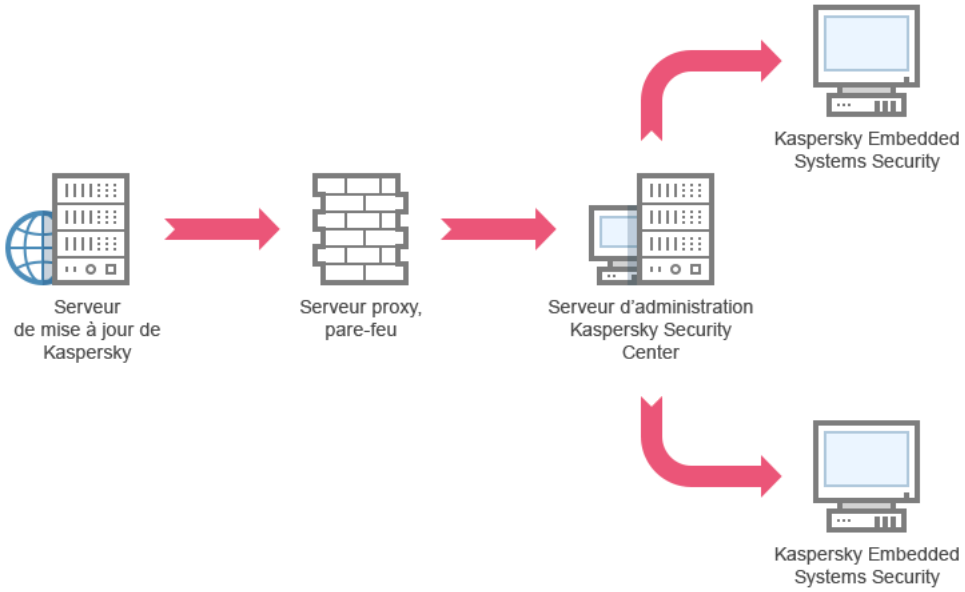


Schéma 3 : Mise à jour des bases et des modules via le Serveur d'administration Kaspersky Security Center

Pour configurer la réception des mises à jour de Kaspersky Embedded Systems Security via le Serveur d'administration de Kaspersky Security Center :

1. Installez l'Agent d'administration sur chacun des appareils protégés. L'Agent d'administration est un module logiciel inclus dans le kit de distribution de Kaspersky Security Center. Il assure l'interaction entre le Serveur d'administration et Kaspersky Embedded Systems Security sur l'appareil protégé. Pour obtenir de plus amples informations sur l'Agent d'administration et sa configuration à l'aide de l'application Kaspersky Security Center, consultez l'*aide de Kaspersky Security Center.*

2. Téléchargement des mises à jour depuis le serveur de mise à jour de Kaspersky vers le Serveur d'administration de Kaspersky Security Center.

   - Configurez la tâche *Téléchargement des mises à jour sur le stockage du Serveur d'administration* pour l'ensemble d'appareils protégé indiqué.

     En guise de source des mises à jour, sélectionnez le serveur de mise à jour de Kaspersky.

3. Diffusez les mises à jour sur les appareils protégés. Pour ce faire, réalisez une des opérations suivantes :

   - Sur Kaspersky Security Center, configurez une tâche de groupe de mise à jour des bases antivirus (des modules de l'application) afin de diffuser les mises à jour aux appareils protégés :
   - Configurez la tâche *Mise à jour* sur chacun des appareils protégés.

     a. En guise de source des mises à jour, désignez le Serveur d'administration de Kaspersky Security Center.

     b. Le cas échéant, planifiez l'exécution de la tâche.

Kaspersky Embedded Systems Security récupérera les mises à jour via le Serveur d'administration de Kaspersky Security Center.

Schéma 4. Mise à jour des bases de l'application à partir d'un disque amovible sécurisé

Pour mettre à jour les bases de données de Kaspersky Embedded Systems Security à l'aide d'un disque amovible sécurisé, procédez comme suit :

1. Connectez le disque amovible sécurisé à l'appareil sur lequel Kaspersky Embedded Systems Security est installé et qui a accès aux mises à jour des bases de données de l'application.
2. Ajoutez une règle d'autorisation du module Contrôle des appareils pour le disque amovible connecté.
3. Dans la Console de l'application, configurez et exécutez la tâche *Copie sécurisée des bases de données de l'application*.
4. Connectez le disque amovible sécurisé contenant les mises à jour des bases de données à l'appareil sur lequel vous devez mettre à jour les bases de données de l'application.
5. Dans la Console de l'application, configurez et exécutez la tâche *Mise à jour sécurisée des bases de données des applications*.

Kaspersky Embedded Systems Security recevra les bases de données de l'application mises à jour à partir du disque amovible sécurisé.

Configuration des tâches de mise à jour

Comment configurer la tâche Mise à jour dans la Console d'administration de Kaspersky Security Center

1. Dans la Console d'administration de Kaspersky Security Center, accédez à la tâche de mise à jour locale ou de groupe que vous souhaitez configurer.
2. Ouvrez la section **Paramètres**.
3. Sous **Paramètres de la mise à jour en mode local** pour Kaspersky Embedded Systems Security connecté au Serveur d'administration de Kaspersky Security Center, configurez les sources des mises à jour :

   a. Cliquez sur **Paramètres**.

   La fenêtre **Mise à jour des bases et des modules de l'application** s'ouvre.

b. Cochez la case en regard des sources de mise à jour que vous souhaitez utiliser :

- Serveur d'administration de Kaspersky Security Center
- Serveurs de mises à jour de Kaspersky

Si nécessaire, cliquez sur le bouton **Ajouter** pour ajouter une source des mises à jour personnalisée.

c. Si vous sélectionnez plusieurs sources des mises à jour, utilisez les boutons **Haut** et **Bas** pour trier les sources des mises à jour par ordre de priorité. Kaspersky Embedded Systems Security accède aux sources des mises à jour strictement dans l'ordre configuré et exécute la tâche de mise à jour à l'aide du paquet de la première source des mises à jour disponible.

Par défaut, Kaspersky Embedded Systems Security utilise le serveur Kaspersky Security Center comme première source de mise à jour. Il est ainsi possible de réduire le trafic lors des mises à jour. Si aucune stratégie n'est appliquée à l'ordinateur, les serveurs Kaspersky sont sélectionnés comme première source de mise à jour dans les paramètres de la tâche locale *Mise à jour*, car l'application peut ne pas avoir accès à Kaspersky Security Center.

d. Si vous avez sélectionné **Serveurs de mises à jour de Kaspersky** comme source des mises à jour, sélectionnez le principe que Kaspersky Embedded Systems Security doit observer lors de la sélection d'un serveur de mises à jour de Kaspersky :

- **Détecter automatiquement**. L'application utilise le serveur de mises à jour de Kaspersky disponible le plus proche.
- **Sélectionner dans la liste**. L'application utilise le serveur de mises à jour de Kaspersky dans le pays sélectionné dans la liste.

e. Cliquez sur le bouton **OK** dans le groupe **Mise à jour des bases et des modules d'application**.

4. Configurer les mises à jour de la base de données de l'application :

a. Cochez ou décochez la case **Télécharger les mises à jour des bases de l'application**.

b. 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 au placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive. Par défaut, la case est décochée.

c. Si vous avez coché la case **Réduire la charge sur les I/O du disque**, dans le champ **RAM utilisée pour l'optimisation, Mo**, spécifiez la quantité de mémoire vive en mégaoctets. 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 640 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

Lors de l'exécution de la tâche *Mise à jour* avec la fonctionnalité d'optimisation du sous-système de disque activée, l'un des événements suivants peut se produire :

- Si la valeur est trop petite, la quantité de RAM allouée peut être insuffisante pour terminer la tâche de mise à jour des bases de l'application (par exemple, lors de la première mise à jour), ce qui entraînera la fin de la tâche avec une erreur.

  Dans ce cas, il est recommandé d'allouer plus de RAM pour la fonction d'optimisation du sous-système de disque.

- Si la valeur est trop grande, au démarrage de la tâche de mise à jour des bases de l'application, il peut être impossible de créer un lecteur virtuel d'une taille sélectionnée en mémoire vive. Par conséquent, la fonctionnalité d'optimisation du sous-système de disque est automatiquement désactivée et la tâche de mise à jour des bases de l'application est exécutée sans la fonctionnalité d'optimisation.

  Dans ce cas, il est recommandé d'allouer moins de RAM pour la fonction d'optimisation du sous-système de disque.

5. Configurez les mises à jour des modules logiciels de l'application :

   a. Cochez ou décochez la case **Télécharger les mises à jour des modules de l'application**.

   Si la case est cochée, Kaspersky Embedded Systems Security signale à l'utilisateur l'existence de mises à jour disponibles pour les modules de l'application et, pendant l'exécution de la tâche *Mise à jour*, il inclut les mises à jour des modules de l'application dans le paquet de mises à jour. Le type des mises à jour des modules d'application qui seront appliquées est configuré séparément. Cette case est cochée par défaut.

   b. Sélectionnez les types de mises à jour du module d'application que vous souhaitez appliquer.

   - **Installer les mises à jour critiques et approuvées**. Si cette option est sélectionnée et que des mises à jour des modules de l'application sont disponibles, Kaspersky Embedded Systems Security installe les mises à jour critiques automatiquement tandis qu'il installera les autres mises à jour uniquement après approbation de leur installation locale via l'interface de l'application ou le Kaspersky Security Center.

   - **Installer uniquement les mises à jour approuvées**. Si cette option est sélectionnée et que des mises à jour des modules sont disponibles, Kaspersky Embedded Systems Security les installe après approbation de leur application, localement via l'interface de l'application ou depuis le Kaspersky Security Center. Cette option est sélectionnée par défaut.

   Si la mise à jour des modules de l'application implique la lecture et l'acceptation de dispositions du Contrat de licence utilisateur final, l'application installera ces mises à jour après l'acceptation de ces dispositions.

6. Configurez la copie des mises à jour dans un dossier pour le stockage local :

   a. Cochez ou décochez la case **Copier les mises à jour dans un dossier pour le stockage local**

   b. Sélectionnez le contenu des mises à jour que l'application doit copier dans le dossier de stockage local :

   - **Copier les mises à jour des bases de l'application**. L'application télécharge uniquement les mises à jour des bases de données.

   - **Copier les mises à jour critiques des modules de l'application**. L'application télécharge uniquement les mises à jour critiques des modules de l'application.

   - **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application**. L'application télécharge les mises à jour des bases de données et les mises à jour critiques des modules d'application.

   c. Indiquez le répertoire local ou de réseau dans lequel Kaspersky Embedded Systems Security copiera les mises à jour reçues.

7. Enregistrez vos modifications.

Comment configurer la tâche Mise à jour dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, ouvrez le nœud **Mise à jour → Mise à jour des bases et des modules d'application**.

2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Propriétés : Mise à jour des bases et des modules d'application** s'ouvre.

3. Sous **Paramètres de la mise à jour en mode local** pour Kaspersky Embedded Systems Security connecté au Serveur d'administration de Kaspersky Security Center, configurez les sources des mises à jour :

   a. Cliquez sur **Paramètres**.

      La fenêtre **Mise à jour des bases et des modules de l'application** s'ouvre.

   b. Cochez la case en regard des sources de mise à jour que vous souhaitez utiliser :

      - Serveur d'administration de Kaspersky Security Center
      - Serveurs de mises à jour de Kaspersky

      Si nécessaire, cliquez sur le bouton **Ajouter** pour ajouter une source des mises à jour personnalisée.

   c. Si vous sélectionnez plusieurs sources des mises à jour, utilisez les boutons **Haut** et **Bas** pour trier les sources des mises à jour par ordre de priorité. Kaspersky Embedded Systems Security accède aux sources des mises à jour strictement dans l'ordre configuré et exécute la tâche de mise à jour à l'aide du paquet de la première source des mises à jour disponible.

      Par défaut, Kaspersky Embedded Systems Security utilise le serveur Kaspersky Security Center comme première source de mise à jour. Il est ainsi possible de réduire le trafic lors des mises à jour. Si aucune stratégie n'est appliquée à l'ordinateur, les serveurs Kaspersky sont sélectionnés comme première source de mise à jour dans les paramètres de la tâche locale *Mise à jour*, car l'application peut ne pas avoir accès à Kaspersky Security Center.

   d. Si vous avez sélectionné **Serveurs de mises à jour de Kaspersky** comme source des mises à jour, sélectionnez le principe que Kaspersky Embedded Systems Security doit observer lors de la sélection d'un serveur de mises à jour de Kaspersky :

      - **Détecter automatiquement**. L'application utilise le serveur de mises à jour de Kaspersky disponible le plus proche.
      - **Sélectionner dans la liste**. L'application utilise le serveur de mises à jour de Kaspersky dans le pays sélectionné dans la liste.

   e. Cliquez sur le bouton **OK** dans le groupe **Mise à jour des bases et des modules d'application**.

4. Configurer les mises à jour de la base de données de l'application :

   a. Cochez ou décochez la case **Télécharger les mises à jour des bases de l'application**.

   b. 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 au placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive. Par défaut, la case est décochée.

c. Si vous avez coché la case **Réduire la charge sur les I/O du disque**, dans le champ **RAM utilisée pour l'optimisation, Mo**, spécifiez la quantité de mémoire vive en mégaoctets. 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 640 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

Lors de l'exécution de la tâche *Mise à jour* avec la fonctionnalité d'optimisation du sous-système de disque activée, l'un des événements suivants peut se produire :

- Si la valeur est trop petite, la quantité de RAM allouée peut être insuffisante pour terminer la tâche de mise à jour des bases de l'application (par exemple, lors de la première mise à jour), ce qui entraînera la fin de la tâche avec une erreur.

  Dans ce cas, il est recommandé d'allouer plus de RAM pour la fonction d'optimisation du sous-système de disque.

- Si la valeur est trop grande, au démarrage de la tâche de mise à jour des bases de l'application, il peut être impossible de créer un lecteur virtuel d'une taille sélectionnée en mémoire vive. Par conséquent, la fonctionnalité d'optimisation du sous-système de disque est automatiquement désactivée et la tâche de mise à jour des bases de l'application est exécutée sans la fonctionnalité d'optimisation.

  Dans ce cas, il est recommandé d'allouer moins de RAM pour la fonction d'optimisation du sous-système de disque.

5. Configurez les mises à jour des modules logiciels de l'application :

a. Cochez ou décochez la case **Télécharger les mises à jour des modules de l'application**.

Si la case est cochée, Kaspersky Embedded Systems Security signale à l'utilisateur l'existence de mises à jour disponibles pour les modules de l'application et, pendant l'exécution de la tâche *Mise à jour*, il inclut les mises à jour des modules de l'application dans le paquet de mises à jour. Le type des mises à jour des modules d'application qui seront appliquées est configuré séparément. Cette case est cochée par défaut.

b. Sélectionnez les types de mises à jour du module d'application que vous souhaitez appliquer.

- **Installer les mises à jour critiques et approuvées**. Si cette option est sélectionnée et que des mises à jour des modules de l'application sont disponibles, Kaspersky Embedded Systems Security installe les mises à jour critiques automatiquement tandis qu'il installera les autres mises à jour uniquement après approbation de leur installation locale via l'interface de l'application ou le Kaspersky Security Center.

- **Installer uniquement les mises à jour approuvées**. Si cette option est sélectionnée et que des mises à jour des modules sont disponibles, Kaspersky Embedded Systems Security les installe après approbation de leur application, localement via l'interface de l'application ou depuis le Kaspersky Security Center. Cette option est sélectionnée par défaut.

Si la mise à jour des modules de l'application implique la lecture et l'acceptation de dispositions du Contrat de licence utilisateur final, l'application installera ces mises à jour après l'acceptation de ces dispositions.

6. Configurez la copie des mises à jour dans un dossier pour le stockage local :

   a. Cochez ou décochez la case **Copier les mises à jour dans un dossier pour le stockage local**.

   b. Sélectionnez le contenu des mises à jour que l'application doit copier dans le dossier de stockage local :

   - **Copier les mises à jour des bases de l'application**. L'application télécharge uniquement les mises à jour des bases de données.
   - **Copier les mises à jour critiques des modules de l'application**. L'application télécharge uniquement les mises à jour critiques des modules de l'application.
   - **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application**. L'application télécharge les mises à jour des bases de données et les mises à jour critiques des modules d'application.

   c. Indiquez le répertoire local ou de réseau dans lequel Kaspersky Embedded Systems Security copiera les mises à jour reçues.

7. Enregistrez vos modifications.

Comment configurer la tâche Mise à jour dans Kaspersky Security Center Web Console

1. Dans Web Console, accédez à la tâche *Mise à jour* locale ou de groupe que vous souhaitez configurer.
2. Ouvrez la section **Paramètres**.
3. Sélectionnez l'onglet **Mode local** pour configurer la tâche *Mise à jour* de Kaspersky Embedded Systems Security connecté au Serveur d'administration de Kaspersky Security Center.
4. Configurez les sources des mises à jour :

   a. Sous **Sources des mises à jour**, cochez la case en regard des sources des mises à jour que vous souhaitez utiliser :

   - **Serveur d'administration de Kaspersky Security Center**
   - **Serveurs de mises à jour de Kaspersky**

   Si nécessaire, cliquez sur le bouton **Ajouter** pour ajouter une source des mises à jour personnalisée.

   b. Si vous sélectionnez plusieurs sources des mises à jour, utilisez les boutons **Haut** et **Bas** pour trier les sources des mises à jour par ordre de priorité. Kaspersky Embedded Systems Security accède aux sources des mises à jour strictement dans l'ordre configuré et exécute la tâche de mise à jour à l'aide du paquet de la première source des mises à jour disponible.

   Par défaut, Kaspersky Embedded Systems Security utilise le serveur Kaspersky Security Center comme première source de mise à jour. Il est ainsi possible de réduire le trafic lors des mises à jour. Si aucune stratégie n'est appliquée à l'ordinateur, les serveurs Kaspersky sont sélectionnés comme première source de mise à jour dans les paramètres de la tâche locale *Mise à jour*, car l'application peut ne pas avoir accès à Kaspersky Security Center.

5. Configurer les mises à jour de la base de données de l'application :

   a. Cochez ou décochez la case **Télécharger les mises à jour des bases de l'application**.

   b. 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 au placement des fichiers de mise à jour sur un disque virtuel dans la mémoire vive. Par défaut, la case est décochée.

   c. Si vous avez coché la case **Réduire la charge sur les I/O du disque**, dans le champ **RAM utilisée pour l'optimisation, Mo**, spécifiez la quantité de mémoire vive en mégaoctets. 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 640 Mo. Le volume minimal de mémoire vive par défaut est de 400 Mo.

      Lors de l'exécution de la tâche *Mise à jour* avec la fonctionnalité d'optimisation du sous-système de disque activée, l'un des événements suivants peut se produire :

      - Si la valeur est trop petite, la quantité de RAM allouée peut être insuffisante pour terminer la tâche (par exemple, lors de la première mise à jour), ce qui entraînera la fin de la tâche avec une erreur.

        Dans ce cas, il est recommandé d'allouer plus de RAM pour la fonction d'optimisation du sous-système de disque.

      - Si la valeur est trop grande, au démarrage de la tâche, il peut être impossible de créer un lecteur virtuel d'une taille sélectionnée en mémoire vive. Par conséquent, la fonctionnalité d'optimisation du sous-système de disque est automatiquement désactivée et la tâche de mise à jour des bases de l'application est exécutée sans la fonctionnalité d'optimisation.

        Dans ce cas, il est recommandé d'allouer moins de RAM pour la fonction d'optimisation du sous-système de disque.

6. Configurez les mises à jour des modules logiciels de l'application :

   a. Cochez ou décochez la case **Télécharger les mises à jour des modules de l'application**.

      Si la case est cochée, Kaspersky Embedded Systems Security signale à l'utilisateur l'existence de mises à jour disponibles pour les modules de l'application et, pendant l'exécution de la tâche *Mise à jour*, il inclut les mises à jour des modules de l'application dans le paquet de mises à jour. Le type des mises à jour des modules d'application qui seront appliquées est configuré séparément. Cette case est cochée par défaut.

   b. Sélectionnez les types de mises à jour du module d'application que vous souhaitez appliquer.

      - **Installer les mises à jour critiques et approuvées**. Si cette option est sélectionnée et que des mises à jour des modules de l'application sont disponibles, Kaspersky Embedded Systems Security installe les mises à jour critiques automatiquement tandis qu'il installera les autres mises à jour uniquement après approbation de leur installation locale via l'interface de l'application ou le Kaspersky Security Center.

      - **Installer uniquement les mises à jour approuvées**. Si cette option est sélectionnée et que des mises à jour des modules sont disponibles, Kaspersky Embedded Systems Security les installe après approbation de leur application, localement via l'interface de l'application ou depuis le Kaspersky Security Center. Cette option est sélectionnée par défaut.

      Si la mise à jour des modules de l'application implique la lecture et l'acceptation de dispositions du Contrat de licence utilisateur final, l'application installera ces mises à jour après l'acceptation de ces dispositions.

7. Configurez la copie des mises à jour dans un dossier pour le stockage local :

   a. Cochez ou décochez la case **Copier les mises à jour dans le dossier**.

   b. Sélectionnez le contenu des mises à jour que l'application doit copier dans le dossier de stockage local :

   - **Copier les mises à jour des bases de l'application**. L'application télécharge uniquement les mises à jour des bases de données.
   - **Copier les mises à jour critiques des modules de l'application**. L'application télécharge uniquement les mises à jour critiques des modules de l'application.
   - **Copier les mises à jour des bases et les mises à jour critiques des modules de l'application**. L'application télécharge les mises à jour des bases de données et les mises à jour critiques des modules d'application.

   c. Indiquez le répertoire local ou de réseau dans lequel Kaspersky Embedded Systems Security copiera les mises à jour reçues.

8. Enregistrez vos modifications.

Mise à jour SMU de l'application

Pour mettre à jour l'application à l'aide du service de mise à jour de Kaspersky (Seamless Update ; SMU), il n'est pas nécessaire de lancer le programme d'installation, contrairement aux autres méthodes de mise à jour. Kaspersky Embedded Systems Security obtient la nouvelle version de l'application avec les bases antivirus provenant de la même source.

Une mise à jour SMU permet de mettre à jour l'application sur tous les ordinateurs de votre organisation vers la version la plus récente. Avant d'appliquer une mise à jour SMU, nous recommandons de tester la nouvelle version de l'application sur quelques ordinateurs. Pour ce faire, il faut mettre à jour manuellement l'application sur ces ordinateurs (par exemple, localement à l'aide de l'Assistant d'installation). Vous ne pouvez pas sélectionner des ordinateurs individuellement lorsque vous effectuez une mise à jour SMU.

La planification des mises à jour de l'application est déterminée par l'équipe de Kaspersky. Pour s'assurer du bon fonctionnement de la nouvelle version de l'application, Kaspersky diffuse des mises à jour disponibles étape par étape. Cela signifie que votre mise à jour SMU pourrait être disponible jusqu'à deux mois après la publication d'une nouvelle version.

Vous pouvez gérer la mise à jour SMU de l'application à l'aide de la tâche *Mise à jour*. Pour que la nouvelle version de l'application soit incluse dans le même paquet que les bases antivirus, vous devez autoriser la mise à jour des *modules d'application* dans les paramètres de la tâche *Mise à jour*.

Étapes d'une mise à jour SMU de l'application

1. **Après la publication d'une nouvelle version de l'application ou la mise à jour d'un module, Kaspersky diffuse la mise à jour.**

2. **L'utilisateur approuve la mise à jour de l'application.**

   Si l'ordinateur est connecté à Kaspersky Security Center, la mise à jour est mise à disposition dans Kaspersky Security Center, dans la section **Mises à jour pour les bases de données de Kaspersky et modules logiciels**. Pour plus de détails sur l'approbation des mises à jour, consultez l'aide de Kaspersky Security Center.

   Si l'ordinateur n'est pas connecté à Kaspersky Security Center, la mise à jour est disponible dans la Console de l'application. Pour approuver la mise à jour, accédez à la section **Mise à jour → Mise à jour de l'application**, sélectionnez une version de l'application et, si nécessaire, acceptez les conditions générales des contrats.

3. **Kaspersky Embedded Systems Security exécute la tâche Mise à jour selon une planification.**

Kaspersky Embedded Systems Security met alors l'application à jour en mode « silencieux ».

Copie sécurisée des bases de données de l'application

La tâche peut être configurée uniquement dans la Console de l'application. Cette tâche ne peut pas être configurée dans la Console d'administration de Kaspersky Security Center ou dans Kaspersky Security Center Web Console.

Pour configurer et lancer la tâche Copie sécurisée des bases de l'application, procédez comme suit :

1. Dans l'arborescence de la console de l'application, dans le menu contextuel du nœud **Mise à jour**, sélectionnez **Démarrer la copie sécurisée des bases de données...**.

   La fenêtre de bienvenue de l'Assistant de copie sécurisée des bases de l'application s'ouvre.

2. Cliquez sur **Suivant >**.

3. Sous **Source des mises à jour**, sélectionnez une source des mises à jour :

   - **Serveur d'administration de Kaspersky Security Center**.

     Cette option n'est disponible que si les applications de Kaspersky de votre réseau sont gérées à partir du système d'accès à distance de Kaspersky Security Center et si l'Agent d'administration (module de Kaspersky Security Center qui fournit la connexion entre les appareils protégés et le serveur d'administration) est installé sur l'appareil protégé.

     Cette option est sélectionnée par défaut.

   - **Serveurs de mises à jour de Kaspersky**.

     Serveurs HTTP et HTTPS de Kaspersky à partir desquels les applications de Kaspersky reçoivent les mises à jour de leurs bases de données et de leurs modules.

   - **Serveurs HTTP ou FTP personnalisés, ou dossiers réseau**.

4. Si, à l'étape précédente, vous avez sélectionné **Serveur d'administration de Kaspersky Security Center**, configurez la fonctionnalité **Utiliser les serveurs de mise à jour de Kaspersky si les serveurs spécifiés ne sont pas disponibles**. Si cette option est activée, Kaspersky Embedded Systems Security utilisera les serveurs de mises à jour de Kaspersky comme source de mises à jour si le Serveur d'administration de Kaspersky Security Center n'est pas disponible.

5. Sous **Paramètres de connexion à la source des mises à jour**, configurez l'utilisation d'un serveur proxy pour la connexion aux sources de mise à jour.

6. Cliquez sur **Suivant >**.

7. Dans la liste déroulante, sélectionnez le disque amovible Rutoken sécurisé connecté sur lequel vous souhaitez enregistrer les bases antivirus de l'application.

   Seul un disque amovible Rutoken spécifiquement autorisé par une règle du module Contrôle des appareils peut être utilisé comme disque amovible sécurisé.

8. Sous **Paramètres de sécurité**, dans le champ **Saisissez le code PIN d'administrateur actuel**, saisissez le code PIN d'administrateur défini sur le disque amovible Rutoken afin de protéger son contenu contre toute lecture, copie ou écriture par d'éventuels intrus.

9. Pour modifier le code PIN d'administrateur actuel, procédez comme suit :

   a. Cochez la case **Modifier le code PIN d'administrateur actuel (seuls les chiffres et les caractères latins sont autorisés)**.

   b. Saisissez le nouveau code PIN.

   c. Confirmez le nouveau code PIN.

10. Définissez un code PIN utilisateur. Ce code PIN sera demandé à l'employé qui mettra à jour les bases de données de l'application à l'aide de la tâche *Mise à jour sécurisée des bases de données des applications* et du disque amovible Rutoken sélectionné :

    a. Saisissez le code PIN utilisateur.

    b. Confirmez le code PIN utilisateur.

11. Cliquez sur **Suivant >**.

La copie sécurisée des bases de l'application sur le disque amovible Rutoken est lancée. Les paramètres sont enregistrés et appliqués pendant l'exécution de la tâche.

Mise à jour sécurisée des bases de données de l'application

La tâche *Mise à jour sécurisée des bases de données des applications* est nécessaire pour mettre à jour les bases de données de l'application à l'aide d'un disque amovible sécurisé et protégé contre la lecture, la copie et l'écriture par des individus malveillants potentiels, sur un réseau d'entreprise fermé et sur les appareils qui n'ont pas accès aux bases de données de l'application.

Cette tâche peut uniquement être lancée via la Console de l'application installée sur le même appareil que Kaspersky Embedded Systems Security. Il est impossible de configurer la tâche dans la Console d'administration ou dans Web Console.

Pour lancer la tâche Mise à jour sécurisée des bases de données des applications, procédez comme suit :

1. Dans l'arborescence de la console de l'application, dans le menu contextuel du nœud **Mise à jour**, sélectionnez **Démarrer la mise à jour sécurisée des bases de données...**.

   La fenêtre de bienvenue de l'Assistant de mise à jour sécurisée des bases de l'application s'ouvre. Appuyez sur le bouton **Suivant >**.

2. Dans la liste déroulante, sélectionnez le disque amovible sécurisé connecté contenant les bases antivirus de l'application.

   Seul un disque amovible Rutoken spécifiquement autorisé par une règle du module Contrôle des appareils peut être utilisé comme disque amovible sécurisé.

3. Saisissez le code PIN du disque amovible Rutoken défini lors de l'étape de copie des bases de données de l'application.

4. Cliquez sur **Terminer**.

   La tâche de mise à jour sécurisée des bases de l'application démarre. Les bases de données de l'application seront copiées à partir du disque amovible Rutoken.

Annulation des mises à jour des bases de l'application Kaspersky Embedded Systems Security

Avant d'exécuter la mise à jour des bases de données, Kaspersky Embedded Systems Security crée une copie de sauvegarde des bases utilisées antérieurement. Si la mise à jour est interrompue ou se solde par un échec, Kaspersky Embedded Systems Security reviendra automatiquement à l'utilisation des bases de données installées antérieurement.

Si vous rencontrez des problèmes après la mise à jour des bases de données, vous pouvez revenir à l'état antérieur des bases grâce à la tâche *Annulation de la dernière mise à jour*.

Pour lancer la tâche Annulation de la dernière mise à jour, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, ouvrez la section **Mise à jour** → **Annulation de la dernière mise à jour**.

2. Dans le panneau des résultats, cliquez sur le lien **Lancer**.

Statistiques sur les tâches de mise à jour

Pendant l'exécution de la tâche Mise à jour, les informations en temps réel sur le volume de données téléchargé depuis le lancement de la tâche ainsi que d'autres statistiques liées à l'exécution de la tâche, s'affichent.

Ces informations sont disponibles dans le journal d'exécution de la tâche quand la tâche est terminée ou arrêtée.

Pour afficher les statistiques de la tâche Mise à jour :

Dans l'arborescence de la Console de l'application, ouvrez la section **Mise à jour** → **Mise à jour des bases et des modules d'application**.

Dans le panneau des résultats, sous **Statistiques**, vous trouverez des informations sur la quantité totale de données obtenues.

Sauvegarde des objets

Cette section fournit des informations sur la sauvegarde des objets malveillants détectés avant leur désinfection ou leur suppression.

Sauvegarde des objets. Sauvegarde

Kaspersky Embedded Systems Security enregistre des copies chiffrées des objets réparés ou supprimés dans le dossier Sauvegarde.

Si l'objet fait partie d'un objet composé (par exemple, d'une archive), Kaspersky Embedded Systems Security enregistre cet objet composé complet dans la Sauvegarde. Par exemple, si Kaspersky Embedded Systems Security considère un des objets de la base de messagerie comme étant infecté, il place l'ensemble de la base de messagerie dans la sauvegarde.

Si la taille de l'objet que Kaspersky Embedded Systems Security copie dans la sauvegarde est importante, le système peut ralentir et l'espace disponible sur le disque dur peut diminuer.

Vous pouvez restaurer les fichiers du dossier de sauvegarde dans le répertoire d'origine ou dans un autre répertoire sur l'appareil protégé. Il est possible de restaurer un fichier depuis la sauvegarde, par exemple si un fichier infecté contient des informations importantes et que Kaspersky Embedded Systems Security ne parvient pas à le désinfecter sans endommager son intégrité et perdre les informations.

La restauration de fichiers à partir de la sauvegarde peut provoquer une infection de l'appareil protégé.

Consultation des objets dans la sauvegarde

Cette section explique comment consulter la liste des fichiers dans la Sauvegarde.

Comment consulter les objets de la Sauvegarde dans la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Avancé** → **Stockages**.
3. Accédez au dossier **Sauvegarde**.
4. Les informations sur les objets placés dans la Sauvegarde sont affichées dans le volet droit de la console.

Comment consulter les objets de la Sauvegarde dans Kaspersky Security Center Web Console

1. Ouvrez Web Console.
2. Dans l'arborescence de la console, sélectionnez **Opérations** → **Stockages**.

3. Accédez au dossier **Sauvegarde**.

4. Les informations sur les objets placés dans la Sauvegarde sont affichées dans le volet droit de la console.

Comment consulter les objets de la Sauvegarde dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Stockages** → **Sauvegarde**.

2. Les informations sur les objets placés dans la Sauvegarde sont affichées dans le volet droit de la console.

Pour trouver l'objet requis dans la liste des objets de la Sauvegarde,

triez les objets ou filtrez-les.

Restauration des fichiers depuis la Sauvegarde

Kaspersky Embedded Systems Security place les fichiers dans la Sauvegarde sous forme chiffrée afin de protéger l'appareil contre une éventuelle action malveillante.

Vous pouvez restaurer les fichiers de la Sauvegarde.

La restauration d'un fichier peut s'imposer dans les situations suivantes :

- Si le fichier original infecté contenait des informations importantes et que Kaspersky Embedded Systems Security n'a pas pu préserver son intégrité et que les informations qu'il contenait sont devenues inaccessibles.

- Vous estimez que le fichier ne présente aucun danger pour l'appareil protégé et vous souhaitez l'utiliser. Afin que Kaspersky Embedded Systems Security ne considère plus ce fichier comme un fichier infecté lors des analyses ultérieures, vous pouvez l'exclure du traitement dans la tâche Protection des fichiers en temps réel et dans les tâches Analyse à la demande.

La restauration de fichiers à partir de la sauvegarde peut provoquer une infection de l'appareil protégé.

Lors de la restauration d'un fichier, vous pouvez sélectionner l'emplacement dans lequel il sera enregistré : l'emplacement d'origine (par défaut), le dossier spécial pour objets restaurés sur l'appareil protégé ou un dossier personnalisé sur l'appareil protégé où est installée la Console de l'application.

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.

Restauration de fichiers à partir de la Sauvegarde dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le dossier **Avancé** → **Stockages**.

2. Accédez au dossier **Sauvegarde**.

3. Réalisez une des opérations suivantes :

   - Pour restaurer un objet, choisissez **Restaurer** dans le menu contextuel du nom de l'objet.

   - Pour restaurer plusieurs objets, sélectionnez les objets que vous souhaitez supprimer à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur l'un des objets sélectionnés, puis sélectionnez la commande **Restaurer** dans le menu contextuel.

4. L'objet sera restauré dans le dossier d'origine.

Restauration de fichiers à partir de la Sauvegarde dans Kaspersky Security Center Web Console

1. Ouvrez Web Console.

2. Dans l'arborescence de la console, sélectionnez **Opérations** → **Stockages**.

3. Accédez au dossier **Sauvegarde**.

4. Sélectionnez les objets de la liste, puis cliquez sur le bouton **Restaurer**.

5. L'objet sera restauré dans le dossier d'origine.

Restauration de fichiers à partir de la Sauvegarde dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Stockages** → **Sauvegarde**.

2. Dans le panneau des résultats du nœud **Sauvegarde**, exécutez une des actions suivantes :

   - Pour restaurer un seul objet, choisissez l'option **Restaurer** dans le menu contextuel de l'objet que vous souhaitez restaurer.

   - Pour restaurer plusieurs objets, sélectionnez les objets que vous souhaitez restaurer à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur l'un des objets sélectionnés, puis sélectionnez la commande **Restaurer** dans le menu contextuel.

3. Dans la fenêtre **Restauration d'objet**, indiquez pour chacun des objets sélectionnés le dossier dans lequel l'objet à restaurer va être enregistré.

   Le nom de l'objet apparaît dans le champ **Objet** de la partie supérieure de la fenêtre. Si vous aviez choisi plusieurs objets, le nom du premier objet de la liste des objets sélectionnés s'affiche.

4. Réalisez une des opérations suivantes :

   - Pour restaurer l'objet dans l'emplacement d'origine, sélectionnez la commande **Restaurer dans le dossier d'origine**.

   - Pour restaurer un objet dans le dossier que vous avez défini en tant qu'emplacement de restauration des objets durant l'installation de l'application, sélectionnez **Restaurer dans le dossier par défaut**.

   - Pour enregistrer un objet dans un autre dossier de l'appareil protégé où vous avez installé la Console de l'application, sélectionnez **Restaurer dans le dossier de l'ordinateur local**, puis sélectionnez le dossier souhaité 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. Afin d'appliquer les conditions de restauration définies au reste des objets sélectionnés, cochez la case **Appliquer à tous les objets sélectionnés**.

7. Cliquez sur **OK**.

8. Kaspersky Embedded Systems Security commence par restaurer le premier des objets que vous avez sélectionnés.

9. Si un objet portant le même nom existe déjà dans l'emplacement indiqué, la fenêtre **Un objet portant ce nom existe déjà** s'ouvre.

    a. Sélectionnez une des actions suivantes de Kaspersky Embedded Systems Security :

    - **Remplacer**, pour remplacer l'objet existant par l'objet restaurer.
    - **Renommer** afin d'enregistrer l'objet restauré sous un autre nom. Saisissez le nouveau nom de l'objet restauré et son chemin d'accès dans le champ.
    - **Renommer en ajoutant un suffixe** afin de renommer l'objet en lui ajoutant un suffixe. Saisissez le suffixe dans le champ.

    b. Si vous sélectionnez plusieurs objets en vue de la restauration, cochez la case **Appliquer à tous les objets sélectionnés** pour appliquer l'action (**Remplacer** ou **Renommer**) au reste de la sélection d'objets. (Si vous avez sélectionné **Renommer**, la case **Appliquer à tous les objets sélectionnés** ne sera pas accessible).

    c. Cliquez sur **OK**.

    L'objet sera restauré. Les informations relatives à la restauration sont consignées dans le journal d'audit système.

Si vous n'aviez pas sélectionné l'option **Appliquer à tous les objets sélectionnés** dans la fenêtre **Restauration d'objet**, la fenêtre **Restauration d'objet** peut s'ouvrir à nouveau. Vous pouvez y indiquer l'emplacement de la restauration de l'objet sélectionné suivant.

Suppression des fichiers de la Sauvegarde

Suppression de fichiers de la Sauvegarde dans la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.

2. Dans l'arborescence de la console, sélectionnez **Avancé** → **Stockages**.

3. Accédez au dossier **Sauvegarde**. Le volet droit affiche la liste des objets dans la Sauvegarde.

4. Réalisez une des opérations suivantes :

   - Pour supprimer un objet, choisissez **Supprimer** dans le menu contextuel de l'objet.

   - Pour supprimer plusieurs objets, sélectionnez les objets que vous souhaitez supprimer à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur l'un des objets sélectionnés, puis sélectionnez la commande **Supprimer** dans le menu contextuel.

5. Les objets sélectionnés sont supprimés de la Sauvegarde.

Suppression de fichiers de la Sauvegarde dans Kaspersky Security Center Web Console

1. Ouvrez Web Console.

2. Dans l'arborescence de la console, sélectionnez **Opérations** → **Stockages**.

3. Accédez au dossier **Sauvegarde**.

4. Sélectionnez les objets de la liste, puis cliquez sur le bouton **Supprimer**.

5. Les objets sélectionnés sont supprimés de la Sauvegarde.

Suppression de fichiers de la Sauvegarde dans la Console d'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Stockages** → **Sauvegarde**.

2. Le volet droit affiche la liste des objets dans la Sauvegarde.

3. Réalisez une des opérations suivantes :

   - Pour supprimer un objet, choisissez **Supprimer** dans le menu contextuel de l'objet.

   - Pour supprimer plusieurs objets, sélectionnez les objets que vous souhaitez supprimer à l'aide de la touche **CTRL** ou **MAJ**, cliquez avec le bouton droit de la souris sur l'un des objets sélectionnés, puis sélectionnez la commande **Supprimer** dans le menu contextuel.

4. Les objets sélectionnés sont supprimés de la Sauvegarde.

Envoi des objets probablement infectés à Kaspersky pour examen

Si le comportement d'un objet indique selon vous la présence éventuelle d'une menace et que Kaspersky Embedded Systems Security le considère comme un objet sain, il se peut que vous soyez en présence d'une menace inconnue dont la signature n'a pas encore été ajoutée aux bases de données. Vous pouvez envoyer cet objet à Kaspersky pour examen. Les experts antivirus de Kaspersky analyseront le fichier et s'ils découvrent une nouvelle menace, ils ajouteront sa signature et l'algorithme de réparation aux bases. Quand vous analysez à nouveau l'objet après la mise à jour des bases de l'application, il est probable que Kaspersky Embedded Systems Security détermine que l'objet est infecté et qu'il le désinfecte. Vous pourrez alors non seulement conserver l'objet mais également éviter une épidémie virale.

Envoyer un objet pour analyse aux experts de Kaspersky à partir de la Console d'administration de Kaspersky Security Center

1. Ouvrez la Console d'administration de Kaspersky Security Center.
2. Dans l'arborescence de la console, sélectionnez **Avancé** → **Stockages**.
3. Accédez au dossier **Sauvegarde**.
4. Réalisez une des opérations suivantes :
   - Pour envoyer un objet, choisissez **Envoyer à Kaspersky** dans le menu contextuel du nom de l'objet.
   - Pour envoyer plusieurs objets, sélectionnez les objets que vous souhaitez envoyer à l'aide de la touche CTRL ou MAJ, cliquez avec le bouton droit de la souris sur un des objets sélectionnés et sélectionnez la commande **Envoyer à Kaspersky** dans le menu contextuel.
5. Sélectionnez le dossier d'enregistrement de l'objet sur votre ordinateur.
6. Après cela, vous êtes invité à accéder au portail Kaspersky Threat Intelligence Portal et à charger l'objet enregistré pour obtenir toutes les informations à son sujet.

Envoyer un objet pour analyse aux experts de Kaspersky à partir de Kaspersky Security Center Web Console

1. Ouvrez Web Console.
2. Dans l'arborescence de la console, sélectionnez **Opérations** → **Stockages**.
3. Accédez au dossier **Sauvegardes de fichiers**.
4. Sélectionnez les objets de la liste, puis cliquez sur le bouton **Envoyer à Kaspersky**.
5. Sélectionnez le dossier d'enregistrement de l'objet sur votre ordinateur.
6. Après cela, vous êtes invité à accéder au portail Kaspersky Threat Intelligence Portal et à charger l'objet enregistré pour obtenir toutes les informations à son sujet.

Kaspersky Security Center Web Console ou la Console d'administration ne peut pas être utilisée pour envoyer à Kaspersky des objets de la Sauvegarde pour analyse s'ils ont été migrés après une mise à jour de la version 3.4 ou une version antérieure de l'application vers la version 4.0 ou une version ultérieure.

Configuration des paramètres de la Sauvegarde

Comment configurer les paramètres de la Sauvegarde dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Complémentaire** → **Stockages** et cliquez sur **Paramètres**.

4. Rendez-vous dans l'onglet **Sauvegarde**.
5. Définissez les paramètres de la sauvegarde (cf. tableau ci-après).
6. Enregistrez vos modifications.

Configuration des paramètres de la Sauvegarde dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez **Complémentaire** → **Stockages** et cliquez sur le bouton **Configurer**.
5. Rendez-vous dans l'onglet **Sauvegarde**.
6. Définissez les paramètres de la sauvegarde (cf. tableau ci-après).
7. Enregistrez vos modifications.

Comment configurer les paramètres de la Sauvegarde dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Stockages** → **Sauvegarde**.
2. Dans le panneau des résultats du nœud **Sauvegarde**, cliquez sur **Propriétés**.
3. Dans la fenêtre **Propriétés : Sauvegarde**, définissez les paramètres de la sauvegarde (cf. tableau ci-après).
4. Enregistrez vos modifications.

Paramètres de sauvegarde

Paramètre	Description
Supprimer les objets après	Si cette fonctionnalité est activée, la limite de conservation maximale des fichiers est définie par l'intervalle renseigné. La durée maximale de conservation par défaut des fichiers est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Embedded Systems Security supprime les fichiers les plus anciens de la sauvegarde.
Limiter la taille de la sauvegarde à	Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security surveille le volume total des objets placés dans la Sauvegarde. En cas de dépassement de cette valeur (fixée par défaut à 400 Mo), Kaspersky Embedded Systems Security consigne l'événement *Dépassement de la taille maximale de la sauvegarde* et publie une notification conformément aux paramètres pour ce type d'événements. Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security ne surveille pas le volume total des objets placés dans la Sauvegarde. Par défaut, la fonctionnalité est désactivée.
Limiter la valeur du seuil de l'espace disponible à	Si cette fonctionnalité est activée, Kaspersky Embedded Systems Security contrôle l'espace libre minimum dans la sauvegarde (100 Mo par défaut). Si l'espace libre est inférieur à la valeur du seuil, Kaspersky Embedded Systems Security consigne l'événement *Dépassement du seuil d'espace disponible dans la sauvegarde* et envoie une notification conformément aux paramètres des notifications sur ce type d'événement. La case **Limiter la valeur du seuil de l'espace disponible à** est active si la case **Limiter la taille de la sauvegarde à** est cochée. Cette option est activée 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.

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 :

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Stockages** → **Sauvegarde**.
2. Dans le panneau des résultats du nœud **Sauvegarde**, cliquez sur **Statistiques**.

   Cela ouvre la fenêtre **Statistiques de sauvegarde**. La fenêtre **Sauvegarde : Statistiques** reprend les informations relatives à l'état de la Sauvegarde à l'heure actuelle (cf. tableau ci-dessous).

Informations sur l'état actuel de la Sauvegarde

Champ	Description
Taille actuelle de la sauvegarde	Volume total de données dans le dossier Sauvegarde ; tient compte de la taille des fichiers chiffrés.
Nombre total d'objets	Nombre d'objets présents actuellement dans la sauvegarde.

Interdire l'accès aux ressources réseau. Sessions réseau bloquées

Cette section décrit comment bloquer les appareils distants et configurer les paramètres pour la Liste des sessions réseau bloquées.

Liste des sessions réseau bloquées

Par défaut, la Liste des sessions réseau bloquées peut être utilisée si l'un des modules suivants est installé : Protection contre les menaces réseau ou Détection comportementale. Ces modules détectent les tentatives à distance de chiffrement, d'ouverture ou d'exécution des objets sur l'appareil protégé ou dans les dossiers partagés de l'appareil de stockage NAS conformément à la liste des sessions réseau bloquées. Les informations relatives aux sessions réseau bloquées de tous les appareils protégés sont envoyées au Kaspersky Security Center. Kaspersky Embedded Systems Security bloque la session en cours et, en termes de session en cours, rend les dossiers partagés ou les dossiers de appareils de stockage NAS inaccessibles.

La liste des sessions réseau bloquées est remplie quand au moins une des tâches suivantes est lancée en mode actif et (quand les conditions indiquées sont remplies) :

- Pour la tâche *Protection contre les menaces réseau* : une activité typique des attaques réseau est détectée.

  Kaspersky Embedded Systems Security efface la liste du groupe lorsque l'application est redémarrée et lorsque les paramètres de la Protection contre les menaces réseau sont modifiés.

- Pour la tâche *Détection comportementale* : le chiffrement malveillant par un appareil accédant aux ressources des fichiers réseau est détecté.

Après la détection d'une activité malveillante ou d'une tentative de chiffrement, la tâche envoie des informations sur la session réseau attaquante à la Liste des sessions réseau bloquées et l'application crée un événement de type *Attention* pour la session en cours de l'hôte attaquant. Toute tentative de cette session pour accéder au dossier réseau partagé protégés sera bloquée.

Si l'identifiant local unique (LUID) d'un hôte à l'origine de la session réseau attaquante est ajouté à la liste des sessions réseau bloquées, Kaspersky Embedded Systems Security détermine l'adresse IP de cet hôte et l'ajoute au lieu du LUID de l'hôte attaquant à la liste des sessions réseau bloquées.

Par défaut, Kaspersky Embedded Systems Security supprime les sessions réseau bloquées de la liste 30 minutes après leur ajout. L'accès aux ressources de fichier réseau est rétabli automatiquement après la suppression des sessions réseau de la liste des sessions réseau bloquées. Vous pouvez indiquer la durée au terme de laquelle les sessions réseau bloquées sont automatiquement débloquées.

Sachez que lorsque vous limitez l'accès à la gestion des stockages pour n'importe quel compte utilisateur, la liste des sessions réseau bloquées reste disponible. Les paramètres pour les sessions réseau bloquées ne sont pas modifiables, sauf si le compte utilisateur sélectionné possède les **Modifier les autorisations** pour l'administration de Kaspersky Embedded Systems Security.

Gestion de la liste des sessions réseau bloquées

Pour ajouter des hôtes qui affichent une activité malveillante ou de chiffrement malveillant quelconque à la Liste des sessions réseau bloquées et bloquer l'accès aux ressources de fichier réseau pour ces sessions, au moins un des modules suivants doit être activé :

- Protection contre les menaces réseau
- Détection comportementale.

Activation du blocage des hôtes douteux dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre de la stratégie, sélectionnez **Contrôle de l'activité réseau** → **Paramètres de la Protection contre les menaces réseau** et cliquez sur **Paramètres**.
4. Dans la fenêtre qui s'ouvre, cochez la case **Protection contre les menaces réseau**.

5. Sous l'onglet **Général**, activez le mode **Bloquer**.

6. Cochez la case **Bloquer les appareils attaquants pendant** et définissez la durée du blocage.

7. Enregistrez vos modifications.

Pour configurer le blocage des sessions réseau douteuses pour le module Détection comportementale dans les propriétés de la stratégie, procédez comme suit :

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Dans la fenêtre de la stratégie, sélectionnez **Protection en temps réel de l'ordinateur → Détection comportementale** et cliquez sur **Paramètres**.

4. Dans la fenêtre qui s'ouvre, cochez la case **Détection comportementale**.

5. Accédez à l'onglet **Protection des dossiers partagés** et cochez la case **Protéger les dossiers partagés**.

6. Sélectionnez **Bloquer la connexion pendant** et spécifiez la durée de blocage.

7. Si nécessaire, spécifiez les zones de protection et les exclusions à l'aide d'une adresse IP et d'un masque.

8. Enregistrez vos modifications.

Activation du blocage des hôtes douteux dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Contrôle de l'activité réseau → Protection contre les menaces réseau** et cliquez sur le bouton **Configurer**.

5. Dans la fenêtre qui s'ouvre, cochez la case **Activer la Protection contre les menaces réseau**.

6. Activez le mode **Interdire**.

7. Cochez la case **Bloquer les appareils attaquants pendant** et définissez la durée du blocage.

8. Si nécessaire, spécifiez les exclusions par adresse IP.

9. Enregistrez vos modifications.

Pour configurer le blocage des sessions réseau douteuses pour le module Détection comportementale, procédez comme suit :

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Rendez-vous dans **Protection en temps réel de l'ordinateur → Détection comportementale** et cliquez sur le bouton **Configurer**.

5. Dans la fenêtre qui s'ouvre, cochez la case **Activer la Détection comportementale**.

6. Accédez à l'onglet **Protection des dossiers partagés** et cochez la case **Activer la protection des dossiers partagés contre le chiffrement externe**.

7. Sélectionnez **Bloquer la connexion** et spécifiez la durée de blocage dans la section **Lors de la détection du chiffrement externe de dossiers partagés**.

8. Si nécessaire, spécifiez les zones de protection et les exclusions à l'aide d'une adresse IP et d'un masque.

9. Enregistrez vos modifications.

Activation du blocage des hôtes douteux dans la Console de l'application

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Protection contre les menaces réseau**.

2. Dans le panneau des résultats du nœud **Protection contre les menaces réseau**, cliquez sur **Propriétés**.

   La fenêtre **Propriétés : Protection contre les menaces réseau** s'ouvre.

3. Dans la fenêtre qui s'ouvre, cochez la case **Protection contre les menaces réseau**.

4. Sous l'onglet **Général**, activez le mode **Bloquer**.

5. Cochez la case **Bloquer les appareils attaquants pendant** et définissez la durée du blocage.

6. Enregistrez vos modifications.

Pour configurer le blocage des sessions réseau douteuses pour le module Détection comportementale, procédez comme suit :

1. Dans l'arborescence de la Console de Kaspersky Embedded Systems Security, sélectionnez **Protection en temps réel de l'ordinateur → Protection contre le chiffrement**.

2. Dans le volet de résultats du nœud **Détection comportementale**, cliquez sur **Propriétés**.

3. Dans la fenêtre qui s'ouvre, cochez la case **Détection comportementale**.

4. Accédez à l'onglet **Protection des dossiers partagés** et cochez la case **Protéger les dossiers partagés**.

5. Sélectionnez **Bloquer la connexion pendant** et spécifiez la durée de blocage.

6. Si nécessaire, spécifiez les zones de protection et les exclusions à l'aide d'une adresse IP et d'un masque.

7. Enregistrez vos modifications.

Configuration de la liste des sessions bloquées via la Console de l'application

1. Dans l'arborescence de la Console de l'application, développez le nœud **Stockages**.

2. Sélectionnez le nœud enfant **Sessions réseau bloquées**.

3. Dans le panneau des résultats, cliquez sur le bouton **Propriétés**.

4. Dans la fenêtre qui s'ouvre, cochez la case **Bloquer les appareils attaquants pendant** et spécifiez la durée du blocage.

5. Pour restaurer l'accès à toutes les sessions réseau bloquées, cliquez sur **Débloquer tout** dans la partie supérieure de la fenêtre.

   Toutes les sessions réseaux bloquées seront supprimées de la liste et débloqués.

6. Pour supprimer les sessions réseau de la liste des sessions réseau bloquées, sélectionnez une ou plusieurs sessions dans la liste dans le panneau des résultats, puis cliquez sur **Débloquer la sélection** dans la partie supérieure de la fenêtre.

   Les sessions réseau sélectionnées sont débloquées.

Enregistrement des événements. Journaux de Kaspersky Embedded Systems Security

Cette section fournit des informations sur l'utilisation des journaux de Kaspersky Embedded Systems Security.

Méthodes d'enregistrement des événements de Kaspersky Embedded Systems Security

Les événements de Kaspersky Embedded Systems Security sont scindés en deux groupes :

- événements liés au fonctionnement des modules de l'application, au traitement des objets dans les tâches de Kaspersky Embedded Systems Security ;
- événements liés à l'administration de Kaspersky Embedded Systems Security, par exemple lancement de l'application, création ou suppression de tâches, modification des paramètres d'une tâche.

Kaspersky Embedded Systems Security enregistre les événements dans le journal à l'aide des méthodes suivantes :

- **Journaux des opérations des modules de l'application**. Les journaux contiennent des informations sur les événements survenus pendant le fonctionnement des modules de l'application.
- **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. Il convient également des informations relatives aux événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur l'appareil protégé.
- **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.

Les fichiers téléchargeables via les liens suivants contiennent des tableaux qui reprennent la liste complète des événements de Kaspersky Embedded Systems Security des catégories suivantes :

- Événements enregistrés par Kaspersky Embedded Systems Security dans le journal des événements.

  TÉLÉCHARGER WEL-EVENTS.ZIP
- Événements que Kaspersky Embedded Systems Security envoie au Serveur d'administration.

  TÉLÉCHARGER KSC-EVENTS.ZIP

Configuration des paramètres des journaux

Vous pouvez modifier les paramètres suivants pour les journaux de Kaspersky Embedded Systems Security :

- Durée de la conservation des événements dans les journaux d'exécution des tâches et du journal d'audit système.
- Emplacement du dossier dans lequel Kaspersky Embedded Systems Security enregistre les fichiers des journaux d'exécution de la tâche et du journal d'audit système.
- Seuils de génération d'événements pour *Les bases sont dépassées*, *Les bases sont fortement dépassées* et *Analyse des zones critiques non réalisée depuis longtemps*.
- Événements consignés par Kaspersky Embedded Systems Security dans les journaux d'exécution de la tâche, dans le journal d'audit système et dans le journal des événements de Kaspersky Embedded Systems Security dans la console Observateur d'événements.
- Événements que Kaspersky Embedded Systems Security envoie au serveur SIEM.

Comment configurer les paramètres des journaux dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Journaux et notifications**.
4. Dans la section **Journaux des tâches**, cliquez sur **Paramètres**.

   La fenêtre **Notifications** s'ouvre.
5. Dans cette fenêtre, sélectionnez le journal à configurer et réglez les paramètres de chaque événement :
   - Emplacement d'enregistrement des événements : rapport local ou journal des événements Windows.
   - Notifications d'événements : Notifier par email, Notifier en utilisant le service de terminal et/ou Notifier en exécutant le fichier exécutable.
   - Envoyer l'événement à un serveur SIEM et/ou à Kaspersky Security Center.
6. Configurez les seuils de génération d'événements en cliquant sur **Paramètres des seuils de génération des événements**.
7. Dans la fenêtre qui s'ouvre, indiquez le nombre de jours au bout duquel les événements suivants doivent être enregistrés : *Les bases sont dépassées*, *Les bases sont fortement dépassées* et *Analyse des zones critiques non réalisée depuis longtemps*.
8. Configurez les notifications par email en cliquant sur **Paramètres des notifications par email**.
9. Enregistrez vos modifications.

Comment configurer les paramètres des journaux dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Journaux et notifications → Journaux des tâches** et cliquez sur le bouton **Configurer**.
5. Ceci ouvre une fenêtre ; dans cette fenêtre, sous l'onglet **Notifications**, sélectionnez le journal à configurer et réglez les paramètres des événements individuels :
   - Emplacement d'enregistrement des événements : rapport local ou journal des événements Windows.
   - Notifications d'événements : Notifier par email, Notifier en utilisant le service de terminal et/ou Notifier en exécutant le fichier exécutable.
   - Envoyer l'événement à un serveur SIEM et/ou à Kaspersky Security Center.
6. Configurez les notifications par email sous l'onglet **Paramètres des notifications par email**.
7. Enregistrez vos modifications.

Comment configurer les paramètres des journaux dans la Console de l'application :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Sélectionnez **Propriétés**.

   La fenêtre **Notifications** s'ouvre.
3. Dans cette fenêtre, sélectionnez le journal à configurer et réglez les paramètres de chaque événement :
   - Emplacement d'enregistrement des événements : rapport local ou journal des événements Windows.
   - Notifications d'événements : Notifier par email, Notifier en utilisant le service de terminal et/ou Notifier en exécutant le fichier exécutable.
   - Envoyer l'événement à un serveur SIEM et/ou à Kaspersky Security Center.
4. Configurez les seuils de génération d'événements en cliquant sur **Paramètres des seuils de génération des événements**.
5. Dans la fenêtre qui s'ouvre, indiquez le nombre de jours au bout duquel les événements suivants doivent être enregistrés : *Les bases dépassées (jours)*, *Les bases sont fortement dépassées (jours)* et *Analyse des zones critiques non réalisée depuis longtemps (jours)*.
6. Configurez les notifications par email en cliquant sur **Paramètres des notifications par email**.
7. Enregistrez vos modifications.

Tri des événements dans le journal

Par défaut, les événements du journal sont classés par ordre chronologique inverse.

Pour trier les événements dans le journal, procédez comme suit :

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Sélectionnez le journal requis.
3. Dans le volet résultats, sélectionnez l'en-tête de la colonne que vous souhaitez utiliser pour trier les événements de la liste.

Le résultat du tri est conservé jusqu'à la prochaine consultation des journaux d'exécution.

Filtrage des événements dans le journal

Vous pouvez configurer le journal pour afficher uniquement les enregistrements relatifs aux événements qui répondent aux conditions de filtrage (filtres) que vous définissez.

Pour filtrer les événements dans le journal, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Journaux et notifications**.
2. Sélectionnez le journal pour lequel vous souhaitez configurer un filtre, puis dans le panneau des résultats, cliquez sur **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 que vous souhaitez utiliser pour filtrer les événements.

   b. Dans la liste **Opérateur**, sélectionnez la condition de filtrage. Les conditions de filtrage varient en fonction de l'option choisie dans la liste **Nom du champ**.

   c. Choisissez la valeur du filtre dans la liste **Valeur du champ**.

   d. Cliquez sur **Ajouter**.

Le filtre ajouté apparaît dans la liste des filtres de la boîte de dialogue **Paramètres du filtre**.

4. Le cas échéant, réalisez une des opérations suivantes :

   - Pour combiner plusieurs filtres à l'aide de l'opérateur logique « ET », sélectionnez **Si toutes les conditions sont remplies**.
   - Afin de réunir quelques filtres selon l'opérateur logique « OU », sélectionnez l'option **Si une condition est remplie**.

5. Cliquez sur le bouton **OK** pour enregistrer les critères de filtrage des événements du journal.

   La liste des événements du journal affiche uniquement les événements qui répondent aux critères de filtrage. Le résultat du filtrage est conservé jusqu'à la prochaine consultation des journaux d'exécution.

Pour désactiver le filtre, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Journaux et notifications**.
2. Sélectionnez le journal pour lequel vous souhaitez supprimer le filtre, puis cliquez sur **Supprimer le filtre**.

   Le journal affichera alors tous les événements.

Suppression des événements du journal

Par défaut, Kaspersky Embedded Systems Security conserve les enregistrements des journaux pendant 30 jours. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution.

Pour supprimer des événements du journal, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Journaux et notifications**.
2. Sélectionnez le journal dont vous souhaitez supprimer les événements et, dans le panneau des résultats, cliquez sur **Nettoyer**.
3. Confirmez l'effacement.

   Le journal est vidé.

Exportation des informations depuis le journal

Vous pouvez exporter les données des journaux dans un fichier CSV ou TXT.

Pour exporter des événements depuis les journaux :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Journaux et notifications**.
2. Sélectionnez un journal et, dans le panneau des résultats, cliquez sur le bouton **Exporter le journal**.

   La fenêtre **Enregistrer sous** s'ouvre.

3. Indiquez le nom, l'emplacement et le type de fichier vers lequel vous souhaitez exporter les données du journal.

4. Cliquez sur **Enregistrer**.

Les informations des journaux sont enregistrées dans le fichier indiqué.

Journal d'audit système

Kaspersky Embedded Systems Security réalise un audit système des événements liés à l'administration de Kaspersky Embedded Systems Security. L'application enregistre les informations relatives au lancement de l'application, au lancement et à l'arrêt de tâches de Kaspersky Embedded Systems Security, aux modifications des paramètres des tâches, à la création et à la suppression de tâches Analyse à la demande. L'application consigne également des informations relatives aux événements liés aux violations de la sécurité ou aux tentatives de violation de la sécurité sur l'appareil protégé. Les enregistrements de l'ensemble de ces événements apparaissent dans le volet résultats lorsque vous sélectionnez le nœud **Audit système** dans la console de l'application.

Par défaut, Kaspersky Embedded Systems Security conserve les entrées du journal d'audit système pendant 30 jours. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution.

Vous pouvez désigner un dossier dans lequel Kaspersky Embedded Systems Security va stocker les fichiers du journal d'audit système, différent du dossier choisi par défaut.

Journaux des modules et des tâches

Les informations sur le fonctionnement des modules et des tâches de Kaspersky Embedded Systems Security s'affichent dans la Console de l'application, dans le panneau des résultats, lorsque vous sélectionnez un nœud avec le nom du module ou de la tâche dans la section **Journaux et notifications**.

Par défaut, Kaspersky Embedded Systems Security conserve les enregistrements dans les journaux des modules et des tâches pendant 30 jours. Pour les tâches : à partir du moment où elles sont terminées. Vous pouvez modifier la durée de conservation des enregistrements dans les journaux d'exécution des tâches et des modules.

Vous pouvez désigner un dossier différent du dossier par défaut dans lequel Kaspersky Embedded Systems Security va enregistrer les fichiers des journaux d'exécution des tâches et des modules. Vous pouvez également sélectionner les événements qui seront consignés dans les journaux d'exécution des tâches et des modules par Kaspersky Embedded Systems Security.

Les journaux d'exécution des tâches reprennent des informations détaillées sur tous les événements survenus dans ces tâches depuis leur lancement ainsi que les statistiques d'exécution des tâches et leurs paramètres.

Pour consulter les statistiques et les informations relatives à une tâche de Kaspersky Embedded Systems Security, procédez comme suit :

1. Dans l'arborescence de la Console de l'application, développez le nœud **Journaux et notifications**.

2. Sélectionnez une tâche et, dans le panneau des résultats, choisissez l'onglet **Statistiques**.

Consultation du journal des événements de Kaspersky Embedded Systems Security dans l'observateur d'événements

Le module logiciel enfichable Observateur d'événements de Microsoft Windows pour Microsoft Management Console permet de consulter le journal des événements de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security y consigne les événements nécessaires au diagnostic des échecs de fonctionnement de l'application.

Vous pouvez sélectionner les événements à enregistrer dans le journal des événements selon les critères suivants :

- **selon le type d'événement**.
- **selon le niveau de détail**. Le niveau de détail correspond au niveau d'importance des événements enregistrés dans le journal (Informatifs, importants ou critiques). Le niveau le plus détaillé est le niveau Informatif qui enregistre tous les événements. Le niveau le moins détaillé est le niveau Critique qui enregistre uniquement les événements critiques.

Pour consulter les informations reprises dans le journal des événements de Kaspersky Embedded Systems Security.

1. Cliquez sur le bouton **Démarrer**, saisissez la commande `mmc` dans la barre de recherche, puis appuyez sur la touche **ENTER**.

   Microsoft Management Console s'ouvre.

2. Choisissez **Fichier** > **Ajouter ou supprimer un module logiciel enfichable**.

   La fenêtre **Ajout et suppression de modules logiciels enfichables** s'ouvre.

3. Dans la liste des modules logiciels enfichables disponibles, sélectionnez **Observateur d'événements** et cliquez sur le bouton **Ajouter**.

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

4. Dans la fenêtre **Sélection d'ordinateur**, indiquez l'appareil protégé sur lequel Kaspersky Embedded Systems Security est installé, puis cliquez sur **OK**.

5. Dans la fenêtre **Ajout et suppression de modules logiciels enfichables**, cliquez sur le bouton **OK**.

   Le nœud **Observateur d'événements** apparaît dans l'arborescence de Microsoft Management Console.

6. Développez le nœud **Observateur d'événements** et sélectionnez le nœud enfant **Journaux des applications et des services** > **Kaspersky Embedded Systems Security**.

Le journal des événements de Kaspersky Embedded Systems Security s'ouvre.

À propos de l'intégration à SIEM

Pour diminuer la charge sur les appareils de faible puissance et réduire le risque de dégradation du système suite à l'augmentation des tailles des journaux de l'application, vous pouvez configurer la publication des événements de l'audit et des événements des tâches exécutées via le protocole syslog sur le *serveur syslog*.

Un serveur syslog est un serveur externe qui sert à la collecte des événements (SIEM). Il stocke et analyse les événements reçu et exécute d'autres actions de gestion de journaux.

Vous pouvez utiliser deux modes d'intégration à SIEM :

- Doubler les événements sur le serveur syslog : dans ce mode, tous les événements d'exécution des tâches dont la publication est configurée dans les paramètres des journaux, ainsi que tous les événements de l'audit système, continuent d'être conservés sur l'appareil protégé même après avoir été envoyés au serveur SIEM.

  Nous conseillons l'utilisation de ce mode pour réduire autant que possible la charge sur l'appareil protégé.

- Supprimer les copies locales des événements : dans ce mode, tous les événements enregistrés au cours du fonctionnement de l'application et publiés dans le serveur SIEM soient supprimés de l'appareil protégé.

  L'application ne supprime jamais les versions locales des Journaux de sécurité.

Kaspersky Embedded Systems Security peut convertir les événements dans les journaux de l'application aux formats pris en charge par le serveur syslog afin que ces événements puissent être transmis et reconnus par le serveur SIEM. L'application prend en charge la conversion au format de données structurées et au format JSON.

Il est recommandé de choisir le format des événements d'après la configuration du serveur SIEM utilisé.

Configuration des paramètres d'intégration à SIEM

L'intégration à SIEM n'est pas appliquée par défaut. Vous pouvez activer et désactiver l'intégration à SIEM, ainsi que configurer les paramètres pertinents.

Vous pouvez réduire le risque que les événements ne soient pas envoyés au serveur SIEM en configurant des connexions à plusieurs serveurs SIEM.

Kaspersky Embedded Systems Security se connecte au premier serveur SIEM de la liste. Si la tentative de connexion échoue, Kaspersky Embedded Systems Security tente de se connecter aux autres serveurs de la liste, un par un.

Kaspersky Embedded Systems Security utilise également les événements de l'audit système pour vous signaler les tentatives ratées de connexion au serveur SIEM ainsi que les erreurs survenues lors de l'envoi des événements au serveur SIEM.

Comment configurer l'intégration SIEM dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.

2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.

3. Sélectionnez la section **Journaux et notifications**.

4. Cliquez sur le bouton **Paramètres** dans le groupe **Intégration SIEM**.

   La fenêtre **Intégration SIEM** s'ouvre.

5. Dans le groupe **Paramètres d'intégration**, cochez la case **Activer la transmission des événements de sécurité vers un serveur SIEM**.

6. Configurez la connexion au serveur SIEM dans le groupe **Paramètres de connexion aux serveurs SIEM** :

   a. Cliquez sur **Ajouter**.

   b. Dans la fenêtre **Ajouter un serveur** qui s'ouvre, saisissez l'adresse du serveur SIEM (IPv4, DNS), le port et le protocole de connexion.

   c. Cliquez sur **Paramètres de sécurité de la connexion TCP**.

   d. Dans la fenêtre **Paramètres de sécurité de la connexion TCP** qui s'ouvre, gérez les paramètres de connexion au serveur SIEM (cf. le tableau ci-dessous).

7. Si nécessaire, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog distant** dans le groupe **Paramètres de transmission d'événements vers le serveur SIEM**. Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le serveur SIEM. Il est recommandé d'utiliser ce mode sur les appareils de faible puissance. Si la case est décochée, l'application envoie uniquement les événements au serveur SIEM. Les copies des journaux continuent d'être conservées localement. Par défaut, la case est décochée.

   L'application ne supprime jamais les versions locales des Journaux de sécurité.

8. Dans le groupe **Format des événements**, sélectionnez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi au serveur SIEM. L'option **Convertir les événements au format STRUCTURED-DATA** est sélectionnée par défaut. Il est recommandé de choisir le format des événements d'après la configuration du serveur SIEM utilisé.

9. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

10. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment configurer l'intégration SIEM dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Journaux et notifications**.

5. Cliquez sur le bouton **Configurer** dans le groupe **Intégration SIEM**.

   La fenêtre **Intégration SIEM** s'ouvre.

6. Cochez la case **Activer la transmission des événements de sécurité vers un serveur SIEM**.

7. Configurez la connexion au serveur SIEM dans le groupe **Paramètres de connexion aux serveurs SIEM** :

   a. Cliquez sur **Ajouter**.

   b. Dans la fenêtre **Serveur SIEM** qui s'ouvre, saisissez l'adresse du serveur SIEM (IPv4, DNS), le port et le protocole de connexion.

   c. Dans le groupe **Protection de la connexion**, cliquez sur le lien **Paramètres de connexion aux serveurs SIEM**.

   d. Dans la fenêtre **Paramètres de connexion aux serveurs SIEM** qui s'ouvre, gérez les paramètres de connexion au serveur SIEM (cf. le tableau ci-dessous).

   e. Dans le groupe **Format des événements**, sélectionnez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi au serveur SIEM. L'option **Convertir les événements au format STRUCTURED-DATA** est sélectionnée par défaut. Il est recommandé de choisir le format des événements d'après la configuration du serveur SIEM utilisé.

   f. Si nécessaire, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog distant** dans le groupe **Paramètres de connexion**. Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le serveur SIEM. Il est recommandé d'utiliser ce mode sur les appareils de faible puissance. Si la case est décochée, l'application envoie uniquement les événements au serveur SIEM. Les copies des journaux continuent d'être conservées localement. Par défaut, la case est décochée.

   > L'application ne supprime jamais les versions locales des Journaux de sécurité.

8. Fermez le cadenas pour appliquer la stratégie aux ordinateurs.

9. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment configurer l'intégration SIEM dans la Console de l'application

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.

2. Sélectionnez **Intégration SIEM**.

   La fenêtre **Intégration SIEM** s'ouvre.

3. Dans le groupe **Paramètres d'intégration**, cochez la case **Activer la transmission des événements de sécurité vers un serveur SIEM**.

4. Configurez la connexion au serveur SIEM dans le groupe **Paramètres de connexion aux serveurs SIEM** :

   a. Cliquez sur **Ajouter**.

   b. Dans la fenêtre **Ajouter un serveur** qui s'ouvre, saisissez l'adresse du serveur SIEM (IPv4, DNS), le port et le protocole de connexion.

   c. Cliquez sur **Paramètres de sécurité de la connexion TCP**.

   d. Dans la fenêtre **Paramètres de sécurité de la connexion TCP** qui s'ouvre, gérez les paramètres de connexion au serveur SIEM (cf. le tableau ci-dessous).

5. Si nécessaire, cochez la case **Supprimer les copies locales des événements qui ont été envoyés à un serveur syslog distant** dans le groupe **Paramètres de transmission d'événements vers le serveur SIEM**. Si la case est cochée, l'application supprime les copies locales des événements une fois publiées dans le serveur SIEM. Il est recommandé d'utiliser ce mode sur les appareils de faible puissance. Si la case est décochée, l'application envoie uniquement les événements au serveur SIEM. Les copies des journaux continuent d'être conservées localement. Par défaut, la case est décochée.

   L'application ne supprime jamais les versions locales des Journaux de sécurité.

6. Dans le groupe **Format des événements**, sélectionnez le format sous lequel vous voulez convertir les événements au moment du fonctionnement de l'application en vue de leur envoi au serveur SIEM. L'option **Convertir les événements au format STRUCTURED-DATA** est sélectionnée par défaut. Il est recommandé de choisir le format des événements d'après la configuration du serveur SIEM utilisé.

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

Paramètres de connexion au serveur SIEM

Paramètre	Description
Délai d'attente (s.)	Délai maximal de réponse du serveur SIEM. À l'expiration du délai, Kaspersky Embedded Systems Security essaie de se connecter à un autre serveur SIEM.
Certificat TLS du serveur	Certificat TLS permettant d'établir une connexion sécurisée avec le serveur SIEM. Vous pouvez obtenir un certificat TLS via l'interface d'administration SIEM.
Utiliser l'authentification bidirectionnelle	Authentification bidirectionnelle lors de l'établissement d'une connexion sécurisée entre Kaspersky Embedded Systems Security et SIEM. Pour utiliser l'authentification bidirectionnelle, vous devez activer l'authentification bidirectionnelle dans les paramètres SIEM, puis obtenir un conteneur crypto et définir un mot de passe pour protéger le conteneur crypto. Un conteneur crypto est une archive PFX contenant un certificat et une clé privée. Après avoir configuré les paramètres SIEM, vous devez activer l'authentification bidirectionnelle dans les paramètres de Kaspersky Embedded Systems Security en cochant la case et charger un conteneur crypto protégé par mot de passe. Le conteneur crypto doit être protégé par un mot de passe. Il n'est pas possible d'ajouter de conteneur crypto avec un mot de passe vide.

Moyens de notification de l'administrateur et des utilisateurs

Vous pouvez configurer la notification de l'administrateur et des utilisateurs qui accèdent à l'appareil sur les événements suivants liés au fonctionnement de Kaspersky Embedded Systems Security et à l'état de la protection antivirus de l'appareil.

- L'administrateur peut obtenir des informations sur les événements de certains types.
- Les utilisateurs du réseau local qui contactent l'appareil protégé et les utilisateurs de terminaux de l'appareil peuvent obtenir des informations sur les événements de type *Objet détecté* qui surviennent pendant la tâche Protection des fichiers en temps réel.

Les notifications de l'administrateur ou des utilisateurs peuvent être activées de plusieurs manières :

- Outils des services des terminaux.

  Vous pouvez utiliser cette méthode pour la notification des utilisateurs de l'appareil protégé de terminal si l'appareil protégé est utilisé comme un terminal.

- Lancement du fichier exécutable.

  Cette méthode lance un fichier exécutable stocké sur le disque local de l'appareil protégé quand un événement se produit.

- Envoi par email.

  Ce mode permet l'envoi d'emails.

Vous pouvez rédiger le texte du message pour les types d'événement individuels. Ce texte peut contenir des champs avec les informations sur l'événement. Un message standard est utilisé par défaut pour les notifications des utilisateurs.

Configuration des notifications de l'administrateur et des utilisateurs

La configuration des notifications sur les événements porte sur le mode de notification et sur la composition du texte du message.

Comment configurer les notifications sur les événements dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Journaux et notifications**.
4. Dans la section **Journaux des tâches**, cliquez sur **Paramètres**.

   La fenêtre **Notifications** s'ouvre.
5. Sélectionnez l'événement pour lequel vous souhaitez sélectionner une méthode de notification, puis cliquez sur **Paramètres des notifications**.

   La fenêtre **Paramètres des notifications** s'ouvre.
6. Pour une notification par email, vous pouvez ajouter le texte du message de notification d'événement sous l'onglet **Email**.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Variable** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.

   Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Par défaut**.
7. Pour une notification par exécution d'un fichier exécutable, sous l'onglet **Fichier exécutable**, sélectionnez un fichier sur le disque local de l'appareil protégé ou saisissez son chemin d'accès complet. Ce fichier sera exécuté sur l'appareil protégé lorsque l'événement se produira. 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.
8. Pour une notification par le service terminal, vous pouvez ajouter le texte du message de notification d'événement sous l'onglet **Service de terminal**.

Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Variable** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.

Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Par défaut**.

9. Enregistrez vos modifications.

Comment configurer les notifications sur les événements dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Journaux et notifications → Journaux des tâches** et cliquez sur le bouton **Configurer**.
5. Une fenêtre s'ouvrira, dans cette fenêtre, cliquez sur l'événement pour lequel vous souhaitez sélectionner un mode de notification.

   La fenêtre **Configuration des notifications** s'ouvre.
6. Pour une notification par email, dans la section **Informer les utilisateurs**, sélectionnez la case **Informer par email** et ajoutez le texte du message de notification d'événement.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Ajouter une variable** et sélectionnez les éléments pertinents dans la liste. Les champs avec les informations sur les événements sont repris dans cette section.

   Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Réinitialiser**.
7. Pour une notification en lançant un fichier exécutable, dans la section **Informer les administrateurs**, sélectionnez la case **Lancer le fichier exécutable** et saisissez le chemin d'accès complet à un fichier sur un disque local de l'appareil protégé. Ce fichier sera exécuté sur l'appareil protégé lorsque l'événement se produira. 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.
8. Pour une notification via le service de terminal, dans la section **Informer les administrateurs**, sélectionnez la case **Informer via le service terminal** et ajoutez le texte du message de notification d'événement.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Ajouter une variable** et sélectionnez les éléments pertinents dans la liste. Les champs avec les informations sur les événements sont repris dans cette section.

   Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Réinitialiser**.
9. Enregistrez vos modifications.

Comment configurer les notifications sur les événements dans la Console de l'application

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Sélectionnez **Propriétés**.

   La fenêtre **Notifications** s'ouvre.
3. Sélectionnez l'événement pour lequel vous souhaitez sélectionner une méthode de notification, puis cliquez sur **Paramètres des notifications**.

   La fenêtre **Paramètres des notifications** s'ouvre.
4. Pour une notification par email, vous pouvez ajouter le texte du message de notification d'événement sous l'onglet **Email**.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Variable** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.

   Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Par défaut**.
5. Pour une notification par exécution d'un fichier exécutable, sous l'onglet **Fichier exécutable**, sélectionnez un fichier sur le disque local de l'appareil protégé ou saisissez son chemin d'accès complet. Ce fichier sera exécuté sur l'appareil protégé lorsque l'événement se produira. 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.
6. Pour une notification par le service terminal, vous pouvez ajouter le texte du message de notification d'événement sous l'onglet **Service de terminal**.

   Pour ajouter des champs d'information sur l'événement, cliquez sur le bouton **Variable** et sélectionnez les options désirées dans la liste déroulante. Les champs avec les informations sur les événements sont repris dans cette section.

   Pour restaurer le texte du message des événements par défaut pour l'événement, cliquez sur le bouton **Par défaut**.
7. Enregistrez vos modifications.

Champs d'information sur les événements

Variable	Description
%EVENT_TYPE%	Type d'événements.
%EVENT_TIME%	Heure à laquelle l'événement est survenu
%EVENT_SEVERITY%	Niveau d'importance de l'événement.
%OBJECT%	Nom de l'objet (dans les tâches Protection en temps réel de l'ordinateur et Analyse à la demande). Dans la tâche de mise à jour des modules de l'application, indiquez le nom de la mise à jour et l'adresse de la page Web contenant les informations relatives à la mise à jour.
%VIRUS_NAME%	Nom de l'objet détecté selon la classification de l'Encyclopédie des virus. Ce nom figure dans le nom complet d'un objet détecté que Kaspersky Embedded Systems Security renvoie suite à la détection d'un objet. Vous pouvez afficher le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
%VIRUS_TYPE%	Type de l'objet détecté selon la classification de Kaspersky, par exemple "virus" ou "cheval de Troie". Figure dans le nom complet d'un objet détecté, renvoyé par Kaspersky Embedded Systems Security lorsque celui-ci considère l'objet comme infecté ou probablement infecté. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
%USER_COMPUTER%	Dans la tâche *Protection des fichiers en temps réel*, désigne le nom de l'appareil protégé de l'utilisateur qui a accédé à l'objet sur l'appareil.

Variable	Description
%USER_NAME%	Dans la tâche *Protection des fichiers en temps réel*, désigne le nom de l'utilisateur qui a accédé à l'objet sur l'appareil.
%FROM_COMPUTER%	Nom de l'appareil protégé d'où provient la notification
%EVENT_REASON%	Cause de l'événement (ce champ n'existe pas pour certains événements).
%ERROR_CODE%	Code d'erreur (concerne uniquement l'événement "erreur interne de la tâche").
%TASK_NAME%	Nom de la tâche (concerne uniquement les événements liés à l'exécution des tâches)
%PROTOCOL%	Protocole utilisé.
%MESSAGE%	Texte du message.
%DEVICE_INSTANCEPATH%	Chemin d'accès à l'instance de l'appareil.
%DEVICE_VID%	Fournisseur de l'appareil
%DEVICE_PID%	Type de contrôleur.
%DEVICE_SERIALNUMBER%	Numéro de série de l'appareil.

Configuration les notifications par email

Comment configurer les notifications par email dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, sélectionnez **Journaux et notifications**.
4. Dans la section **Journaux des tâches**, cliquez sur **Paramètres**.
   La fenêtre **Notifications** s'ouvre.
5. Cliquez sur **Paramètres des notifications par email**.
6. Dans la fenêtre qui s'ouvre, cochez la case **Envoyer les notifications sur les événements**.
7. Sous **Envoi de notifications au nom de**, spécifiez les informations sur l'expéditeur : adresse de l'expéditeur, serveur SMTP, port du serveur SMTP, nom d'utilisateur et mot de passe.
8. Sous **Destinataire des notifications**, précisez l'adresse email du destinataire.
9. Pour tester les paramètres, cliquez sur le bouton **Envoyer un message d'essai**.

   La fonctionnalité de message de test est disponible uniquement dans la Console d'administration de Kaspersky Security Center et dans la Console de l'application.

10. Indiquez le mode d'envoi : **Lorsque l'événement survient** ou **Selon la planification (non définie)**. Pour configurer la planification, cliquez sur **Modifier**.
11. Enregistrez vos modifications.

Configuration configurer les notifications par email dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Rendez-vous dans **Journaux et notifications → Journaux des tâches** et cliquez sur le bouton **Configurer**.
5. Une fenêtre s'ouvre ; dans cette fenêtre, sélectionnez l'onglet **Paramètres des notifications par email**.
6. Cochez la case **Envoyer les notifications sur les événements**.
7. Spécifiez les informations sur l'expéditeur : adresse de l'expéditeur, serveur SMTP, port du serveur SMTP, nom d'utilisateur et mot de passe.
8. Spécifiez l'adresse email du destinataire.
9. Indiquez le mode d'envoi : **Lorsque des événements surviennent** ou **Selon la planification**. Le cas échéant, configurez la planification.
10. Enregistrez vos modifications.

Comment configurer les notifications par email dans la Console de l'application

1. Dans l'arborescence de la console de l'application, ouvrez le menu contextuel du nœud **Journaux et notifications**.
2. Sélectionnez **Propriétés**.

   La fenêtre **Notifications** s'ouvre.
3. Cliquez sur **Paramètres des notifications par email**.
4. Dans la fenêtre qui s'ouvre, cochez la case **Envoyer les notifications sur les événements**.
5. Sous **Envoi de notifications au nom de**, spécifiez les informations sur l'expéditeur : adresse de l'expéditeur, serveur SMTP, port du serveur SMTP, nom d'utilisateur et mot de passe.
6. Sous **Destinataire des notifications**, précisez l'adresse email du destinataire.
7. Pour tester les paramètres, cliquez sur le bouton **Envoyer un message d'essai**.

   > La fonctionnalité de message de test est disponible uniquement dans la Console d'administration de Kaspersky Security Center et dans la Console de l'application.

8. Indiquez le mode d'envoi : **Lorsque l'événement survient** ou **Selon la planification (non définie)**. Pour configurer la planification, cliquez sur **Modifier**.
9. Enregistrez vos modifications.

Configuration de l'interaction avec le Serveur d'administration

IL faut sélectionner les types des objets au sujet desquels Kaspersky Embedded Systems Security va envoyer des informations au Serveur d'administration de Kaspersky Security Center.

Comment configurer l'intégration avec le Serveur d'administration dans la Console d'administration de Kaspersky Security Center.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la section **Journaux et notifications**, cliquez sur le bouton **Paramètres** dans la sous-section **Interaction avec le Serveur d'administration**.
4. Une fenêtre s'ouvre. Dans cette fenêtre, choisissez les types d'objets au sujet desquels Kaspersky Embedded Systems Security va transmettre des informations au serveur d'administration de Kaspersky Security Center :
   - **À propos des fichiers de la Sauvegarde**
   - **À propos des fichiers non traités**
   - **À propos des appareils installés**
   - **À propos d'une chaîne de développement de menaces**
5. Enregistrez vos modifications.

   Kaspersky Embedded Systems Security transmet les informations relatives aux types d'objets choisis au Serveur d'administration.

Comment configurer l'interaction avec le Serveur d'administration dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Dans la section **Journaux et notifications**, cliquez sur le bouton **Configurer** dans la sous-section **Interaction avec le Serveur d'administration**.
5. Une fenêtre s'ouvre. Dans cette fenêtre, choisissez les types d'objets au sujet desquels Kaspersky Embedded Systems Security va transmettre des informations au serveur d'administration de Kaspersky Security Center :
   - **Fichiers de la sauvegarde**
   - **À propos des fichiers non traités**

- **Sessions réseau bloquées**
- **Appareils installés**

6. Enregistrez vos modifications.

Gestion du chiffrement du disque BitLocker

BitLocker est une technologie de chiffrement intégrée au système d'exploitation Windows. Kaspersky Embedded Systems Security vous permet de contrôler et de gérer Bitlocker à l'aide de Kaspersky Security Center. BitLocker chiffre le volume logique. Pour en savoir plus sur le fonctionnement de BitLocker, consultez la documentation de Microsoft.

Kaspersky Embedded Systems Security ne prend pas en charge l'administration de BitLocker sur les ordinateurs Windows Vista et Windows Server 2008.

Lors du chiffrement du disque, BitLocker place le programme de démarrage et les autres fichiers auxiliaires dans la system partition. Cette partition n'est pas chiffrée. Lors de l'installation de Windows, le système d'exploitation crée la partition système automatiquement. Si le disque est entièrement partitionné avant l'installation de Windows, le système d'exploitation ne peut pas créer de partition système. Dans ce cas, lorsque vous démarrez le chiffrement de disque BitLocker, le système d'exploitation vous invite à repartitionner le disque et à créer une partition système. Une fois que vous aurez créé une partition système, le système d'exploitation lancera le chiffrement BitLocker.

Kaspersky Embedded Systems Security ne prend pas en charge le chiffrement BitLocker des disques amovibles.

BitLocker fournit un stockage sécurisé des clés d'accès à l'aide d'un module de plateforme sécurisée. *Trusted Platform Module* (TPM) : puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Un module de plateforme sécurisée est généralement installé sur la carte mère de l'ordinateur et interagit avec tous les autres modules du système par le bus matériel. L'utilisation du module de plateforme sécurisée est le moyen le plus sûr de stocker des clés d'accès BitLocker, car ce module permet de vérifier l'intégrité du système avant le démarrage. Sur les ordinateurs sans TPM, vous pouvez également chiffrer des disques. Dans ce cas, la clé d'accès sera chiffrée à l'aide d'un mot de passe. Ainsi, BitLocker utilise les méthodes d'authentification suivantes :

- TPM.
- TPM et code PIN.
- Mot de passe.

Avant de chiffrer un disque, BitLocker crée une clé de récupération. Kaspersky Embedded Systems Security lit la clé de récupération et l'envoie à Kaspersky Security Center, ce qui vous permet de restaurer l'accès au disque si l'utilisateur a oublié le mot de passe, par exemple.

Après avoir chiffré le disque dur du système, l'utilisateur doit passer par l'authentification BitLocker pour lancer le système d'exploitation. Après l'authentification, BitLocker autorise l'utilisateur à se connecter. BitLocker n'est pas compatible avec la technologie d'authentification unique (SSO).

Si un utilisateur chiffre un disque à l'aide de BitLocker, Kaspersky Embedded Systems Security envoie à Kaspersky Security Center les informations sur le chiffrement du disque ainsi que la clé de récupération.

Si vous utilisez des stratégies de groupe pour Windows, désactivez l'administration de BitLocker dans les paramètres de la stratégie. Les paramètres de la stratégie Windows peuvent entrer en conflit avec les paramètres de la stratégie de Kaspersky Embedded Systems Security. Lors du chiffrement d'un disque, des erreurs peuvent se produire.

Lancement du chiffrement de disque BitLocker

Avant de lancer le chiffrement du disque, il est recommandé de s'assurer que l'ordinateur n'est pas infecté. Pour ce faire, lancez une analyse complète ou une analyse des zones critiques de l'ordinateur. Le chiffrement du disque sur un ordinateur infecté par un rootkit peut provoquer le dysfonctionnement de l'ordinateur.

Le fonctionnement de BitLocker sur des ordinateurs tournant sous un système d'exploitation Windows pour serveurs peut requérir l'installation du module BitLocker Drive Encryption. Installez le module à l'aide des outils du système d'exploitation (Assistant d'ajout de rôles et de fonctionnalités). Pour en savoir plus sur l'installation de Chiffrement de disque BitLocker, consultez la documentation Microsoft.

Comment exécuter le chiffrement de disque BitLocker dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Sélectionnez la section **Chiffrement des données**.
4. Dans la liste déroulante **Mode de chiffrement**, choisissez **Chiffrer tous les disques durs**.

   Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel le chiffrement a été réalisé peut être lancé après le chiffrement.

5. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).
6. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment exécuter le chiffrement de disque BitLocker dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.
   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données**.

5. Cliquez sur le bouton **Configurer** dans la sous-section **Chiffrement du disque**.

6. Dans la liste déroulante **Mode de chiffrement**, choisissez **Chiffrer tous les disques durs**.

   Si plusieurs systèmes d'exploitation sont installés sur l'ordinateur, seul le système d'exploitation dans lequel le chiffrement a été réalisé peut être lancé après le chiffrement.

7. Configurez les paramètres complémentaires de chiffrement de disque BitLocker (cf. tableau ci-dessous).

8. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Vous pouvez utiliser la Console de l'application pour contrôler le processus de chiffrement ou de déchiffrement du disque sur l'ordinateur d'un utilisateur.

Une fois la stratégie appliquée, en fonction des paramètres d'authentification, l'application affiche les requêtes suivantes dans la fenêtre Interface de diagnostic compacte ou dans la Console de l'application :

- TPM uniquement. Aucune entrée d'utilisateur n'est requise. Le disque sera chiffré au redémarrage de l'ordinateur.
- TPM + PIN / Mot de passe. En présence d'un module TPM, une fenêtre de saisie d'un code PIN s'ouvre. En l'absence d'un module TPM, une fenêtre de saisie de mot de passe pour l'identification avant le chargement s'ouvre.
- Mot de passe uniquement. Vous verrez une fenêtre d'invite de saisie de mot de passe pour l'authentification avant le démarrage.

Si la compatibilité avec la norme FIPS (norme fédérale de traitement de l'information) est activée dans le système d'exploitation, une fenêtre de demande de connexion d'un appareil de stockage de masse pour l'enregistrement du fichier de clé de récupération s'ouvre dans les systèmes d'exploitation Windows 8 et dans les versions antérieures. Vous pouvez enregistrer plusieurs fichiers de clés de récupération sur un seul appareil de stockage.

Une fois que vous avez défini un mot de passe ou un code PIN, BitLocker vous invite à redémarrer l'ordinateur de l'utilisateur afin de vérifier sa compatibilité avec BitLocker. Kaspersky Embedded Systems Security affiche une notification correspondante dans la fenêtre Interface de diagnostic compacte ou dans la Console de l'application. Ensuite, l'utilisateur doit passer par la procédure d'authentification BitLocker. Une fois la procédure d'authentification de BitLocker terminée, il faudra vous connecter. BitLocker commence le chiffrement du disque une fois le système d'exploitation chargé.

En l'absence d'accès aux clés du chiffrement, l'utilisateur peut demander la clé de récupération à l 'administrateur du réseau local de l'organisation (si la clé de la récupération n'avait pas été enregistrée sur l'appareil de stockage de masse ou si elle avait été perdue).

Paramètres du module Chiffrement de disque BitLocker

Paramètre	Description
Autoriser l'utilisation de l'authentification BitLocker qui requiert une saisie au clavier avant le démarrage sur les tablettes	L'utilisation d'une authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage, même si la plateforme ne dispose pas de cette possibilité (par exemple, claviers tactiles sur les tablettes). Le clavier tactile des tablettes n'est pas accessible dans cet environnement. Pour réaliser une authentification BitLocker sur de telles tablettes, l'utilisateur doit absolument connecter un clavier USB par exemple. Si la case est cochée, l'utilisation de l'authentification qui requiert une saisie au clavier dans l'environnement préalable au démarrage est autorisée. Il est recommandé d'utiliser ce paramètre uniquement pour les appareils qui, pendant le chargement préalable, disposent de modes alternatifs de saisie de données, par exemple un clavier USB en plus du clavier tactile. Si cette case est décochée, le chiffrement de disque BitLocker n'est pas possible sur les tablettes.
Utiliser le chiffrement au niveau matériel (Windows 8 et versions ultérieures)	Si la case est cochée, l'application adopte le chiffrement au niveau du matériel. Cela permet d'augmenter la vitesse du chiffrement et de réduire l'utilisation des ressources de l'ordinateur.
Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures)	La case active/désactive la fonction qui limite le secteur de chiffrement aux secteurs occupés du disque dur. Cette restriction permet de réduire la durée du chiffrement. L'activation ou la désactivation de la fonctionnalité **Chiffrer uniquement l'espace occupé (Windows 8 et versions ultérieures)** après le lancement du chiffrement ne modifie pas ce paramètre tant que les disques durs ne sont pas déchiffrés. Il faut cocher ou décocher la case avant le début du chiffrement. Si la case est cochée, seule la partie du disque dur qui contient des fichiers est chiffrée. Kaspersky Embedded Systems Security chiffre les nouvelles données automatiquement au fur et à mesure qu'elles sont ajoutées. Si la case est décochée, tout le disque dur est chiffré, y compris les restes des fichiers supprimés ou modifiés auparavant. Cette fonction est recommandée pour les nouveaux disques durs dont les données n'ont pas été modifiées ou supprimées. Si vous appliquez le chiffrement sur un disque dur déjà utilisé, il est conseillé de chiffrer tout le disque dur. Cela garantit la protection de toutes les données, mêmes celles qui ont été supprimées mais qui pourraient être restaurées. Par défaut, la case est décochée.

Paramètre	Description
Méthode d'authentification	**Trusted Platform Module (TPM)** Si vous avez choisi cette option, BitLocker utilise le Trusted Platform Module (TPM). Module de plateforme sécurisée (en anglais, Trusted Platform Module (TPM)) : puce développée pour proposer les fonctions principales associées à la sécurité (par exemple, pour stocker des clés de chiffrement). Le Trusted Platform Module s'installe en général sur la carte mère de l'ordinateur et interagit avec les autres modules système via le bus matériel. Pour les ordinateurs tournant sous les systèmes d'exploitation Windows 7 et Windows Server 2008 R2, seul le chiffrement à l'aide du module TPM est disponible. Si le module TPM n'est pas installé, le chiffrement BitLocker n'est pas possible. L'utilisation d'un mot de passe sur ces ordinateurs n'est pas prise en charge. L'appareil équipé du Trusted Platform Module peut créer des clés de chiffrement qui peuvent être déchiffrées uniquement à l'aide de celui-ci. Le Trusted Platform Module chiffre les clés de chiffrement à l'aide de la clé racine de stockage correspondante. La clé racine de stockage se trouve à l'intérieur du Trusted Platform Module. Cela offre un niveau de sécurité complémentaire pour les clés de chiffrement contre les tentatives d'attaque. Cette action est sélectionnée par défaut. Vous pouvez définir une couche de protection supplémentaire pour l'accès à la clé de chiffrement, et chiffrer la clé à l'aide d'un mot de passe ou d'un code PIN : **Utiliser un code PIN pour le TPM**. Quand la case est cochée, l'utilisateur doit saisir un code PIN pour accéder à la clé de chiffrement conservée dans le module de plateforme sécurisée (TPM). Si cette case n'est pas cochée, l'utilisateur n'est pas autorisé à utiliser le code PIN. Pour accéder à la clé de chiffrement, l'utilisateur utilise un mot de passe. **Trusted Platform Module (TPM) ou mot de passe si le TPM n'est pas disponible** Si cette option est sélectionnée, l'utilisateur peut accéder aux clés de chiffrement à l'aide d'un mot de passe en l'absence du Trusted Platform Module (TPM). Si la case n'est pas cochée et que le TPM n'est pas disponible, le chiffrement complet du disque ne démarre pas. **Mot de passe uniquement (Windows 8 et versions ultérieures)** Si vous avez choisi cette option, Kaspersky Embedded Systems Security demande le mot de passe à l'utilisateur lorsque celui-ci souhaite accéder au disque chiffré. Cette option peut être choisie si la Trusted Platform Module (TPM) n'est pas utilisée. La méthode d'authentification sélectionnée doit être configurée en précisant les exigences en matière de mot de passe ou de code PIN : • **Longueur minimale du code PIN (caractères)**. • **Utiliser un code PIN amélioré (lettres et chiffres)**. Le code PIN renforcé permet l'utilisation d'autres caractères en plus des caractères numériques : lettres latines majuscules et minuscules, caractères spéciaux et espaces. • **Longueur minimale du mot de passe (caractères)**. • **Limiter la durée de validité du mot de passe/code PIN pour le TPM (jours)**.
Recréer automatiquement la clé de récupération (jours)	Mettez automatiquement à jour le mot de passe pour restaurer l'accès à un disque protégé par BitLocker. Si la case est cochée, précisez la période de validité du mot de passe de la clé de récupération.

Déchiffrement d'un disque dur protégé par BitLocker

L'utilisateur peut déchiffrer indépendamment le disque à l'aide des outils du système d'exploitation (la fonction *Désactiver BitLocker*). Après cela, Kaspersky Embedded Systems Security vous invite à chiffrer de nouveau le disque. Kaspersky Embedded Systems Security proposera de chiffrer le disque jusqu'à ce que vous activiez le déchiffrement du disque dans la stratégie.

Comment déchiffrer un disque dur protégé par BitLocker à l'aide de la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Sélectionnez la section **Chiffrement des données**.

4. Dans la liste déroulante **Mode de chiffrement**, choisissez **Déchiffrer tous les disques durs**.
5. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Comment déchiffrer un disque dur protégé par BitLocker à l'aide de Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Passez à la section **Chiffrement des données**.
5. Cliquez sur le bouton **Configurer** dans la sous-section **Chiffrement du disque**.
6. Dans la liste déroulante **Mode de chiffrement**, choisissez **Déchiffrer tous les disques durs**.
7. Cliquez sur le bouton **OK** pour enregistrer les modifications.

Vous pouvez utiliser la Console de l'application pour contrôler le processus de chiffrement ou de déchiffrement du disque.

Restauration de l'accès au disque protégé par BitLocker

Si l'utilisateur a oublié le mot de passe d'accès au disque dur chiffré par BitLocker, il faut lancer la procédure de récupération (Requête-Réponse).

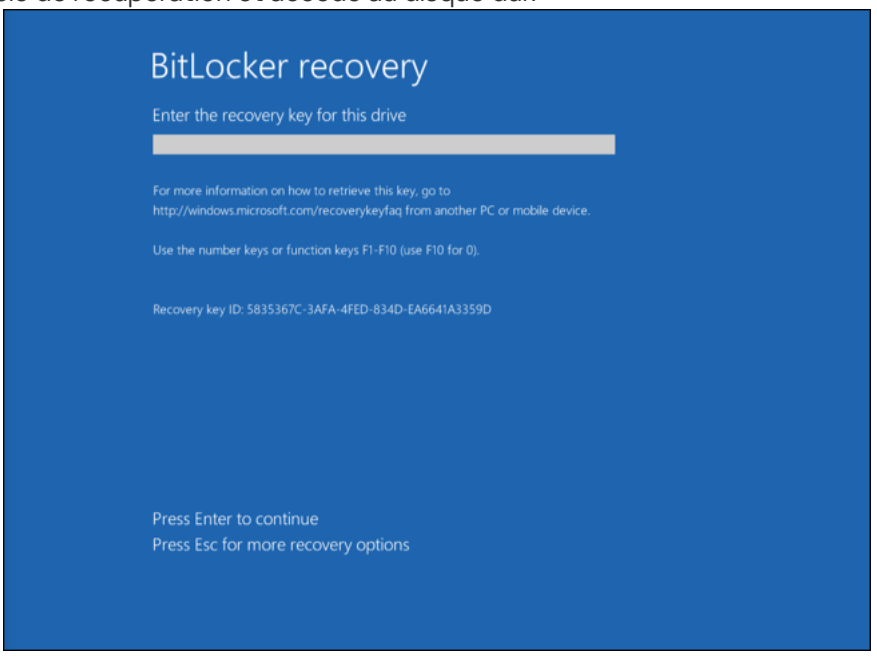
> Si le système d'exploitation prend en charge la norme FIPS (Federal Information Processing Standard), alors, dans les systèmes d'exploitation Windows 8 et antérieures, le fichier de clé de récupération aura été enregistré sur un disque amovible avant le chiffrement. Pour restaurer l'accès au disque, connectez le disque amovible et suivez les instructions à l'écran.

La restauration de l'accès au disque dur chiffré par BitLocker comprend les étapes suivantes :

1. L'utilisateur communique à l'administrateur l'identifiant de la clé de récupération (cf. figure ci-dessous).
2. L'administrateur vérifie l'identifiant de la clé de récupération dans les propriétés de l'ordinateur dans Kaspersky Security Center. L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant qui apparaît dans les propriétés de l'ordinateur.

   Si les identifiants des clés de récupération correspondent, l'administrateur remet la clé de récupération à l'utilisateur.

3. L'utilisateur saisit la clé de récupération et accède au disque dur.



Restauration de l'accès au disque dur chiffré à l'aide de BitLocker

Restauration de l'accès au disque système

Pour lancer la procédure de récupération, l'utilisateur doit appuyer sur la touche **Échap** lors de l'identification avant le chargement.

Comment consulter la clé de récupération pour un disque système chiffré à l'aide de BitLocker dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Appareils administrés**.
2. Rendez-vous dans l'onglet **Appareils**.
3. Ouvrez le menu contextuel de l'ordinateur de l'utilisateur qui a fait la demande de récupération de l'accès aux données chiffrées.
4. Sélectionnez **Autoriser l'accès en mode hors ligne** dans le menu contextuel.
5. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération** sous l'onglet **Accès au disque système avec protection BitLocker**.

   Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

6. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Comment consulter la clé de récupération pour un disque système chiffré à l'aide de BitLocker dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Ressources (Appareils)**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.
3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.
4. Vérifiez l'identifiant de la clé de récupération L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant repris dans les paramètres de l'ordinateur.

   Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

5. Cliquez sur **Obtenir la clé**.
6. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Après le chargement du système d'exploitation, Kaspersky Embedded Systems Security invite l'utilisateur à modifier le mot de passe ou le code PIN. Une fois que vous avez défini un nouveau mot de passe ou un nouveau code PIN, BitLocker génère un nouveau mot de passe de récupération, que l'application transmet à Kaspersky Security Center.

Restauration de l'accès à disque autre que le disque système

Pour lancer la procédure de récupération, l'utilisateur doit cliquer sur le lien **Forgot your password** dans la fenêtre d'accès au disque. Une fois que l'utilisateur a obtenu l'accès au lecteur chiffré, il peut activer le déverrouillage automatique du disque lors de l'authentification Windows dans les paramètres de BitLocker.

Comment consulter la clé de récupération pour un disque hors système chiffré à l'aide de BitLocker dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez le dossier **Avancé → Chiffrement et protection des données → Disques chiffrés**.
2. Dans l'espace de travail, sélectionnez l'appareil chiffré pour lequel vous souhaitez créer un fichier de clé d'accès, puis dans le menu contextuel de l'appareil, cliquez sur **Obtenir l'accès à l'appareil dans Kaspersky Embedded Systems Security**.
3. Demandez à l'utilisateur de fournir l'identifiant de clé de récupération qui apparaît dans la fenêtre de saisie du mot de passe de BitLocker et comparez-le à l'identifiant du champ **Identifiant de la clé de récupération**.

   Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

4. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Comment consulter la clé de récupération pour un disque hors système chiffré à l'aide de BitLocker dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Opérations → Chiffrement et protection des données → Disques chiffrés**.
2. Cochez la case en regard du nom de l'ordinateur dont vous souhaitez restaurer l'accès au disque.
3. Cliquez sur **Autoriser l'accès à l'appareil en mode déconnecté**.

   L'Assistant d'octroi de l'accès à l'appareil s'ouvre.
4. Suivez les instructions de l'Assistant d'octroi de l'accès à l'appareil.

   a. Sélectionnez le plug-in Kaspersky Embedded Systems Security.

   b. Vérifiez l'identifiant de la clé de récupération L'identifiant fourni par l'utilisateur doit correspondre à l'identifiant repris dans les paramètres de l'ordinateur.

   > Si les identifiants ne correspondent pas, cette clé ne convient pas pour restaurer l'accès au disque système indiqué. Confirmez que le nom de l'ordinateur choisi correspond au nom de l'ordinateur de l'utilisateur.

   c. Cliquez sur **Obtenir la clé**.
5. Transmettez à l'utilisateur la clé indiquée dans le champ **Clé de récupération**.

Interruption de la protection BitLocker pour mettre à jour un logiciel

Il existe un certain nombre de considérations particulières concernant la mise à jour du système d'exploitation, l'installation de paquets de mise à jour pour le système d'exploitation ou la mise à jour d'autres logiciels lorsque la protection BitLocker est activée. L'installation des mises à jour peut exiger le redémarrage de l'ordinateur à plusieurs reprises. Après chaque redémarrage, l'utilisateur doit procéder à l'authentification BitLocker. Pour vous assurer que les mises à jour s'installent correctement, vous pouvez désactiver temporairement l'authentification BitLocker. Dans ce cas, le disque reste chiffré et l'utilisateur a accès aux données après s'être connecté au système. Pour gérer l'authentification BitLocker, vous pouvez utiliser la tâche *Gestion de la protection BitLocker*. Vous pouvez utiliser cette tâche pour préciser le nombre de redémarrages de l'ordinateur qui ne nécessitent pas d'authentification BitLocker. De cette façon, une fois que les mises à jour sont installées et que la tâche *Gestion de la protection BitLocker* est terminée, l'authentification BitLocker est automatiquement activée. Vous pouvez activer l'authentification BitLocker à tout moment.

Comment interrompre la protection BitLocker dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Tâches**.

   La liste des tâches s'ouvre.
2. Cliquez sur **Nouvelle tâche**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Sélection du type de tâche

Choisissez **Kaspersky Embedded Systems Security for Windows (4.1)** → **Gestion de la protection BitLocker**.

Étape 2. Gestion de la protection BitLocker

Configurez l'authentification BitLocker. Pour interrompre la protection BitLocker, sélectionnez **Autoriser temporairement le contournement de l'authentification BitLocker** et saisissez le nombre de redémarrages sans authentification BitLocker (1 à 15 fois). Si nécessaire, saisissez une date et une heure d'expiration pour la tâche. À l'heure indiquée, la tâche est automatiquement désactivée, et l'utilisateur doit terminer l'authentification BitLocker lorsque l'ordinateur est redémarré.

Étape 3. Sélection des appareils auxquels la tâche va être affectée

Sélectionnez les ordinateurs sur lesquels la tâche va être exécutée. Les options suivantes existent :

- Attribuer une tâche à un groupe d'administration. Dans ce cas, la tâche est attribuée aux ordinateurs qui appartiennent au groupe d'administration créé antérieurement.
- Choisir les ordinateurs détectés dans le réseau par le Serveur d'administration – *les appareils non distribués*. L'ensemble d'appareils peut reprendre des appareils dans des groupes d'administration et des appareils non distribués.
- Définir les adresses des appareils manuellement ou les importer depuis une liste. Vous pouvez définir les noms NetBIOS, les adresses IP, ainsi que les plages d'adresses IP des appareils auxquels il faut attribuer la tâche.

Étape 4. Définition du nom de la tâche

Saisissez le nom de la tâche, par exemple *Mise à jour vers Windows 10*.

Étape 5. Fin de la création de la tâche

Quittez l'Assistant. Le cas échéant, cochez la case **&Lancer la tâche à la fin de l'Assistant**. Vous pouvez suivre la progression de l'exécution de la tâche dans les propriétés de celle-ci.

Interruption de la protection BitLocker à l'aide de Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources** → **Tâches**.

   La liste des tâches s'ouvre.

2. Cliquez sur **Ajouter**.

L'Assistant de création de tâche démarre. Suivez les instructions de l'Assistant.

Étape 1. Configuration des paramètres principaux de la tâche

Configurez les paramètres principaux de la tâche.

1. Dans la liste déroulante **Application**, sélectionnez **Kaspersky Embedded Systems Security**.
2. Dans la liste déroulante **Type de tâche**, choisissez **Gestion de la protection BitLocker**.
3. Dans le champ **Nom de la tâche**, saisissez une courte description, par exemple, *Mise à jour vers Windows 10*.
4. Dans le groupe **Appareils auxquels la tâche sera affectée**, sélectionnez la zone d'action de la tâche.

Étape 2. Gestion de la protection BitLocker

Configurez l'authentification BitLocker. Pour interrompre la protection BitLocker, sélectionnez **Autoriser temporairement le contournement de l'authentification BitLocker** et saisissez le nombre de redémarrages sans authentification BitLocker (1 à 15 fois). Si nécessaire, saisissez une date et une heure d'expiration pour la tâche. À l'heure indiquée, la tâche est automatiquement désactivée, et l'utilisateur doit terminer l'authentification BitLocker lorsque l'ordinateur est redémarré.

Étape 3. Fin de la création de la tâche

Quittez l'Assistant. La nouvelle tâche apparaît dans la liste des tâches.

Pour exécuter la tâche, cochez la case en regard de la tâche et cliquez sur le bouton **Démarrer**.

Ainsi, lorsque la tâche est en cours d'exécution, après le prochain redémarrage de l'ordinateur, BitLocker ne demande pas à l'utilisateur de s'authentifier. Après chaque redémarrage de l'ordinateur sans authentification BitLocker, Kaspersky Embedded Systems Security génère un événement correspondant et enregistre le nombre de redémarrages restants.

Lorsque le nombre de redémarrages indiqué ou le délai d'expiration de la tâche est atteint, l'authentification BitLocker est automatiquement activée. Pour accéder aux données, l'utilisateur doit procéder à une authentification BitLocker.

Sur les ordinateurs fonctionnant sous Windows 7, BitLocker ne peut pas compter les redémarrages de l'ordinateur. Le comptage des redémarrages sur les ordinateurs Windows 7 est géré par Kaspersky Embedded Systems Security. Ainsi, pour activer automatiquement l'authentification BitLocker après chaque redémarrage, Kaspersky Embedded Systems Security doit être démarré.

Pour activer l'authentification BitLocker à l'avance, ouvrez les propriétés de la tâche *Gestion de la protection BitLocker* et sélectionnez **Demander une authentification à chaque fois en pré-lancement**.

Intégration aux systèmes tiers

Cette section décrit l'intégration de Kaspersky Embedded Systems Security aux fonctions et technologies tierces.

Compteurs de performance pour l'application Moniteur système

Compteurs de performance est un module de Kaspersky Embedded Systems Security que vous pouvez utiliser pour surveiller les performances des applications pendant le fonctionnement des modules de protection. Kaspersky Embedded Systems Security enregistre les compteurs de performance lors de l'installation.

Il est possible de consulter les compteurs de performance de l'application à l'aide de l'application « Moniteur système », disponible dans le panneau de configuration Windows. Pour en savoir plus sur l'utilisation des compteurs de performance, consultez le site Internet du Support technique de Microsoft.

Grâce aux compteurs de performances, vous pouvez, par exemple, détecter les pénuries de ressources lorsque Kaspersky Embedded Systems Security s'exécute en même temps que d'autres applications, ainsi que diagnostiquer les plantages et identifier les paramètres inappropriés de Kaspersky Embedded Systems Security.

Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)

Nombre de requêtes non traitées en raison d'un manque de ressources système (Number of requests not processed due to lack of resources)

Description	Total de requêtes du pilote d'intercepteur de fichiers non traitées en raison d'un manque de ressources système (par exemple, mémoire vive) ; le décompte s'opère depuis la dernière exécution de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security ignore les requêtes de traitement d'objet qui ne sont pas traitées par le pilote d'interception de fichiers.
Fonction	Le compteur permet de repérer et de résoudre une éventuelle baisse de la qualité de la Protection en temps réel de l'ordinateur provoquée par un manque de ressources.
Valeur normale / seuil	0 / 1
Intervalle de calcul des relevés recommandé	1 heure.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si le compteur affiche une valeur différente de zéro, le processus de Kaspersky Embedded Systems Security a besoin de plus de mémoire vive pour traiter les requêtes. Il se peut que les processus actifs d'autres applications utilisent toute la mémoire vive disponible.

Nombre de requêtes soumises pour traitement

Nombre de requêtes soumises pour traitement

Description	Nombre d'objets en attente de traitement par les processus actifs.
Fonction	Le compteur permet de surveiller la charge des processus de travail de Kaspersky Embedded Systems Security et le niveau général de l'activité de fichiers sur l'appareil protégé.
Valeur normale / seuil	La valeur du compteur peut varier en fonction du niveau d'activité fichier sur l'appareil protégé.
Intervalle de calcul des relevés recommandé	Une minute.
Recommandation pour la configuration si la valeur dépasse la valeur limite	S/O

Nombre d'objets traités par seconde

Nombre d'objets traités par seconde

Description	Nombre d'objets traités par unité de temps pendant laquelle ces objets ont été traités ; le décompte s'opère sur des intervalles de temps égaux
Fonction	Ce compteur affiche la vitesse de traitement des objets ; il permet d'identifier une baisse des performances de l'appareil protégé en raison d'un manque de temps de processeur actif pour le processus de Kaspersky Embedded Systems Security ou d'erreurs de fonctionnement de Kaspersky Embedded Systems Security et d'y remédier.
Valeur normale / seuil	Varie / non.
Intervalle de calcul des relevés recommandé	Une minute.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Les valeurs du compteur dépendent des paramètres définies dans Kaspersky Embedded Systems Security et de la charge des processus des autres applications sur l'appareil protégé. Observez le niveau moyen du compteur au cours d'une longue période. Si la valeur moyenne du compteur diminue, c'est peut-être à cause de l'une des situations suivantes : • Le processus de Kaspersky Embedded Systems Security ne dispose pas des ressources de processeur suffisantes pour traiter les objets. Accordez à Kaspersky Embedded Systems Security plus de temps de processeur, par exemple en réduisant la charge des autres applications sur l'appareil protégé. • Un échec s'est produit dans le fonctionnement de Kaspersky Embedded Systems Security (plusieurs flux sont gelés). Relancez Kaspersky Embedded Systems Security.

Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)

Nombre d'éléments dans la file d'attente des objets infectés (Number of elements in the infected objects queue)

Description	Nombre d'objets infectés attendant d'être traités (réparation ou suppression) en ce moment.
Fonction	Ce compteur permet d'identifier : • Interruption de la protection en temps réel de l'ordinateur en raison d'échecs potentiels des gestionnaires d'interception de fichier. • Surcharge des processus suite à une répartition inégale du temps de processeur entre différents processus de travail et Kaspersky Embedded Systems Security. • Les épidémies de virus.
Valeur normale / seuil	La valeur du compteur peut être différente de zéro tant que Kaspersky Embedded Systems Security traite les objets probablement infectés ou infectés découverts mais elle revient sur zéro juste après le traitement / La valeur du compteur est différente de zéro pendant une longue période.

Intervalle de calcul des relevés recommandé	Une minute.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur n'est pas égale à zéro pendant une longue période : • Kaspersky Embedded Systems Security ne traite pas les objets (il se peut que le gestionnaire d'intercepteurs de fichiers soit en échec) ; Relancez Kaspersky Embedded Systems Security. • Il peut ne pas y avoir assez de temps de processeur pour traiter les objets. Accordez à Kaspersky Embedded Systems Security plus de temps de processeur, par exemple en réduisant la charge des autres applications sur l'appareil protégé. • Une épidémie de virus s'est déclenchée. L'émergence d'une épidémie de virus est également indiquée par le nombre élevé d'objets infectés ou probablement infectés découverts dans le module Protection des fichiers en temps réel. Les informations relatives au nombre d'objets détectés figurent dans les statistiques du module ou dans le journal d'exécution du module.

Total de requêtes rejetées (Total number of requests denied)

Total de requêtes rejetées (Total number of requests denied)

Description	**Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui n'ont pas été acceptées par les processus de l'application, le calcul est réalisé depuis la dernière exécution de Kaspersky Embedded Systems Security.** **L'application ignore les objets dont les requêtes de traitement sont rejetées par les processus de Kaspersky Embedded Systems Security.**
Fonction	Ce compteur permet d'identifier : • Protection en temps réel de l'ordinateur réduite en raison d'une surcharge des processus de Kaspersky Embedded Systems Security. • Interruption de la protection en temps réel de l'ordinateur en raison d'échecs des gestionnaires d'interception de fichier.
Valeur normale / seuil	0 / 1
Intervalle de calcul des relevés recommandé	1 heure.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Le nombre de requêtes de traitement rejetées correspond au nombre d'objets ignorés. Les situations suivantes sont envisageables en fonction du "comportement" du compteur : • Le compteur indique que plusieurs demandes ont été rejetées pendant un certain temps : le processus de Kaspersky Embedded Systems Security fonctionnait au maximum de sa capacité. L'application n'a pas pu analyser les objets. Pour éviter que des objets ne soient ignorés, augmentez les ressources système allouées à l'application. • Le nombre de requêtes rejetées est bien supérieur au seuil critique et augmente rapidement : échec du gestionnaire d'intercepteurs de fichiers. Kaspersky Embedded Systems Security n'analyse pas les objets à l'accès. Relancez Kaspersky Embedded Systems Security.

Total de requêtes ignorées (Total number of requests skipped).

Total de requêtes ignorées (Total number of requests skipped).

Description	Total de requêtes du pilote des intercepteurs de fichiers pour le traitement des objets qui ont été acceptées par Kaspersky Embedded Systems Security et qui n'ont pas généré d'événement sur la fin du traitement, ce nombre est calculé depuis la dernière exécution de l'application. Si une requête de traitement d'un objet est acceptée par un des processus de travail, mais n'envoie pas un événement signalant que le traitement est terminé, le pilote transmet cette requête à un autre processus et la valeur du compteur **Total des requêtes ignorées** augmente d'une unité. Si le pilote a utilisé tous les processus et qu'aucun d'eux n'a accepté la requête de traitement (ils étaient occupés) ou n'a envoyé d'événement indiquant que le traitement est terminé, Kaspersky Embedded Systems Security ignore cet objet, et la valeur du compteur **Total des requêtes rejetées** augmente d'une unité.
Fonction	Ce compteur permet d'identifier un recul des performances en raison d'un arrêt des flux du gestionnaire des intercepteurs de fichiers.
Valeur normale / seuil	0 / 1

Intervalle de calcul des relevés recommandé	1 heure.
Recommandation pour la configuration si la valeur dépasse la valeur limite	Si la valeur du compteur diffère de zéro, cela signifie qu'un ou plusieurs flux du gestionnaire d'intercepteurs de fichiers sont gelés. La valeur du compteur correspond au nombre de flux gelés en ce moment. Si la vitesse d'analyse n'est pas satisfaisante, redémarrez Kaspersky Embedded Systems Security afin de rétablir les flux gelés.

Nombre maximum de flux du gestionnaire d'intercepteurs de fichiers

Depuis la version 4.1 de Kaspersky Embedded Systems Security, le compteur « Nombre maximal de flux du répartiteur d'interception de fichiers » n'est pas pris en charge.

Nombre moyen de flux du gestionnaire d'intercepteurs de fichiers

Depuis la version 4.1 de Kaspersky Embedded Systems Security, le compteur « Nombre moyen de flux du répartiteur d'interception de fichiers » n'est pas pris en charge.

Compteurs et interruptions SNMP de Kaspersky Embedded Systems Security

Si vous avez inclus le module Prise en charge du protocole SNMP dans les modules antivirus à installer, vous pouvez consulter les compteurs et les interruptions de Kaspersky Embedded Systems Security à l'aide du protocole Simple Network Management Protocol (SNMP).

Pour consulter les compteurs et les interruptions de Kaspersky Embedded Systems Security depuis le poste de travail de l'administrateur, lancez sur l'appareil protégé le service SNMP (SNMP Service) et le service d'interruptions SNMP (SNMP Trap Service) ainsi que le service SNMP (SNMP Service) sur le poste de travail de l'administrateur.

Compteurs SNMP de Kaspersky Embedded Systems Security

Cette section contient des tableaux décrivant les paramètres des compteurs SNMP de Kaspersky Embedded Systems Security.

Compteurs de performance

Compteurs de performance

Compteur	Définition
currentRequestsAmount	Nombre de requêtes soumises pour traitement
currentInfectedQueueLength	Nombre d'éléments dans la file d'attente des objets infectés
currentObjectProcessingRate	Nombre d'objets traités par seconde
currentWorkProcessesNumber	Nombre actuel de processus de travail utilisés par Kaspersky Embedded Systems Security

Compteur de sauvegarde

Compteur de sauvegarde

Compteur	Définition
currentBackupStorageSize	Volume total de données en sauvegarde (Mo)

Compteurs généraux

Compteurs généraux

Compteur	Définition
lastCriticalAreasScanAge	Intervalle de temps, en secondes, écoulé depuis la fin de la tâche *Analyse des zones critiques*.
licenseExpirationDate	Date d'expiration de la licence. Si des clés active et additionnelle ont été ajoutées, la date affichée est la date d'échéance de la licence associée à la clé additionnelle.
currentApplicationUptime	Durée de fonctionnement de Kaspersky Embedded Systems Security depuis sa dernière exécution (en centièmes de secondes).

Compteur de mise à jour

Compteur de mise à jour

Compteur	Définition
avBasesAge	Temps écoulé, en centièmes de seconde, depuis la date de création des dernières mises à jour des bases de données installées.

Compteurs de Protection des fichiers en temps réel

Compteurs de Protection des fichiers en temps réel

Compteur	Définition
totalObjectsProcessed	Nombre total d'objets analysés depuis le dernier lancement du module Protection des fichiers en temps réel
totalInfectedObjectsFound	Nombre total d'objets infectés ou autres détectés depuis le dernier lancement du module Protection des fichiers en temps réel
totalSuspiciousObjectsFound	Nombre total d'objets probablement infectés détectés depuis le dernier lancement du module Protection des fichiers en temps réel
totalVirusesFound	Nombre total d'objets détectés depuis le dernier lancement du module Protection des fichiers en temps réel

Compteur	Définition
totalObjectsQuarantined	Nombre total d'objets infectés, probablement infectés ou autres placés en quarantaine par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsNotQuarantined	Nombre total d'objets infectés ou probablement infectés que Kaspersky Embedded Systems Security a tenté de placer en quarantaine en vain ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsDisinfected	Nombre total d'objets infectés désinfectés par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsNotDisinfected	Nombre total d'objets infectés ou autres que Kaspersky Embedded Systems Security a tenté de désinfecter en vain ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsDeleted	Nombre total d'objets infectés, probablement infectés ou autres supprimés par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsNotDeleted	Nombre total d'objets infectés, probablement infectés ou autres que Kaspersky Embedded Systems Security a tenté de supprimer en vain ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsBackedUp	Nombre total d'objets infectés ou autres placés dans la Sauvegarde par Kaspersky Embedded Systems Security ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
totalObjectsNotBackedUp	Nombre total d'objets infectés ou autres que Kaspersky Embedded Systems Security a tenté de placer dans la Sauvegarde en vain ; ce nombre est calculé depuis le dernier lancement du module Protection des fichiers en temps réel
currentFileMonitorTaskStatus	État du module Protection des fichiers en temps réel : • `1` signifie que le module est activé et assure la protection. • `0` signifie que le module n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.

Compteurs du Scanner AMSI

Compteurs du Scanner AMSI

Compteur	Définition
currentScriptCheckerTaskStatus	État du module Scanner AMSI : • `1` signifie que le module est activé et assure la protection. • `0` signifie que le module n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.
totalScriptsProcessed	Nombre de scripts traités depuis le dernier lancement du module Scanner AMSI.
totalInfectedlDangerousScriptsFound	Nombre de scripts dangereux détectés depuis le dernier lancement du module Scanner AMSI.
totalSuspiciousScriptsFound	Nombre total de scripts suspects détectés depuis le dernier lancement du module Scanner AMSI.
totalScriptsBlocked	Nombre total de scripts bloqués depuis le dernier lancement du module Scanner AMSI. La valeur du compteur change si le module est activé dans **Bloquer** et est égale à la valeur du compteur totalInfectedlDangerousScriptsFound.

Interruptions SNMP de Kaspersky Embedded Systems Security et leur option

Les options des interruptions SNMP de Kaspersky Embedded Systems Security sont résumées comme suit :

- eventThreatDetected : Objet détecté.

Les options d'interruptions sont les suivantes :

- eventDateAndTime
- eventSeverity
- computerName
- userName
- objectName
- threatName
- detectType
- detectCertainty

- eventBackupStorageSizeExceeds : Dépassement de la taille maximale de la sauvegarde. La quantité totale de données dans la Sauvegarde dépasse la valeur spécifiée par **Limiter la taille de la sauvegarde à**. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds : Dépassement du seuil d'espace disponible dans la sauvegarde. La quantité d'espace libre dans la Sauvegarde est inférieure ou égale à la valeur spécifiée par **Valeur du seuil de l'espace disponible (Mo)**. Kaspersky Embedded Systems Security poursuit la mise en sauvegarde des objets infectés.

  Les options d'interruptions sont les suivantes :

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotBackuped : Objet non sauvegardé.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName

- computerName
- storageObjectNotAddedEventReason

- eventBackupInternalError : erreur de sauvegarde.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated : Les bases sont dépassées. Nombre de jours écoulés depuis la dernière exécution de la tâche *Mise à jour* (tâche locale, tâche de groupe ou tâche pour les sélections d'appareils protégés).

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated : Les bases sont fortement dépassées. Nombre de jours écoulés depuis la dernière exécution de la tâche *Mise à jour* (tâche locale, tâche de groupe ou tâche pour les sélections d'appareils protégés).

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted : L'application a été lancée.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown : L'application a été arrêtée.

Les options d'interruptions sont les suivantes :

- eventSeverity
- eventDateAndTime
- eventSource

- eventCriticalAreasScanWasntPerformForALongTime : Analyse des zones critiques non réalisée depuis longtemps. Nombre de jours écoulés depuis la dernière exécution de la tâche *Analyse des zones critiques*.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired : La licence a expiré.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon : La licence expire bientôt. Le nombre de jour restant avant la fin de la validité de la licence est compté

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError : erreur d'exécution de la tâche.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode

- knowledgeBaseId
- taskName

- eventUpdateError : erreur lors de l'exécution de la tâche *Mise à jour*.

  Les options d'interruptions sont les suivantes :

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason
  - eventSource

Descriptions et valeurs possibles des options d'interruptions SNMP de Kaspersky Embedded Systems Security

Les descriptions des options d'interruption et valeurs possibles des paramètres sont reprises ci-après :

- eventDateAndTime : date et heure de l'événement
- eventSeverity : niveau d'importance

  L'option peut prendre les valeurs suivantes :

  - critical (1) – critique
  - warning (2) – avertissement
  - info (3) – informations
- userName : nom d'utilisateur (par exemple, nom de l'utilisateur qui a tenté d'accéder à un fichier infecté).
- computerName : nom de l'appareil protégé (par exemple, nom de l'appareil protégé depuis lequel un utilisateur a tenté d'accéder à un fichier infecté).
- eventSource : module fonctionnel qui a généré l'événement.

  L'option peut prendre les valeurs suivantes :

  - unknown (0) – Module fonctionnel inconnu
  - quarantine (1) – Quarantaine
  - backup (2) – Sauvegarde
  - reporting (3) – Journaux d'exécution des tâches
  - updates (4) – Mise à jour
  - realTimeProtection (5) – Protection des fichiers en temps réel

- onDemandScanning (6) – Analyse à la demande
- product (7) – événement lié au fonctionnement de Kaspersky Embedded Systems Security dans son ensemble plutôt qu'au fonctionnement de ses différents modules
- systemAudit (8) – Journal d'audit système

- eventReason : déclencheur de l'événement : cause de l'événement.

  L'option peut prendre les valeurs suivantes :

  - reasonUnknown (0) – cause indéterminée.
  - reasonInvalidSettings (1) – uniquement pour les événements de sauvegarde et de quarantaine. S'affiche si le dossier Quarantaine ou Sauvegarde est indisponible (autorisations d'accès insuffisantes ou dossier non valide spécifié dans les paramètres de quarantaine, par exemple, spécification d'un chemin réseau). Dans ce cas, Kaspersky Embedded Systems Security utilise le dossier de sauvegarde ou de quarantaine indiqué par défaut.

- objectName : nom de l'objet (par exemple, nom du fichier dans lequel le virus a été détecté).
- threatName : nom de l'objet selon la classification de l'Encyclopédie des virus. Ce nom figure dans le nom complet que Kaspersky Embedded Systems Security renvoie suite à la détection de l'objet. Vous pouvez consulter le nom complet de l'objet détecté dans le journal d'exécution de la tâche.
- detectType : type d'objet détecté.

  L'option peut prendre les valeurs suivantes :

  - undefined (0) – Non défini
  - virware – Virus et vers de réseau traditionnels
  - trojware – Chevaux de Troie
  - malware – Autres applications malveillantes
  - adware – Logiciels publicitaires
  - pornware – Logiciels à caractère pornographique
  - riskware – Applications légitimes pouvant être utilisées par des individus malintentionnés pour endommager l'appareil ou les données personnelles de l'utilisateur

- detectCertainty : coefficient de certitude pour la détection d'une menace.

  L'option peut prendre les valeurs suivantes :

  - Suspicion (probablement infecté) – Kaspersky Embedded Systems Security a détecté une correspondance partielle entre une section du code de l'objet et une section connue de code malveillant.
  - Sure (infecté) – Kaspersky Embedded Systems Security a détecté une correspondance complète entre une section du code de l'objet et une section connue de code malveillant.

- days : nombre de jours (par exemple, nombre de jours avant la date d'expiration de la licence).
- errorCode : code d'erreur.

- taskName : nom de la tâche.
- updaterErrorEventReason : cause de l'erreur de mise à jour.

  L'option peut prendre les valeurs suivantes :

  - reasonUnknown (0) – cause indéterminée.
  - reasonAccessDenied – accès refusé.
  - reasonUrlsExhausted – la liste des sources de mise à jour est épuisée.
  - reasonInvalidConfig – fichier de configuration incorrect.
  - reasonInvalidSignature – signature non valide.
  - reasonCantCreateFolder – création du répertoire impossible.
  - reasonFileOperError – erreur de fichier.
  - reasonDataCorrupted – objet endommagé.
  - reasonConnectionReset – connexion réinitialisée.
  - reasonTimeOut – délai d'attente de la connexion expiré.
  - reasonProxyAuthError – erreur d'authentification sur le serveur proxy.
  - reasonServerAuthError – erreur d'authentification sur le serveur.
  - reasonHostNotFound – appareil introuvable.
  - reasonServerBusy – serveur indisponible.
  - reasonConnectionError – erreur de connexion.
  - reasonModuleNotFound – objet introuvable.
  - reasonBlstCheckFailed (16) – erreur lors de la vérification de la liste de refus des clés. Il se peut qu'une mise à jour des bases de l'application ait été diffusée au moment de la mise à jour. Essayez à nouveau de réaliser la mise à jour dans quelques minutes.
- storageObjectNotAthreatddedEventReason : cause du non-placement de l'objet dans la Sauvegarde ou en quarantaine.

  L'option peut prendre les valeurs suivantes :

  - reasonUnknown (0) – cause indéterminée.
  - reasonStorageInternalError – erreur de base de données ; Kaspersky Embedded Systems Security doit être restauré.
  - reasonStorageReadOnly – la base de données est en lecture seule ; Kaspersky Embedded Systems Security doit être restauré.

- reasonStorageIOError – erreur d'entrées-sorties : a) Kaspersky Embedded Systems Security est endommagé et doit être restauré ; b) le disque sur lequel les fichiers de Kaspersky Embedded Systems Security sont stockés est endommagé.
- reasonStorageCorrupted – le stockage est endommagé ; Kaspersky Embedded Systems Security doit être restauré.
- reasonStorageFull – la base de données est pleine ; de l'espace disque doit être libéré.
- reasonStorageOpenError – impossible d'ouvrir le fichier de base de données ; Kaspersky Embedded Systems Security doit être restauré.
- reasonStorageOSFeatureError – certaines fonctionnalités du système d'exploitation ne répondent pas aux exigences de Kaspersky Embedded Systems Security.
- reasonObjectNotFound – l'objet en cours de placement en quarantaine n'existe pas sur le disque.
- reasonObjectAccessError – autorisations insuffisantes pour utiliser l'API de sauvegarde : le compte utilisé pour effectuer l'opération ne dispose pas des autorisations d'opérateur de sauvegarde.
- reasonDiskOutOfSpace – espace insuffisant sur le disque.

Intégration de WMI

Kaspersky Embedded Systems Security prend en charge l'intégration à Windows Management Instrumentation (WMI) : vous pouvez utiliser les systèmes clients qui emploient WMI pour recevoir des données via la norme Web-Based Enterprise Management (WBEM) afin d'obtenir des informations sur l'état de Kaspersky Embedded Systems Security et de ses modules.

Une fois installé, Kaspersky Embedded Systems Security enregistre un module exclusif dans le système afin de créer un espace de noms Kaspersky Embedded Systems Security sur l'appareil protégé. Un espace de noms Kaspersky Embedded Systems Security vous permet d'utiliser des catégories et des instances Kaspersky Embedded Systems Security et leurs propriétés.

Les valeurs de certaines propriétés d'instance dépendent des types de tâche.

Une *tâche non périodique* est une tâche d'application qui n'est pas limitée dans le temps et qui peut être exécutée en permanence ou arrêtée. Ces tâches n'affichent pas la progression de l'exécution. Les résultats de la tâche sont enregistrés en continu pendant l'exécution de la tâche en tant qu'événements uniques (par exemple, détection d'un objet infecté par une tâche quelconque de Protection en temps réel de l'ordinateur). Ce type de tâche est administré via les stratégies de Kaspersky Security Center.

Une *tâche périodique* est une tâche d'application limitée dans le temps et dont la progression de l'exécution est affichée en pourcentage. Les résultats de la tâche sont générés quand la tâche est terminée et sont représentés en tant qu'élément unique ou qu'état modifié de l'application (par exemple, mise à jour des bases de l'application terminée, fichiers de configuration créés pour les tâches de création de règles). Plusieurs tâches périodiques du même type peuvent être exécutées simultanément sur un seul appareil protégé (par exemple, trois tâches d'analyse à la demande avec différentes zones d'analyse). Les tâches périodiques peuvent être administrées via Kaspersky Security Center en tant que tâches de groupe.

Si vous créez les requêtes d'espace de noms WMI à l'aide d'outils et si vous recevez les données dynamiques depuis les espaces de noms WMI sur votre réseau d'entreprise, vous pourrez obtenir les informations relatives à l'état actuel de l'application (cf. tableau ci-dessous).

Propriété de l'instance	Description	Valeurs
`ProductName`	Nom de l'application installée.	Nom complet de l'application sans le numéro de version.
`ProductVersion`	Numéro de version complet de l'application installée.	Numéro de version de l'application complet, avec le numéro de build.
`InstalledPatches`	Ensemble des noms affichés pour les correctifs installés.	Liste des correctifs critiques installés pour l'application.
`IsLicenseInstalled`	État de l'activation de l'application.	État de la clé utilisée pour activer l'application. Valeurs possibles : • `False` Aucune clé de licence n'a été ajoutée. • `True` Une clé de licence a été ajoutée.
`LicenseDaysLeft`	Affiche le nombre de jours restants avant l'expiration de la licence en cours.	Nombre de jour restants avant l'expiration de la licence en cours; Valeurs non positives possibles : • `0` La licence a expiré. • `-1` Impossible d'obtenir des informations sur la clé active ou la clé indiquée ne peut pas être utilisée pour activer l'application (par exemple, elle est bloquée sur la base d'une liste de refus de clés).
`AVBasesDatetime`	L'horodatage de la version actuelle des bases antivirus.	Date et heure de création des bases antivirus actuelles. Si l'application installée n'utilise pas de bases antivirus, le champ affiche la valeur `{Not installed}`.
`IsExploitPreventionEnabled`	État du module Protection contre les Exploits.	État du module Protection contre les Exploits. Valeurs possibles : • `True` Le module Protection contre les Exploits est activé et assure la protection. • `False` Le module Protection contre les Exploits n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.
`ProtectionTasksRunning`	L'ensemble des tâches de protection en cours d'exécution.	Liste des tâches de protection, de contrôle et de surveillance en cours d'exécution. Ce champ doit tenir compte de toutes les tâches non périodiques en cours d'exécution. Si aucune tâche non périodique n'est en cours d'exécution, le champ affiche la valeur `{No}`.
`IsAppControlRunning`	État du module Contrôle du lancement des applications.	Valeurs possibles • `True` Le module Contrôle du lancement des applications est activé et assure la protection. • `False` Le module Contrôle du lancement des applications n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.
`AppControlMode`	Mode de fonctionnement du module Contrôle du lancement des applications.	Valeurs possibles : • `Active` Le mode **Bloquer** est défini dans les paramètres du module. • `Statistics Only` Le mode **Informer** est défini dans les paramètres du module. • `Not installed` Le module Contrôle du lancement des applications n'est pas installé. • `Unknown` Le module est désactivé.
`AppControlRulesNumber`	Nombre total de règles du contrôle du lancement des applications.	Nombre de règles actuellement définies dans les paramètres du module Contrôle du lancement des applications.
`AppControlLastBlocking`	Horodatage de la dernière interdiction de lancement d'une application par le module Contrôle du lancement des applications, quel que soit son mode de fonctionnement.	Date et heure de la dernière interdiction de lancement d'une application par le module Contrôle du lancement des applications. Ce champ reprend toutes les applications bloquées, quel que soit le mode de fonctionnement du module. Si aucune interdiction de lancement d'une application n'est enregistrée au moment du traitement de la requête WMI, le champ affiche la valeur `{No}`.

Propriété de l'instance	Description	Valeurs
`PeriodicTasksRunning`	L'ensemble des tâches de périodiques en cours d'exécution.	Liste des tâches d'analyse à la demande, de mise à jour et d'inventaire en cours d'exécution. Ce champ doit contenir toutes les tâches périodiques en cours d'exécution. Si aucune tâche périodique n'est en cours d'exécution, le champ affiche la valeur `{No}`.
`ConnectionState`	État de la connexion entre le module WMI Provider et le service Kaspersky Embedded Systems Security Service.	Informations relatives à l'état de la connexion entre le module WMI Provider et le service Kaspersky Embedded Systems Security Service. Valeurs possibles : • `Success` La connexion a été établie avec succès : le client WMI peut recevoir l'état de l'application. • `Failed. Error Code: <code>` La connexion n'a pas pu être établie en raison d'une erreur portant le code indiqué.
`IsDumpingEnabled`	État de l'enregistrement du vidage mémoire.	Valeurs possibles • `True` L'enregistrement du vidage mémoire est activé. • `False` L'enregistrement du vidage mémoire est désactivé.
`DumpsFolder`	Dossier de stockage des fichiers de vidage.	Chemin d'accès complet au dossier. Si l'enregistrement du vidage est désactivé, ce champ est vide.
`IsTracingEnabled`	État du traçage de l'application.	Valeurs possibles • `True` Le traçage de l'application est activé. • `False` Le traçage de l'application est désactivé.
`TraceFolder`	Dossier de stockage des fichiers de traçage.	Chemin d'accès complet au dossier. Si le traçage de l'application est désactivé, ce champ est vide.
`AllTasksState`	État de toutes les tâches.	Informations sur l'état des tâches au format `{<profile-name_1>, <profile-type_1>, <profile-state_1>,... <profile-name_N>, <profile-type_N>, <profile-state_N>}`, où `profile-name` correspond au nom de la tâche, `profile-type` au type de la tâche et `profile-state` à l'état actuel de la tâche. Valeurs d'état possibles : • `not started` La tâche n'a pas encore démarré. • `running` La tâche est en cours d'exécution. • `running ma` La tâche est en cours d'exécution, mais une erreur s'est produite lors de son exécution. • `paused` La tâche est suspendue. • `stopped` La tâche est arrêtée. • `completed` La tâche s'est terminée avec succès. • `failed` La tâche s'est terminée avec une erreur. • `disabled` La tâche est désactivée et ne peut pas être exécutée. • `starting` La tâche est en cours de démarrage. • `pausing` La tâche est en cours de suspension. • `stopping` La tâche est en cours d'arrêt. • `<unknown>` Impossible de déterminer l'état.
`IsDevControlRunning`	État du module Contrôle des appareils.	Valeurs possibles : • `True` Le module Contrôle des appareils est activé et assure la protection. • `False` Le module Contrôle des appareils n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.
`IsKSNRunning`	État du module Kaspersky Security Network.	Valeurs possibles : • `True` Le module Kaspersky Security Network est activé et assure la protection. • `False` Le module Kaspersky Security Network n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.

Propriété de l'instance	Description	Valeurs
`IsOASRunning`	État du module Protection des fichiers en temps réel.	Valeurs possibles : • `True` Le module Protection des fichiers en temps réel est activé et assure la protection. • `False` Le module Protection des fichiers en temps réel n'assure pas la protection. Par exemple : désactivé, pas installé, violation du Contrat de licence.

Ces données représentent les propriétés de l'instance `KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security`, où :

- `KasperskySecurity_ProductInfo` est le nom de la classe Kaspersky Embedded Systems Security.
- `.ProductName=Kaspersky Embedded Systems Security` sont des propriétés clés de Kaspersky Embedded Systems Security.

La classe est instanciée dans l'espace de noms `ROOT\Kaspersky\Security`.

Managed Detection and Response

Kaspersky Embedded Systems Security prend en charge l'intégration avec la solution Managed Detection and Response.

Kaspersky Managed Detection and Response (également appelé MDR) offre une protection 24 heures sur 24 contre le volume croissant de menaces qui contournent les barrières de sécurité automatisées aux organisations qui peinent à trouver l'expertise et le personnel ou qui possèdent des ressources internes limitées. Contrairement aux offres similaires disponibles sur le marché, ce service s'appuie sur une expérience éprouvée en matière de recherche efficace sur les attaques ciblées afin d'assurer une défense continue contre les menaces les plus complexes. Ce service contribue à améliorer la résilience de votre entreprise face aux cybermenaces, tout en libérant vos ressources existantes afin qu'elles puissent se concentrer sur d'autres tâches.

MDR utilise les données de télémétrie reçues des terminaux et Machine learning. MDR envoie les données de l'incident aux experts de Kaspersky. Les experts peuvent alors traiter l'incident et, par exemple, ajouter une nouvelle entrée dans les bases antivirus. Les experts peuvent également émettre des recommandations sur le traitement de l'incident et, par exemple, suggérer d'isoler l'ordinateur du réseau. Pour en savoir plus à propos du fonctionnement de la solution, veuillez consulter l'aide de Kaspersky Managed Detection and Response.

Configuration de l'intégration MDR

L'intégration avec Kaspersky Managed Detection and Response comprend les étapes suivantes :

1. **Installation du module Managed Detection and Response**

   Le module Managed Detection and Response est utilisé pour l'intégration de Kaspersky Embedded Systems Security à la solution Managed Detection and Response. Pour installer ce module à l'aide des paramètres du paquet d'installation ou de l'Assistant d'installation, ou en modifiant l'ensemble des modules de l'application dans le Panneau de configuration Windows, sélectionnez **Managed Detection and Response**. Vous pouvez également installer le module à l'aide de la tâche *Modifier les modules de Kaspersky Embedded Systems Security*.

   > Pour installer le module Managed Detection and Response sans redémarrer l'ordinateur à l'aide de la tâche *Modifier les modules de Kaspersky Embedded Systems Security*, vous devez désactiver l'option **Vérifier la présence d'applications incompatibles d'éditeurs tiers** dans les paramètres de la tâche.

2. **Configuration de Kaspersky Private Security Network**

   À partir de la mise à jour de juillet 2025, la solution Managed Detection and Response peut fonctionner sans le fichier de configuration KPSN. Pour en savoir plus sur la manière dont la solution MDR utilise Kaspersky Security Network, consultez l'aide de Kaspersky Managed Detection and Response.

   Si votre configuration ne répond pas aux exigences pour fonctionner sans fichiers de configuration KPSN, chargez le fichier de configuration KPSN dans les propriétés du Serveur d'administration. Le fichier de configuration KPSN se trouve à l'intérieur de l'archive ZIP du fichier de configuration MDR. Vous pouvez également charger le fichier de configuration KPSN à l'aide de la ligne de commande.

   Pour en savoir plus à propos de la configuration de Kaspersky Private Security Network, veuillez consulter l'aide de Kaspersky Security Center.

3 Activation de Kaspersky Managed Detection and Response

Pour activer la solution Managed Detection and Response dans Kaspersky Embedded Systems Security, vous devez disposer d'une licence distincte pour le module complémentaire Kaspersky Managed Detection and Response for Embedded Systems Security. Pour en savoir plus sur l'activation de la solution, consultez l'aide de Kaspersky Managed Detection and Response.

Kaspersky Embedded Systems Security ne prend pas en charge les fichiers de configuration MDR (fichiers BLOB). Toutes les ressources seront placées dans le locataire racine.

4 Activation du module Managed Detection and Response

Comment activer le module Managed Detection and Response dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Sélectionnez la section **Serveurs de collecte de télémétrie**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Managed Detection and Response**.

   La fenêtre **Managed Detection and Response** s'ouvre.
5. Cochez la case **Managed Detection and Response**.
6. Enregistrez vos modifications.

Comment activer le module Managed Detection and Response dans la Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Serveurs de collecte de télémétrie**.
5. Cliquez sur le bouton **Paramètres** dans le groupe **Managed Detection and Response**.

   La fenêtre **Managed Detection and Response** s'ouvre.
6. Cochez la case **Managed Detection and Response DÉSACTIVÉ**.
7. Enregistrez vos modifications.

Comment activer le module Managed Detection and Response dans la Console de l'application

1. Dans l'arborescence de la Console de l'application, sélectionnez la section **Serveurs de collecte de télémétrie → Managed Detection and Response**.
2. Dans le panneau des résultats, cliquez sur le lien **Propriétés**.

   La fenêtre **Managed Detection and Response** s'ouvre sous l'onglet **Général**.

3. Cochez la case **Managed Detection and Response**.

4. Enregistrez vos modifications.

Vous pouvez également activer le module Managed Detection and Response à l'aide de la ligne de commande.

5 **Configuration de l'octroi de télémétries à d'autres modules de l'application**

Vous devez activer les modules suivants pour que Kaspersky Managed Detection and Response puisse fonctionner :

- Kaspersky Security Network (mode élargi).
- Protection des fichiers en temps réel.
- Scanner AMSI.
- Détection comportementale.
- Protection contre les Exploits.
- Protection contre les menaces réseau.
- Pare-feu.
- Analyse à la demande.

Pour que Kaspersky Managed Detection and Response fonctionne avec le Serveur d'administration via Kaspersky Security Center Web Console, vous devez également établir une nouvelle connexion sécurisée, une *connexion en arrière-plan*. Kaspersky Managed Detection and Response vous invite à établir une connexion d'arrière-plan lorsque vous déployez la solution. Confirmez que la connexion d'arrière-plan existe.

Établissement d'une connexion en arrière-plan dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Paramètres** → **Intégration**.

2. Passez à la section **Intégration**.

3. Activez le commutateur **Connexion en arrière-plan pour l'intégration Activé**.

4. Enregistrez vos modifications.

Gestion de Kaspersky Embedded Systems Security via la ligne de commande

Vous pouvez gérer et administrer Kaspersky Embedded Systems Security via la ligne de commande.

Pour gérer Kaspersky Embedded Systems Security via la ligne de commande, procédez comme suit :

1. Sur l'appareil, exécutez un interpréteur de ligne de commande (par exemple, cmd.exe) avec les autorisations de l'administrateur local.

2. En utilisant la commande `cd`, accédez au dossier dans lequel se trouve le fichier kavshell.exe.

   Exemple

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
   ```

   Vous pouvez également ajouter le chemin du fichier exécutable à la variable système %PATH% pendant la phase d'installation de l'application et exécuter la commande sans avoir à naviguer jusqu'au dossier de l'application.

3. Utilisez le modèle suivant pour exécuter la commande :

   ```
   KAVSHELL <command> [options]
   ```

   Vous pouvez consulter la liste des commandes d'administration de l'application à l'aide de la commande `KAVSHELL HELP`. Pour obtenir de l'aide sur la syntaxe d'une commande en particulier, saisissez `KAVSHELL HELP <command>`.

Par conséquent, Kaspersky Embedded Systems Security exécute l'action indiquée.

APPCONTROL. Importation des règles du Contrôle du lancement des applications

La commande `KAVSHELL APPCONTROL` permet d'importer les règles du module Contrôle du lancement des applications à partir d'un fichier XML et de supprimer toutes les règles de la liste des règles du module. Pour générer un fichier XML contenant des règles, vous pouvez utiliser une tâche *Générateur de règles pour le Contrôle du lancement des applications* locale ou de groupe.

Syntaxe de la commande

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Argument requis. Importation des règles du Contrôle du lancement des applications depuis le fichier XML spécifié : • `/APPEND` ajoute toutes les règles du fichier à la liste des règles du module. Si une règle figure déjà dans la liste, elle est dupliquée. • `/REPLACE` remplace toute la liste existante des règles du module par les règles du fichier. • `/MERGE` fusionne les règles du fichier avec la liste existante des règles. Si une règle figure déjà dans la liste, elle n'est pas dupliquée. Pour supprimer toutes les règles du module Contrôle du lancement des applications, utilisez `/CLEAR`.
`<path to XML file>`	Requis si `/APPEND`, `/REPLACE` et `/MERGE` sont transmis. Chemin d'accès complet au fichier XML contenant les règles.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG. Configuration du module Contrôle du lancement des applications

La commande `KAVSHELL APPCONTROL /CONFIG` permet de gérer les paramètres du module Contrôle du lancement des applications.

Syntaxe de la commande

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/MODE: <applyrules|statistics>`	Argumentaire facultatif. Mode de fonctionnement du module Contrôle du lancement des applications : • `applyrules` : Kaspersky Embedded Systems Security contrôle le lancement des applications à l'aide des règles du Contrôle du lancement des applications. • `statistics` (valeur par défaut) : Kaspersky Embedded Systems Security autorise le lancement de toutes les applications. Dans ce mode, l'application enregistre uniquement les informations relatives à tous les lancements d'applications, aux règles qui s'appliquent aux applications lancées et aux actions qui auraient été effectuées si le module fonctionnait en mode `applyrules`.
`/DLL:<no|yes>`	Argumentaire facultatif. Surveillance du chargement des DDL : • `no` (valeur par défaut) : Kaspersky Embedded Systems Security ne contrôle pas le chargement des modules DLL à l'aide des règles du Contrôle du lancement des applications. Le chargement des modules DLL est autorisé. • `yes` : si cette fonctionnalité est activée, Kaspersky Embedded Systems Security autorise ou interdit le chargement des modules DLL à l'aide des règles du Contrôle du lancement des applications.

`/SAVETOFILE:<path to XML file>`	Argumentaire facultatif. Enregistrement de la liste des règles du Contrôle du lancement des applications dans le fichier XML indiqué.
`/SDC`	Argumentaire facultatif. Exportez le cache de distribution des applications vers le fichier de configuration XML indiqué par l'option `/SAVETOFILE`.
`/CLEARSDC`	Argumentaire facultatif. Suppression du cache de distribution des logiciels.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE. Générateur de règles pour le Contrôle du lancement des applications

Vous pouvez utiliser la commande `KAVSHELL APPCONTROL /GENERATE` pour gérer la tâche *Générateur de règles pour le Contrôle du lancement des applications*.

Syntaxe de la commande

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`<path to folder>`	Obligatoire si `/SOURCE` n'est pas spécifié. Chemin d'accès à un dossier contenant des fichiers exécutables, des packages MSI et des scripts. La tâche créera des règles d'autorisation si des fichiers des types spécifiés et situés dans les dossiers spécifiés sont lancés.
`/SOURCE:<path to file with folders list>`	Obligatoire si `<path to folder>` n'est pas spécifié. Chemin d'accès à un fichier TXT contenant une liste de dossiers comprenant les fichiers exécutables pour lesquels des règles d'autorisation seront créées automatiquement.
`/MASKS:<edms>`	Argumentaire facultatif. Extensions des fichiers exécutables pour lesquels des règles d'autorisation seront créées automatiquement. Vous pouvez inclure dans la zone d'application de la tâche les fichiers portant les extensions suivantes : • `e` pour les fichiers EXE • `d` pour les fichiers DLL • `m` pour les fichiers MSI • `s` pour les scripts
`/RUNAPP`	Argumentaire facultatif. Créer des règles d'autorisation sur la base des applications en cours d'exécution.

`/RULES:<ch|cp|h>`	Argumentaire facultatif. Critère que la tâche appliquera lors de la création des règles d'autorisation du Contrôle du lancement des applications : • `ch` pour utiliser le certificat numérique. En cas d'absence de certificat, utiliser, utiliser le hash SHA256. • `cp` pour utiliser le certificat numérique. En cas d'absence de certificat, utiliser la valeur du chemin d'accès au fichier exécutable. • `h` pour utiliser le hash SHA256.
`/STRONG`	Argumentaire facultatif. Utilisation de l'objet et de l'empreinte du certificat numérique du fichier comme critère de déclenchement des règles d'autorisation du Contrôle du lancement des applications. Utilisé avec le paramètre `/RULES:<ch|cp>`.
`/USER:<user or group of users>`	Argumentaire facultatif. Nom de l'utilisateur ou du groupe d'utilisateurs auxquels les règles seront appliquées.
`/EXPORT:<path to XML file>`	Argumentaire facultatif. Chemin d'accès et nom du fichier XML dans lequel vous souhaitez enregistrer les règles spécifiées.
`/IMPORT:<a|r|m>`	Argumentaire facultatif. Importer les règles générées dans la liste des règles du Contrôle du lancement des applications : • `a` ajoute toutes les règles du fichier à la liste des règles du module. Si une règle figure déjà dans la liste, elle est dupliquée. • `r` remplace toute la liste existante des règles du module par les règles du fichier. • `m` fusionne les règles du fichier avec la liste existante des règles. Si une règle figure déjà dans la liste, elle n'est pas dupliquée.
`/PREFIX:<prefix for rules names>`	Spécification d'un préfixe pour les noms des règles d'autorisation du Contrôle du lancement des applications.
`/UNIQUE`	Ajout aux règles d'informations sur l'appareil protégé, sur la base desquelles les règles d'autorisation du Contrôle du lancement des applications sont générées.
`/ADDPATH`	Ajouter le chemin d'accès d'un fichier exécutable aux règles générées sur la base de hashs.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG. Prise en charge de la technologie AM-PPL

La commande `KAVSHELL CONFIG` permet d'administrer la protection des processus de l'application au moyen de la technologie AM-PPL.

Pour que la commande fonctionne correctement, vous devez désactiver le mécanisme d'Autodéfense.

Syntaxe de la commande

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PPL:<ON|OFF>`	Argument requis. Active ou désactive la prise en charge de la technologie AM-PPL : • `ON` : activer la prise en charge de la technologie AM-PPL. • `OFF` : désactiver la prise en charge de la technologie AM-PPL.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

DEVCONTROL. Importation des règles du Contrôle des appareils

La commande `KAVSHELL DEVCONTROL` permet d'importer les règles du module Contrôle des appareils à partir d'un fichier XML produit par la commande *Générateur de règles pour le Contrôle des appareils* ou de supprimer toutes les règles de la liste des règles du module.

Syntaxe de la commande

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Argument requis. Importation des règles du Contrôle des appareils à partir du fichier XML indiqué : • `/APPEND` ajoute toutes les règles du fichier à la liste des règles du module. Si une règle figure déjà dans la liste, elle est dupliquée. • `/REPLACE` remplace toute la liste existante des règles du module par les règles du fichier. • `/MERGE` fusionne les règles du fichier avec la liste existante des règles. Si une règle figure déjà dans la liste, elle n'est pas dupliquée. Pour supprimer toutes les règles du module Contrôle des appareils, utilisez `/CLEAR`.
`<path to XML file>`	Requis si `/APPEND`, `/REPLACE` et `/MERGE` sont transmis. Chemin d'accès complet au fichier XML contenant les règles.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.

Paramètre	Description
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP. Enregistrement des vidages de la mémoire

La commande `KAVSHELL DUMP` permet d'activer ou de désactiver le vidage de la mémoire.

Syntaxe de la commande

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/ON`	Activer la création de fichiers de vidage.
`/F:` `<dump_file_folder>`	Argument requis. Définit le dossier dans lequel les fichiers de vidage sont enregistrés.
`/SNAPSHOT`	Crée un vidage de la mémoire d'un processus en cours d'exécution portant l'ID indiqué. Le fichier de vidage est enregistré dans le dossier indiqué par l'option `/F`.
`/P:<process_ID>`	Obligatoire si `/SNAPSHOT` est spécifié. Définit l'ID d'un processus. Vous pouvez déterminer l'ID du processus à l'aide de la commande `tasklist`.
`/OFF`	Désactiver la création de fichiers de vidage.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EXITPOLICY. Désactivation de la stratégie sur l'appareil

La commande `KAVSHELL EXITPOLICY` désactive la stratégie de Kaspersky Security Center sur l'appareil. Après la désactivation de la stratégie, tous les paramètres de Kaspersky Embedded Systems Security deviennent disponibles à la configuration, y compris ceux marqués dans la stratégie par un cadenas fermé ( ).

Syntaxe de la commande

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT. Exportation des paramètres de l'application

La commande `KAVSHELL EXPORT` permet d'exporter les paramètres de Kaspersky Embedded Systems Security dans un fichier de configuration au format XML. Vous pouvez enregistrer tous les paramètres de l'application ainsi que les paramètres des modules distincts dans un fichier de configuration.

Syntaxe de la commande

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

Options de la commande

Paramètre	Description
`<profile>`	Argument requis. Saisissez le nom du profil de paramètres à exporter. Un profil est un module, une tâche ou une fonctionnalité de Kaspersky Embedded Systems Security. Pour connaître la liste des profils disponibles, utilisez la commande `KAVSHELL EXPORT /?`. Pour exporter tous les paramètres de l'application, indiquez le profil `product`.
`<file name>`	Argument requis. Indiquez le nom du fichier au format XML dans lequel exporter les paramètres du profil. Vous pouvez également indiquer le chemin d'accès au fichier. Exemple : `C:\Test\settings.xml` • Si seul un nom de fichier est indiqué dans la commande, l'application tente de placer le fichier dans son dossier d'installation. Si les mécanismes d'Autodéfense de l'application sont activés, l'exportation échouera, car l'Autodéfense de l'application bloque la création d'un nouveau fichier dans le dossier de l'application. Pour exporter les paramètres de l'application, indiquez le chemin d'accès au fichier.

`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.
`/PWD: <password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.

Exemple

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET. Nettoyage de la base iSwift

Kaspersky Embedded Systems Security peut utiliser la technologie iSwift, qui permet à l'application d'éviter de réanalyser les fichiers qui n'ont pas été modifiés depuis la dernière analyse. La commande `KAVSHELL FBRESET` efface la base de données qui stocke les informations relatives aux fichiers sains analysés. Une fois la base de données effacée, Kaspersky Embedded Systems Security analyse tous les fichiers auxquels l'application accède pour la première fois.

Syntaxe de la commande

```
KAVSHELL FBRESET
```

FIM /BASELINE. Contrôle de l'intégrité du système par rapport à une référence

Vous pouvez utiliser la commande `KAVSHELL FIM /BASELINE` pour gérer la tâche *Contrôle de l'intégrité du système par rapport à une référence*.

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/CREATE`	Démarrage d'une nouvelle tâche *Contrôle de l'intégrité du système par rapport à une référence* qui créera un instantané de l'état du système.
`/SCAN`	Exécutez les tâches *Contrôle de l'intégrité du système par rapport à une référence* avec l'ID de l'instantané du système ou le nom alternatif d'une tâche existante.
`/CLEAR`	Suppression de l'état de référence. Indiquez l'ID d'un instantané du système ou le nom alternatif de la tâche qui a créé l'instantané. Si aucun nom alternatif de tâche ni aucun ID d'instantané n'est indiqué, l'application supprime tous les instantanés.
`/EXPORT`	Exportez les données de tous les instantanés ou de l'instantané indiqué à l'aide de l'option `/BL` dans un fichier TXT situé dans le dossier indiqué.
`/SHOW`	Affichez les données de tous les instantanés de l'état du système ou de l'instantané indiqué par l'option `/BL`.

`<monitoring scope>`	Obligatoire si /L n'est pas spécifié. Définit la zone de surveillance de la tâche. Vous pouvez utiliser les caractères `*` et `?` pour saisir un masque de chemin.
`/L`	Obligatoire si `<monitoring scope>` n'est pas spécifié. Permet d'indiquer le chemin d'accès au fichier TXT contenant la liste des zones de surveillance.
`/MD5`	Argumentaire facultatif. Ne peut pas être utilisé avec le paramètre `/SHA256`. Définit l'algorithme MD5 pour le calcul de la somme de contrôle. L'algorithme MD5 est utilisé par défaut.
`/SHA256`	Argumentaire facultatif. Ne peut pas être utilisé avec le paramètre `/MD5`. Définit l'algorithme SHA256 pour le calcul de la somme de contrôle. L'algorithme MD5 est utilisé par défaut.
`/SF`	Argumentaire facultatif. Inclut tous les sous-dossiers dans la zone de surveillance de la tâche. Par défaut, les sous-dossiers ne sont pas inclus dans la zone de surveillance.
`/ALIAS:<existing task id>`	Obligatoire si `/BL` n'est pas spécifié. Nom alternatif de la tâche. Vous pouvez connaître le nom alternatif de la tâche à l'aide de la commande `KAVSHELL FIM /BASELINE /SHOW`.
`/BL:<id baseline>`	Obligatoire si `/ALIAS` n'est pas spécifié. Définit l'ID de l'instantané système. Vous pouvez connaître l'ID de référence à l'aide de la commande `KAVSHELL FIM /BASELINE /SHOW`.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

AIDE. Affichage de l'aide sur les commandes

Pour afficher la liste de toutes les commandes disponibles de Kaspersky Embedded Systems Security, exécutez l'une des commandes suivantes :

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Pour afficher la description et la syntaxe d'une commande, exécutez l'une des commandes suivantes :

```
KAVSHELL HELP <command>
```

```
KAVSHELL <command> /?
```

Exemple

```
KAVSHELL HELP SCAN
```

IMPORT. Importation des paramètres de l'application

La commande `KAVSHELL IMPORT` permet d'importer les paramètres de Kaspersky Embedded Systems Security à partir d'un fichier de configuration au format XML. Vous pouvez créer le fichier de configuration à l'aide de la commande `KAVSHELL EXPORT`.

Syntaxe de la commande

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`<file name>`	Argument requis. Indiquez le chemin d'accès complet au fichier XML depuis lequel vous souhaitez importer les paramètres, y compris son nom et son extension.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -4 : Objet introuvable.
- -9 : Échec de la tentative de lancement de l'appareil administré sous un autre compte utilisateur.
- -99 : erreur inconnue.
- -501 : L'opération a réussi, mais une erreur ou un avertissement s'est produit pendant l'exécution (par exemple, l'application n'a pas importé les paramètres de certains modules).

- -502 : Le fichier d'importation est manquant ou son format n'est pas reconnu.
- -503 : Paramètres incompatibles (le fichier de configuration a été exporté depuis une autre application ou une version ultérieure et incompatible de Kaspersky Embedded Systems Security).

KSN. Utilisation de KSN/KPSN

Vous pouvez utiliser la commande `KAVSHELL KSN` pour sélectionner une solution Kaspersky chargée de déterminer la réputation des fichiers ou des sites Internet. Kaspersky Embedded Systems Security prend en charge les solutions d'infrastructure suivantes pour utiliser les bases de données de réputation de Kaspersky :

- *Kaspersky Security Network (KSN)* est la solution utilisée par la majorité des applications de Kaspersky. Les participants au KSN reçoivent des informations de Kaspersky et envoient également à Kaspersky des données sur les objets détectés sur leur ordinateur afin que les analystes de Kaspersky puissent réaliser une analyse complémentaire et enrichir les bases de données de réputation et de statistiques.
- *Kaspersky Private Security Network (KPSN)* est une solution qui permet aux utilisateurs d'ordinateurs dotés de Kaspersky Embedded Systems Security ou d'autres programmes de Kaspersky d'accéder aux bases de données sur les réputations de Kaspersky Security Network ainsi qu'à d'autres statistiques sans envoyer de données à KSN depuis leurs ordinateurs. Le KPSN a été mis au point pour les entreprises clientes qui ne peuvent pas participer à Kaspersky Security Network pour les raisons suivantes par exemple :
  - absence de connexion des postes de travail locaux à Internet ;
  - interdiction législative ou restriction imposée par la sécurité de l'entreprise sur l'envoi de données hors du pays ou hors du réseau local de l'organisation.

Syntaxe de la commande

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/GLOBAL`	Passage à l'utilisation de Kaspersky Security Network.
`/PRIVATE <settings-file>`	Passage à l'utilisation de Kaspersky Private Security Network. Indiquez le nom du fichier de configuration contenant les paramètres de Kaspersky Private Security Network. Ce fichier porte l'extension .PKCS7 ou .PEM.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KL Admin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KL Admin.

Exemple

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE. Activation de l'application

La commande `KAVSHELL LICENSE` permet de gérer les clés et les codes d'activation de Kaspersky Embedded Systems Security.

Syntaxe de la commande

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
Aucune option spécifiée.	L'instruction affiche les informations suivantes sur les clés ajoutées : • Clé. • Type de licence (commerciale). • Durée de validité de la licence associée à la clé. • État de la clé (active ou complémentaire). Si l'état est *, la clé ajoutée est une clé additionnelle.
`/ADD:<key_file | activation code>`	Activation de Kaspersky Embedded Systems Security à l'aide d'un fichier clé. Si l'application est déjà activée, la clé est ajoutée en tant que clé de licence de réserve.
`/R`	Si l'option `/R` est transmise, le code d'activation ou la clé est ajouté comme code ou clé de réserve.
`/DEL:<license key serial number>`	Supprimez la clé ou le code d'activation indiqué.
`/REFRESH:<license id>`	Mettez à jour l'état de la licence indiquée.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -4 : clé portant le numéro indiqué introuvable.
- -5 : erreur de syntaxe.
- -6 : opération incorrecte (la clé a déjà été ajoutée).
- -99 : erreur inconnue.
- -301 : la licence n'est pas valide.
- -303 : la licence correspond à une autre application.

MDR. Configuration de l'intégration de Managed Detection and Response

La commande `KAVSHELL MDR` permet de configurer l'intégration de Kaspersky Embedded Systems Security avec la solution Managed Detection and Response.

Syntaxe de la commande

```
KAVSHELL MDR /ENABLE [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<password>] [/LOGIN:<user name>] |
/SHOW
```

Options de la commande

Paramètre	Description
`MDR /<enable|disable|show>`	Argument requis. Permet d'activer, de désactiver ou d'afficher les paramètres actuels du module Managed Detection and Response.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL MDR /ENABLE /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

OMSINFO. Création d'un fichier JSON contenant des informations sur l'application

La commande `KAVSHELL OMSINFO` permet de créer un fichier JSON contenant des informations sur l'état actuel de l'application et les menaces détectées, que vous pouvez ensuite charger dans des systèmes de surveillance.

Syntaxe de la commande

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

Options de la commande

Paramètre	Description
`<oms_info_json_file_name>`	Chemin d'accès complet au fichier JSON, y compris son nom et son extension.

Exemple

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

MOT DE PASSE. Accès protégé par mot de passe aux fonctionnalités de Kaspersky Embedded Systems Security

La commande `KAVSHELL PASSWORD` permet d'administrer l'accès protégé par mot de passe aux fonctionnalités de Kaspersky Embedded Systems Security. Si cette fonctionnalité est activée, l'application demande un nom d'utilisateur et un mot de passe lors de la suppression, de la modification ou de la récupération de l'application et lors de l'exécution d'actions sur la ligne de commande susceptibles de réduire le niveau de protection de l'appareil.

Syntaxe de la commande

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/SET`	Active la demande de mot de passe pour confirmer les actions critiques.

`/NEW:<new password>`	Obligatoire si `/SET` est spécifié.
	Définit un nouveau mot de passe.
	Lors de la création d'un mot de passe, il est recommandé de respecter les conditions suivantes :
	• Le mot de passe ne contient pas le nom du compte ou le nom de l'ordinateur.
	• Le mot de passe comporte au moins 8 caractères.
	• Le mot de passe contient des caractères appartenant à au moins trois des catégories suivantes :
	  • Lettres latines majuscules (A à Z)
	  • Lettres latines minuscules (a à z)
	  • Chiffres (0-9)
	  • Point d'exclamation (!), signe dollar ($), signe dièse (#) et signe de pourcentage (%)

`/RESET`	Désactive la demande de mot de passe pour confirmer les actions critiques.
`/PWD:<password>`	Argument requis. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

PATCHCOMPATIBILITYRESET. Suppression d'un correctif de la liste des correctifs incompatibles

La commande `KAVSHELL PATCHCOMPATIBILITYRESET` permet de supprimer de la liste des correctifs incompatibles un correctif portant le GUID indiqué. Vous pouvez indiquer plusieurs GUID séparés par des espaces.

Syntaxe de la commande

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

Exemple

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

REMOTEACCESS. Gestion des paramètres de connexion à distance de la Console de l'application

La commande `KAVSHELL REMOTEACCESS` permet de gérer les paramètres de connexion à distance de la Console de l'application à l'appareil sur lequel Kaspersky Embedded Systems Security est installé.

Syntaxe de la commande

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

Options de la commande

Paramètre	Description
`/SET [UIPORT | UIKLPORT]`	Définissez le numéro de port : • `UIPORT` est le port de connexion à l'aide des identifiants Windows. • `UIKLPORT` est le port de connexion à l'aide des identifiants des utilisateurs créés manuellement.
`/PORT=<new_port>`	Obligatoire si `/SET` est spécifié. Numéro de port. Plage de valeurs possibles : 1–65535.
`/RESET UIKLPORT`	Fermez le port de connexion à l'aide des identifiants des utilisateurs créés manuellement.
`/SHOW`	Affichez les numéros de port actuels.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
```

```
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID. Réinitialisation de l'identifiant de l'appareil

La commande `KAVSHELL RESETMDRMACHINEID` permet de réinitialiser l'identifiant de l'appareil utilisé par la solution Managed Detection and Response.

Syntaxe de la commande

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

ROLLBACK. Annulation de la dernière mise à jour

La commande `KAVSHELL ROLLBACK` lance la tâche *Annulation de la dernière mise à jour*.

Syntaxe de la commande

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL ROLLBACK
```

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -99 : erreur inconnue.
- -221 : La copie de sauvegarde de la base de données est introuvable ou corrompue.
- -222 : La copie de sauvegarde de la base de données est corrompue.

RTP. Protection des fichiers en temps réel

La commande `KAVSHELL RTP` permet d'activer ou de désactiver le module Protection des fichiers en temps réel.

Syntaxe de la commande

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`</START|/STOP>`	Activez ou désactivez le module Protection des fichiers en temps réel : • `/START` active le module. • `/STOP` désactive le module.
`/PWD:<password>`	Option obligatoire pour la commande `KAVSHELL RTP /STOP`. Mot de passe du compte utilisateur KL Admin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KL Admin.

Exemple

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

ANALYSE. Analyse à la demande

Vous pouvez utiliser la commande `KAVSHELL SCAN` pour créer et démarrer la tâche *Analyse à la demande*. Pour lancer une tâche d'analyse à la demande existante via la ligne de commande, utilisez la commande `KAVSHELL TASK`.

Syntaxe de la commande

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
```

```
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Options de la commande

Paramètre	Description
`<scan_scope>`	Argument requis. Liste de fichiers, de dossiers, de chemins d'accès réseau ou de zones d'analyse standard séparés par des espaces. Zones d'analyse standard : • `/MEMORY` analyse tous les processus en mémoire. • `/SHARED` analyse les dossiers partagés. • `/STARTUP` analyse les objets de démarrage. • `/REMDRIVES` analyse les disques amovibles. • `/FIXDRIVES` analyse tous les disques durs locaux. • `/MYCOMP` analyse l'ensemble de l'ordinateur. Vous pouvez indiquer plusieurs valeurs séparées par des espaces.
`/L:<file_name>`	Argumentaire facultatif. Chemin d'accès au fichier contenant la liste des zones d'analyse. Le fichier doit être créé manuellement et enregistré au format TXT. Le fichier doit être enregistré avec l'encodage UTF-8 sans BOM.
`/F<A|C|E>`	Argumentaire facultatif. Objets à inclure dans la zone d'analyse : • `/FA` : analyser tous les objets. L'application analyse tous les fichiers sans exception, quels que soient leur format et leur extension. • `/FC` : analyser les objets en fonction de leur format. L'application analyse uniquement les objets dont le format figure dans la liste des formats des objets infectables. • `/FE` : analyser les objets en fonction de leur extension. L'application analyse uniquement les objets dont l'extension figure dans la liste des extensions des objets infectables.
`/NEWONLY`	Argumentaire facultatif. Analyser uniquement les nouveaux fichiers et les fichiers modifiés. Si cet argument n'est pas transmis, Kaspersky Embedded Systems Security analyse tous les objets.
`/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>`	Argumentaire facultatif. Action que vous souhaitez que l'application effectue sur les objets infectés et les autres objets : • `DISINFECT` : Désinfecter ; informer si la désinfection est impossible. • `DISINFDEL` : Désinfecter ; supprimer si la désinfection est impossible. • `DELETE` : Supprimer. • `REPORT` (valeur par défaut) : Informer. • `AUTO` : Recommandé.
`/AS:<QUARANTINE|DELETE|REPORT|AUTO>`	Argumentaire facultatif. Action que vous souhaitez que l'application effectue sur les objets infectés : • `QUARANTINE` : placer en quarantaine. • `DELETE` : Supprimer. • `REPORT` (valeur par défaut) : Informer. • `AUTO` : Recommandé.

Paramètre	Description
/E:<ABMSPO>	Excluez les types d'objets indiqués. Valeurs possibles : • A : archives ZIP, CAB, RAR et ARJ, ainsi que les archives d'autres formats. • B : fichiers des bases de données de messagerie de Microsoft Outlook et Microsoft Outlook Express. • M : fichiers au format de messagerie, tels que les messages Microsoft Outlook et Microsoft Outlook Express. • S : archives autoextractibles. • P : fichiers exécutables compactés par des compacteurs de code binaire, tels que UPX ou ASPack. • O : objets intégrés à des fichiers (tels que les macros Microsoft Word ou les pièces jointes aux emails). Vous pouvez indiquer plusieurs valeurs de paramètre.
/EM=<file mask>	Exclusion de l'analyse des fichiers sur la base d'un masque. Par exemple : • Le masque *.exe reprend tous les chemins d'accès aux fichiers portant l'extension EXE. • Le masque example* reprend tous les chemins d'accès aux fichiers nommés EXAMPLE.
/ET=<scan duration in seconds>	Exclusion de l'analyse des fichiers dont la durée d'analyse dépasse la valeur spécifiée en secondes. La valeur par défaut est de 60 secondes.
/ES=<size in megabytes>	Exclusion de l'analyse des fichiers dont la taille dépasse la valeur spécifiée en mégaoctets. La valeur par défaut est 100 Mo.
/TZOFF	Ne pas appliquer les exclusions de la zone de confiance.
/NOICHECKER	Désactivation de l'utilisation de la technologie iChecker (activée par défaut).
/NOISWIFT	Désactivation de l'utilisation de la technologie iSwift (activée par défaut).
/NOCHECKMSSIGN	Ne pas analyser les fichiers signés numériquement par Microsoft.
/ANALYSERLEVEL	Activation de l'utilisation de l'analyse heuristique et configuration du niveau d'analyse. Les niveaux d'analyse heuristique suivants sont disponibles : • 1 : superficielle. • 2 : moyenne. • 3 : minutieuse. Si cet argument n'est pas indiqué, l'application n'utilise pas l'analyse heuristique.
/EXCLUDE=<list of exlusion	Liste des fichiers, dossiers ou chemins réseau qui seront exclus de la zone d'analyse de la tâche. Vous pouvez indiquer plusieurs valeurs séparées par des espaces.
/W=<file path>	Chemin et nom du fichier du journal d'exécution de la tâche. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.
/ANSI	Utilisez le codage ANSI pour les événements consignés dans le journal d'exécution de la tâche. Le paramètre /ANSI ne sera pas appliqué si le paramètre /W n'est pas transmis. Si le paramètre /ANSI n'est pas spécifié, Unicode est utilisé pour générer le journal d'exécution de la tâche.
/ALIAS:<alternate name>	Attribuez à la tâche un nom temporaire permettant de la référencer pendant son exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à l'aide de la commande KAVSHELL TASK. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâches dans l'application. Si cet argument n'est pas transmis, le nom de la tâche est attribué comme suit : scan_<kavshell_pid>. Par exemple : scan_1234.

Exemple

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Valeurs de retour de la commande :

- 0 : opération terminée avec succès (aucune menace détectée).
- 1 : opération annulée.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -4 : l'objet est introuvable (le fichier contenant la liste des zones d'analyse est introuvable).
- -5 : erreur de syntaxe ou zone d'analyse non définie.
- -80 : objets infectés détectés.
- -81 : objets probablement infectés détectés.
- -82 : erreurs de traitement des objets lors de l'analyse.
- -83 : objets non analysés détectés.
- -84 : objets endommagés détectés.
- -85 : échec de la création du journal d'exécution de la tâche.
- -99 : erreur inconnue.
- -301 : la licence n'est pas valide.

SCANCRITICAL. Analyse des zones critiques

La commande `KAVSHELL SCANCRITICAL` lance la tâche *Analyse des zones critiques*.

Syntaxe de la commande

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/W`	Argumentaire facultatif. Spécifiez un nom de fichier avec l'extension .LOG pour le journal d'exécution de la tâche exporté. Vous pouvez également indiquer le chemin d'accès au fichier. Si seul un nom de fichier est indiqué dans la commande, l'application tente de placer le fichier dans son dossier d'installation. Si les mécanismes d'Autodéfense de l'application sont activés, l'exportation échouera, car l'Autodéfense de l'application bloque la création d'un nouveau fichier dans le dossier de l'application. Pour exporter le journal, indiquez le chemin d'accès au fichier.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.

`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

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

SERVERBINDINGDISABLE. Désactivation de la protection de la connexion au Serveur d'administration

La commande `KAVSHELL SERVERBINDINGDISABLE` désactive localement la protection de la connexion au Serveur d'administration. La commande lance la tâche *Protection de la connexion au Serveur d'administration*, qui supprime le mot de passe de la connexion de l'ordinateur au Serveur d'administration.

Syntaxe de la commande

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

START. Démarrage du service de l'application

La commande `KAVSHELL START` démarre Kaspersky Embedded Systems Security Service.

Syntaxe de la commande

```
KAVSHELL START
```

STARTPOLICY. Activation de la stratégie

La commande `KAVSHELL STARTPOLICY` active la stratégie de Kaspersky Security Center sur l'appareil protégé. Les paramètres de l'application sont alors configurés conformément à la stratégie.

Syntaxe de la commande

```
KAVSHELL STARTPOLICY
```

STOP. Arrêt du service de l'application

La commande `KAVSHELL STOP` arrête Kaspersky Embedded Systems Security Service.

Syntaxe de la commande

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KL Admin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KL Admin.

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -5 : erreur de syntaxe.
- -6 : opération non valide (le service Kaspersky Embedded Systems Security Service est déjà arrêté).
- -7 : le service n'est pas enregistré
- -8 : le démarrage automatique du service est désactivé.
- -9 : Échec de la tentative de lancement de l'appareil administré sous un autre compte utilisateur.
- -99 : erreur inconnue.

TASK. Gestion des tâches

La commande `KAVSHELL TASK` permet d'administrer les tâches de Kaspersky Embedded Systems Security : lancer, suspendre, reprendre ou arrêter une tâche, ainsi que consulter son état actuel et ses statistiques.

Syntaxe de la commande

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

Options de la commande

Paramètre	Description
Pas de paramètres	Renvoie la liste de toutes les tâches existantes de Kaspersky Embedded Systems Security. La liste contient les champs suivants : le nom alternatif de la tâche (nom court supplémentaire attribué aux tâches par Kaspersky Embedded Systems Security for Windows), la catégorie de la tâche (système ou utilisateur) et son état actuel.
`<alternative name>`	Nom alternatif de la tâche que vous souhaitez administrer. Pour consulter les noms alternatifs des tâches de Kaspersky Embedded Systems Security, saisissez la commande `KAVSHELL TASK` sans paramètre.
`/START`	Lancement d'une tâche.
`/STOP`	Arrêt d'une tâche.
`/STATE`	Afficher l'état actuel de la tâche.
`/STATISTICS`	Afficher les statistiques de la tâche.
`/PWD: <password>`	Option obligatoire pour la commande `KAVSHELL TASK /STOP`. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Syntaxe de la commande

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -4 : l'objet est introuvable (la tâche est introuvable).
- -5 : erreur de syntaxe ou zone d'analyse non définie.
- -6 : opération invalide (par exemple, la tâche n'est pas lancée, est déjà lancée ou ne peut pas être suspendue).
- -99 : erreur inconnue.
- -301 : la licence n'est pas valide.

- 401 : tâche non lancée (pour la commande `KAVSHELL TASK <task name> /STATE`).
- 402 : tâche déjà lancée (pour la commande `KAVSHELL TASK <task name> /STATE`).
- 403 : tâche suspendue (pour la commande `KAVSHELL TASK <task name> /STATE`).
- -404 : échec de l'opération (une modification de l'état de la tâche a provoqué un échec).

TRAÇAGE. Traçage du fonctionnement de l'application

La commande `KAVSHELL TRACE` permet d'activer ou de désactiver le traçage de l'application.

Syntaxe de la commande

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

Options de la commande

Paramètre	Description
`</ON | /OFF>`	Argument requis. Activer ou désactiver le traçage de l'application.
`/F:<traces_folder>`	Obligatoire si `/ON` est spécifié. Chemin d'accès au dossier dans lequel les fichiers de traçage seront enregistrés.
`/S:<traces_size_in_MB>`	Argumentaire facultatif. Taille maximale du fichier de traçage en mégaoctets. Valeurs disponibles : de 1 à 4 095 Mo. La valeur par défaut est 100 Mo.
`/LVL: <debug|info|warning|error|critical>`	Argumentaire facultatif. Niveau de détail des informations de débogage. • `critical` signifie que le fichier de traçage enregistre uniquement les messages relatifs aux erreurs critiques. • `error` signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, ainsi que les avertissements. • `warning` signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements et des informations complémentaires. • `info` (valeur par défaut) signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application. • `debug` signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.
`/R:<max trace files to rotate>`	Argumentaire facultatif. Nombre maximal de fichiers dans un journal de traçage. Valeurs disponibles : de 1 à 999. La valeur par défaut est 5.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.

/LOGIN:<user name>	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Exemple

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE. Mise à jour des bases de données et des modules de l'application

Vous pouvez utiliser la commande `KAVSHELL UPDATE` pour gérer la tâche *Mise à jour*.

Syntaxe de la commande

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Options de la commande

Paramètre	Description
<update_source | /AK | /KL>	Argument requis. Sélectionnez la source de mise à jour : • <update_source> pour utiliser des sources de mise à jour personnalisées. Vous pouvez indiquer le chemin d'accès à un dossier sur l'appareil protégé, le chemin d'accès à un dossier réseau au format UNC ou l'adresse d'un serveur HTTP ou FTP sur lequel se trouve le dossier contenant les mises à jour. • /AK pour utiliser le Serveur d'administration de Kaspersky Security Center comme source de mise à jour. • /KL pour utiliser les serveurs de mise à jour de Kaspersky comme source de mise à jour. Vous pouvez indiquer plusieurs valeurs séparées par des espaces.
/NOUSEKL	Argumentaire facultatif. Ne pas utiliser les serveurs de mise à jour de Kaspersky si les autres sources de mise à jour ne sont pas disponibles (valeur par défaut).
/PROXY:<IP address>:<port>	Argumentaire facultatif. Adresse IP ou nom symbolique du serveur proxy et numéro de port.
/AUTHTYPE:<0-2>	Argumentaire facultatif. Type d'authentification du serveur proxy : • 0 pour l'authentification NTLM avec le compte utilisateur actuel. • 1 pour l'authentification NTLM avec un compte utilisateur dont le nom d'utilisateur et le mot de passe sont spécifiés à l'aide des options /PROXYUSER et /PROXYPWD. • 2 pour l'authentification à l'aide du nom d'utilisateur et du mot de passe spécifiés par les options /PROXYUSER et /PROXYPWD.
/PROXYUSER:<user_name>	Paramètre obligatoire si les paramètres /AUTHTYPE:1 ou /AUTHTYPE:2 sont transmis. Nom d'utilisateur qui sera utilisé pour accéder au serveur proxy. Si /AUTHTYPE:0 est spécifié, les options /PROXYUSER:<user_name> et /PROXYPWD:<password> sont ignorées.
/PROXYPWD:<password>	Paramètre obligatoire si les paramètres /AUTHTYPE:1 ou /AUTHTYPE:2 sont transmis. Mot de passe de l'utilisateur qui sera utilisé pour accéder au serveur proxy. Si /AUTHTYPE:0 est spécifié, les options /PROXYUSER:<user_name> et /PROXYPWD:<password> sont ignorées. Si le paramètre /PROXYUSER est spécifié et que le paramètre /PROXYPWD est omis, le mot de passe sera considéré comme une chaîne vide.
/NOPROXYFORKL	Argumentaire facultatif. Ne pas utiliser les paramètres du serveur proxy pour se connecter aux serveurs de mise à jour de Kaspersky.

`/USEPROXYFORCUSTOM`	Argumentaire facultatif. Utiliser les paramètres du serveur proxy pour se connecter aux sources de mise à jour définies par l'utilisateur.
`/USEPROXYFORLOCAL`	Argumentaire facultatif. Utilise les paramètres du serveur proxy pour la connexion aux sources locales des mises à jour.
`/NOFTPPASSIVE`	Argumentaire facultatif. Si cette option est spécifiée, Kaspersky Embedded Systems Security utilise le mode actif pour la connexion au serveur FTP. Si cette option n'est pas transmise, Kaspersky Embedded Systems Security utilise si possible le mode de connexion passif.
`/TIMEOUT:<s>`	Argumentaire facultatif. Délai d'attente de connexion au serveur FTP ou HTTP, en secondes. Valeur par défaut : 10 secondes.
`/REG:<code_by_iso3166>`	Argumentaire facultatif. Code du pays dans lequel se trouve l'appareil protégé, conformément à la norme ISO 3166-1. Exemple : `/REG:GR`. Si ce paramètre est omis ou si un code de pays non valide est spécifié, Kaspersky Embedded Systems Security détermine l'emplacement en fonction des paramètres régionaux de l'appareil protégé sur lequel la Console de l'application est installée. L'application utilise les informations de localisation lors de la sélection d'un serveur de mise à jour.
`/W=<file path>`	Chemin et nom du fichier du journal d'exécution de la tâche. Un relancement de l'instruction selon les mêmes paramètres de consignation écrase le fichier journal existant.
`/ANSI`	Utilisez le codage ANSI pour les événements consignés dans le journal d'exécution de la tâche. Le paramètre `/ANSI` ne sera pas appliqué si le paramètre `/W` n'est pas transmis. Si le paramètre `/ANSI` n'est pas spécifié, Unicode est utilisé pour générer le journal d'exécution de la tâche.
`/ALIAS:<alternate name>`	Attribuez à la tâche un nom temporaire permettant de la référencer pendant son exécution. Par exemple, vous pouvez consulter les statistiques de la tâche à l'aide de la commande `KAVSHELL TASK`. Le nom alternatif de la tâche doit être unique parmi tous les noms alternatifs de tâches dans l'application. Si cet argument n'est pas transmis, le nom de la tâche est attribué comme suit : update_<kavshell_pid>. Par exemple : update_1234.
`/PWD:<password>`	Argumentaire facultatif. Mot de passe du compte utilisateur KLAdmin ou d'un compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le mot de passe sur la ligne suivante.
`/LOGIN:<user name>`	Argumentaire facultatif. Nom du compte utilisateur disposant des autorisations suffisantes. Si cette option n'est pas définie, l'application vous demandera le nom d'utilisateur sur la ligne suivante. Il n'est pas nécessaire de saisir cette valeur si vous avez saisi le mot de passe KLAdmin.

Syntaxe de la commande

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

Valeurs de retour de la commande :

- 0 : l'opération s'est terminée avec succès.
- 200 : Tous les objets sont à jour.
- -2 : le service n'est pas lancé.
- -3 : autorisations insuffisantes pour exécuter la commande.
- -5 : erreur de syntaxe.

- -99 : erreur inconnue.
- -206 : Les fichiers d'extension ne sont pas présents dans la source indiquée ou leur format est inconnu.
- -209 : Erreur de connexion à la source des mises à jour.
- -232 : Erreur d'authentification lors de la connexion au serveur proxy.
- -234 : Erreur de connexion à Kaspersky Security Center.
- -235 : Kaspersky Embedded Systems Security n'a pas subi d'authentification lors de la connexion à la source des mises à jour.
- -236 : Les bases de l'application sont corrompues.
- -301 : la licence n'est pas valide.

Contacter le Support Technique

Cette section explique comment obtenir le Support Technique et les conditions à remplir pour en profiter.

Modes d'obtention de l'assistance technique

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans d'autres sources d'informations relatives à Kaspersky Embedded Systems Security, contactez le Support technique. Les experts du Support technique répondront à vos questions sur l'installation et l'utilisation de Kaspersky Embedded Systems Security.

Kaspersky fournit une assistance pour Kaspersky Embedded Systems Security pendant son cycle de vie (consultez la page relative au cycle de vie de l'application). Avant de contacter le Support Technique, veuillez prendre connaissance des règles d'octroi de l'assistance technique.

Vous pouvez contacter les experts du Support technique d'une des manières suivantes :

- En visitant le site Internet du Support Technique
- Envoyer une demande au Support Technique de Kaspersky via le portail Kaspersky CompanyAccount

Assistance technique via Kaspersky CompanyAccount

Kaspersky CompanyAccount est un portail à disposition des entreprises qui utilisent les applications de Kaspersky. Le portail Kaspersky CompanyAccount est conçu pour permettre une interaction entre les utilisateurs et les experts de Kaspersky via des requêtes électroniques. Le portail Kaspersky CompanyAccount permet un suivi du traitement par les experts de Kaspersky des requêtes électroniques et propose un historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte utilisateur Kaspersky CompanyAccount. À l'aide d'un seul compte, vous pouvez centraliser l'administration des demandes électroniques envoyées par les employés à Kaspersky et gérer les droits d'accès de ces employés à Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe

- Français
- Japonais

Vous pouvez obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique.

Fourniture d'informations diagnostiques avancées aux experts du Support Technique

Pour améliorer l'efficacité de l'assistance et du dépannage des applications, le Support Technique peut vous demander de modifier temporairement les paramètres de l'application à des fins de débogage dans le cadre d'un diagnostic. Pour ce faire, il peut être nécessaire d'effectuer les opérations suivantes :

- Activation de la fonctionnalité de traitement et de stockage des informations de diagnostic avancées.
- Configuration détaillée des paramètres de chacun des modules logiciels, qui ne sont pas accessibles via les éléments standards de l'interface utilisateur.
- Modification des paramètres de stockage et de transmission des informations de diagnostic traitées.
- Configurer l'interception et l'enregistrement dans un fichier du trafic réseau.

Toutes les informations nécessaires à l'exécution des actions répertoriées (description du déroulement des opérations, des paramètres modifiables, des fichiers de configuration, des scripts, des fonctionnalités supplémentaires de la ligne de commande, des modules de débogage, des utilitaires spécialisés, etc.), ainsi que la composition des données analysées à des fins de débogage, seront données par les experts du Support Technique. Les informations diagnostiques avancées récupérées sont stockées sur l'ordinateur de l'utilisateur. La transmission automatique des données stockées vers Kaspersky n'a pas lieu.

Une fois que vous aurez communiqué votre problème aux experts du Support Technique, ceux-ci pourront vous demander de générer un rapport sur le fonctionnement de Kaspersky Embedded Systems Security à envoyer au Support Technique. Le personnel du Support Technique de Kaspersky peut également vous demander de créer un fichier de traçage, d'envoyer un fichier d'image mémoire, et de fournir un rapport à partir de l'utilitaire Kaspersky Get System Info.

L'analyse des données que vous envoyez permet aux experts du Support Technique de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet de rechercher la présence éventuelle de menaces dans les processus actifs, de rechercher la présence éventuelle de menaces sur l'ordinateur, de désinfecter ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

Les actions listées ci-dessus peuvent être exécutées uniquement sous la direction des experts du Support Technique en suivant les instructions reçues de leur part. La modification des paramètres de l'application sans assistance d'une manière non décrite dans la documentation de l'application ou dans les recommandations des experts du Support Technique peut entraîner des ralentissements et des dysfonctionnements du système d'exploitation, une baisse du niveau de protection de l'ordinateur, ainsi qu'une violation de la disponibilité et de l'intégrité des informations traitées.

Traçage du fonctionnement de l'application

Le *traçage de l'application* désigne l'enregistrement détaillé des activités de l'application et des messages sur les événements survenus pendant le fonctionnement de l'application. Au cours du processus de traçage, l'application crée un ensemble de fichiers avec les données relatives au fonctionnement des différents modules d'application.

Lancez le traçage de l'application conformément aux instructions du Support Technique de Kaspersky.

Les fichiers de traçage permettent de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

Comment activer et configurer le traçage des applications dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Diagnostic de dysfonctionnement**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.

   La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre sous l'onglet **Paramètres de traçage des applications**.
5. Utilisez la case **Activer le traçage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   Par défaut, le traçage du fonctionnement de l'application est désactivé.
6. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour cela, il faut indiquer le chemin d'accès complet au dossier local dans le champ **Dossier des fichiers de traçage**.

   Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

   Dans le dossier sélectionné, Kaspersky Embedded Systems Security crée un sous-dossier nommé « logs-Kaspersky Embedded Systems Security-<uid> » pour stocker les fichiers de traçage, où <uid> est un identifiant de journal unique à 8 caractères.
7. Sélectionnez le niveau de détail des informations de débogage :

   - **Normal** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application (option par défaut).
   - **Critique** signifie que le fichier de traçage enregistre uniquement les messages relatifs aux erreurs critiques.
   - **Diagnostic** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, ainsi que les avertissements.

- **Important** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements et des informations complémentaires.
- **Détaillé** signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.

Un opérateur du Support Technique détermine le niveau de détails requis pour résoudre un éventuel problème.

8. Pour supprimer les anciens fichiers de traçage, activez la fonctionnalité **Supprimer les fichiers de traçage les plus anciens**.

   Si cette fonctionnalité est activée, configurez la taille maximale et le nombre de fichiers de traçage :

   a. Définissez le paramètre **Taille maximale d'un fichier de traçage (Mo)**.

      Valeurs disponibles : de 1 à 4 095 Mo. La valeur par défaut est 100 Mo.

   b. Définissez le paramètre **Nombre maximal de fichiers pour un journal de traçage**.

      Valeurs disponibles : de 1 à 999. La valeur par défaut est 5.

9. Enregistrez vos modifications.

Comment activer et configurer le traçage des applications dans la Console de l'application

1. Dans l'arborescence de la console de l'application, sélectionnez le nœud **Kaspersky Embedded Systems Security** et réalisez l'une des actions suivantes :
   - Dans le panneau des résultats du nœud, cliquez sur le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez **Propriétés de l'application**.

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

2. Sélectionnez l'onglet **Diagnostic de dysfonctionnement**.

3. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.

   La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre.

4. Sélectionnez l'onglet des paramètres de traçage.
   - **Paramètres de traçage des applications**. Kaspersky Embedded Systems Security commence le traçage pour l'application.
   - **Paramètres de traçage de la Console de l'application**. Si la Console de l'application et Kaspersky Embedded Systems Security sont installés sur des ordinateurs différents, vous ne pouvez démarrer le traçage que pour la Console de l'application.

5. Utilisez la case **Activer le traçage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   Par défaut, le traçage du fonctionnement de l'application est désactivé.

6. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour ce faire, cliquez sur le bouton **Parcourir** et sélectionnez le dossier requis.

   Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

Dans le dossier sélectionné, Kaspersky Embedded Systems Security crée un sous-dossier nommé « logs-Kaspersky Embedded Systems Security-<uid> » pour stocker les fichiers de traçage, où <uid> est un identifiant de journal unique à 8 caractères.

7. Sélectionnez le niveau de détail des informations de débogage :

   - **Normal** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application (option par défaut).
   - **Critique** signifie que le fichier de traçage enregistre uniquement les messages relatifs aux erreurs critiques.
   - **Diagnostic** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, ainsi que les avertissements.
   - **Important** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements et des informations complémentaires.
   - **Détaillé** signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.

   Un opérateur du Support Technique détermine le niveau de détails requis pour résoudre un éventuel problème.

8. Pour supprimer les anciens fichiers de traçage, activez la fonctionnalité **Supprimer les fichiers de traçage les plus anciens**.

   Si cette fonctionnalité est activée, configurez la taille maximale et le nombre de fichiers de traçage :

   a. Définissez le paramètre **Taille maximale d'un fichier de traçage (Mo)**.

      Valeurs disponibles : de 1 à 4 095 Mo. La valeur par défaut est 100 Mo.

   b. Définissez le paramètre **Nombre maximal de fichiers pour un journal de traçage**.

      Valeurs disponibles : de 1 à 999. La valeur par défaut est 5.

9. Enregistrez vos modifications.

Comment activer et configurer le traçage des applications dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic de dysfonctionnement**.
5. Dans le groupe **Paramètres de diagnostic des dysfonctionnements**, utilisez la case **Activer le traçage des applications** pour activer ou désactiver le traçage du fonctionnement de l'application.

   Par défaut, le traçage du fonctionnement de l'application est désactivé.
6. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour cela, il faut indiquer le chemin d'accès complet au dossier local dans le champ **Dossier des fichiers de trace (chemin d'accès complet au dossier, par exemple : C:\\Traces\\)**.

Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

Dans le dossier sélectionné, Kaspersky Embedded Systems Security crée un sous-dossier nommé « logs-Kaspersky Embedded Systems Security-<uid> » pour stocker les fichiers de traçage, où <uid> est un identifiant de journal unique à 8 caractères.

7. Sélectionnez le niveau de détail des informations de débogage :

   - **Normal** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements, ainsi que des informations relatives au fonctionnement normal de l'application (option par défaut).
   - **Critique** signifie que le fichier de traçage enregistre uniquement les messages relatifs aux erreurs critiques.
   - **Diagnostic** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, ainsi que les avertissements.
   - **Important** signifie que le fichier de traçage enregistre les messages relatifs à toutes les erreurs, les avertissements et des informations complémentaires.
   - **Détaillé** signifie que le fichier de traçage enregistre toutes les informations relatives au fonctionnement de l'application.

   Un opérateur du Support Technique détermine le niveau de détails requis pour résoudre un éventuel problème.

8. Pour supprimer les anciens fichiers de traçage, activez la fonctionnalité **Supprimer les anciens fichiers de traçage**.

   Si cette fonctionnalité est activée, configurez la taille maximale et le nombre de fichiers de traçage :

   a. Définissez le paramètre **Taille maximale des fichiers de traçage (Mo)**.

      Valeurs disponibles : de 1 à 4 095 Mo. La valeur par défaut est 100 Mo.

   b. Définissez le paramètre **Nombre maximal de fichiers pour un journal de traçage**.

      Valeurs disponibles : de 1 à 999. La valeur par défaut est 5.

9. Enregistrez vos modifications.

Vous pouvez également activer et configurer le traçage de l'application dans l'Interface de diagnostic compacte et via la ligne de commande.

À propos de la composition et de la conservation des fichiers de traçage

Vous seul êtes responsable de la sécurité des informations récupérées, et plus exactement du contrôle et de la restriction de l'accès aux informations récupérées et conservées sur l'ordinateur avant leur envoi à Kaspersky.

Les fichiers de traçage sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application.

Les fichiers de traçage sont conservés dans le dossier suivant : %ProgramData%\Kaspersky Lab\KESS.4.1\Traces.

Les fichiers de traçage portent le nom suivant : KESS<4.1_dateXX.XX_timeXX.XX_pidXXX.><type de fichier de traçage>.log.

Vous pouvez consulter les données consignées dans les fichiers de traçage.

Tous les fichiers de traçage contiennent les données communes suivantes :

- Heure de l'événement
- Numéro du flux d'exécution
- Module de l'application à l'origine de l'événement
- Degré de gravité de l'événement (information, avertissement, critique, erreur)
- Description de l'événement d'exécution de la commande du module de l'application et résultat de l'exécution de cette commande.

Contenu des fichiers de traçage SRV.log, GUI.log et ALL.log

Les fichiers de traçage SRV.log, GUI.log et ALL.log peuvent contenir, outre les informations générales, les informations suivantes :

- Données personnelles, dont le nom de famille et le prénom si ces données font partie du chemin d'accès aux fichiers sur l'ordinateur local.
- Nom d'utilisateur et mot de passe s'ils sont transmis en clair. Ces données peuvent être consignées dans les fichiers de traçage lors de l'analyse du trafic Internet.
- Nom d'utilisateur et mot de passe s'ils figurent dans les en-têtes du protocole HTTP.
- Nom du compte utilisateur d'accès à Microsoft Windows, si celui-ci fait partie du nom du fichier.
- Votre adresse de messagerie électronique ou l'adresse Internet avec le nom du compte utilisateur et le mot de passe s'ils figurent dans le nom de l'objet détecté.
- Adresse du serveur proxy, nom de l'ordinateur, adresse IP, nom de l'utilisateur employé pour l'autorisation sur le serveur Proxy. Ces données sont consignées dans les fichiers de traçage si l'application utilise un serveur proxy.
- Adresses IP externes d'où la connexion avec votre ordinateur a été établie.
- Données de trafic réseau. Ces données sont écrites dans les fichiers de traçage si des modules de surveillance du trafic sont activés.
- Données reçues des serveurs de Kaspersky (par exemple, la version des bases antivirus).
- Statuts des modules de Kaspersky Embedded Systems Security et informations sur leur fonctionnement.
- Données sur les actions des utilisateurs dans l'application.
- Événements du système d'exploitation.

Contenu des fichiers de traçage HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Le fichier de traçage HST.log contient, outre les données générales, les informations relatives à l'exécution de la tâche de mise à jour des bases de données de l'application et des modules.

Le fichier de traçage BL.log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement de l'application, ainsi que les données indispensables à la résolution des problèmes de fonctionnement de l'application. Ce fichier est créé si l'application est lancée avec le paramètre avp.exe –bl.

Le fichier de traçage Dumpwriter.log contient, outre les données générales, les informations de service indispensables à la résolution des problèmes survenus pendant l'écriture du fichier dump de l'application.

Le fichier de traçage WD.log contient, outre les données générales, les informations sur les événements survenus pendant le fonctionnement du service avpsus, y compris les événements de mise à jour des modules de l'application.

Le fichier de traçage AVPCon.dll.log contient, outre les données générales, les informations relatives aux événements survenus pendant le fonctionnement du module de communication avec Kaspersky Security Center.

Contenu du fichier de traçage du module du scanner AMSI

Outre les données générales, le fichier de traçage AMSI.log contient des informations sur les résultats des analyses sollicitées par des applications tierces.

Contenu des fichiers de traçage des plug-ins Internet de l'application

Les fichiers de traçage du plug-in Internet de l'application sont conservés sur l'ordinateur doté de Kaspersky Security Center Web Console, dans le dossier Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

Les fichiers de traçage du plug-in Internet de l'application sont nommés de la manière suivante : logs-ess_windows-<type of trace file>.DESKTOP-<date of file update>.log. Web Console commence à enregistrer les données après l'installation et supprime les fichiers de traçage après sa suppression.

Les fichiers de traçage des plug-ins Internet de l'application contiennent, outre les données générales, les informations suivantes :

- le mot de passe de l'utilisateur KLAdmin pour le déverrouillage de l'interface de Kaspersky Embedded Systems Security ;
- le mot de passe temporaire pour le déverrouillage de l'interface de Kaspersky Embedded Systems Security ;
- le nom d'utilisateur et le mot de passe pour le serveur de messagerie SMTP ;
- le nom d'utilisateur et le mot de passe pour le serveur proxy ;

- Nom d'utilisateur et mot de passe pour la tâche *Modification de la sélection des modules de l'application* ;
- les identifiants et les chemins indiqués dans les propriétés de la stratégie et les tâches de Kaspersky Embedded Systems Security.

Enregistrement des vidages de la mémoire

Le fichier de vidage de la mémoire contient toutes les informations relatives à la mémoire de travail des processus de Kaspersky Embedded Systems Security au moment de la défaillance de l'application.

Les fichiers de vidage de mémoire sont conservés sur votre ordinateur pendant toute la durée d'utilisation de l'application et sont supprimés de manière définitive lors de la suppression de l'application.

> Les vidages enregistrés peuvent contenir des données confidentielles. Pour contrôler l'accès aux données, vous devez garantir vous-même la protection des fichiers de vidage de mémoire.

Par défaut, les fichiers de vidage de la mémoire sont stockés dans le dossier suivant : %ProgramData%\Kaspersky Lab\KESS.4.1\Traces.

Comment activer ou désactiver l'enregistrement du vidage de la mémoire dans la Console d'administration de Kaspersky Security Center

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Diagnostic de dysfonctionnement**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.

   La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre sous l'onglet **Paramètres de traçage des applications**.
5. Sélectionnez l'onglet **Paramètres de vidage des applications**.
6. Utilisez la case **Créer un fichier de vidage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   L'enregistrement du vidage de la mémoire est désactivé par défaut.
7. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour cela, il faut indiquer le chemin d'accès complet au dossier local dans le champ **Dossier des fichiers de vidage**.

   > Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.
8. Enregistrez vos modifications.

Comment activer ou désactiver l'enregistrement du vidage de la mémoire dans la Console de l'application

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

   - Dans le panneau des résultats du nœud, cliquez sur le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez **Propriétés de l'application**.

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

2. Sélectionnez l'onglet **Diagnostic de dysfonctionnement**.

3. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.

   La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre.

4. Ouvrez l'onglet des paramètres de vidage :

   - **Paramètres de vidage des applications**. Kaspersky Embedded Systems Security enregistre tous les vidages de l'application.
   - **Paramètres de vidage de la Console des applications**. Si la Console de l'application et Kaspersky Embedded Systems Security sont installés sur des ordinateurs différents, vous ne pouvez enregistrer des vidages que pour la Console de l'application.

5. Utilisez la case **Créer un fichier de vidage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   L'enregistrement du vidage de la mémoire est désactivé par défaut.

6. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour ce faire, cliquez sur le bouton **Parcourir** et sélectionnez le dossier requis.

   Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

7. Enregistrez vos modifications.

Comment activer ou désactiver l'enregistrement du vidage de la mémoire dans Kaspersky Security Center Web Console

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.

2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.

3. Sélectionnez l'onglet **Paramètres de l'application**.

4. Sélectionnez la section **Diagnostic de dysfonctionnement**.

5. Dans le groupe **Paramètres des fichiers de vidage**, utilisez la case **Créer un fichier de vidage** pour activer ou désactiver le traçage du fonctionnement de l'application.

   L'enregistrement du vidage de la mémoire est désactivé par défaut.

6. Si nécessaire, modifiez le dossier par défaut dans lequel Kaspersky Embedded Systems Security enregistrera les fichiers de traçage. Pour cela, il faut indiquer le chemin d'accès complet au dossier local dans le champ **Dossier des fichiers de vidage (chemin d'accès complet au dossier, par exemple : C:\\Dumps\\)**.

   Le dossier doit être créé au préalable et être accessible en écriture pour le compte SYSTEM. Vous ne pouvez pas indiquer un dossier réseau, un disque ou des variables d'environnement.

7. Enregistrez vos modifications.

Vous pouvez également activer ou désactiver l'enregistrement du vidage de la mémoire dans l'Interface de diagnostic compacte.

Protection des fichiers dump et de traçage

Les fichiers dump et les fichiers de traçage contiennent des informations sur le système d'exploitation, ainsi que des données de l'utilisateur. Pour empêcher l'accès non autorisé à ces données, vous pouvez activer la protection des fichiers dump et des fichiers de traçage.

Si la protection des fichiers de vidage et des fichiers de traçage est activée, l'accès aux fichiers est réservé aux utilisateurs suivants :

- Les fichiers dump sont accessibles aux administrateurs local et système ainsi qu'à l'utilisateur qui a activé l'enregistrement des fichiers dump et des fichiers de traçage.
- Les fichiers de traçage sont accessibles uniquement aux administrateurs local et système.

Comment activer la protection des fichiers dump et des fichiers de traçage dans la Console d'administration de Kaspersky Security Center

1. Dans la fenêtre principale de Web Console, sélectionnez **Gestion des ressources → Stratégies**.
2. Cliquez sur le nom de la stratégie de Kaspersky Embedded Systems Security.

   La fenêtre des propriétés de la stratégie s'ouvre.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Sélectionnez la section **Diagnostic de dysfonctionnement**.
5. Utilisez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage.
6. Enregistrez vos modifications.

1. Dans l'arborescence de la Console d'administration de Kaspersky Security Center, sélectionnez **Stratégies**.
2. Sélectionnez la stratégie requise et ouvrez les propriétés de la stratégie d'un double-clic.
3. Dans la fenêtre des propriétés de la stratégie, accédez à la section **Diagnostic de dysfonctionnement**.
4. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.
5. La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre.

6. Utilisez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage.

7. Enregistrez vos modifications.

Comment activer la protection des fichiers dump et des fichiers de traçage dans la Console de l'application

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

   - Dans le panneau des résultats du nœud, cliquez sur le lien **Propriétés de l'application**.
   - Dans le menu contextuel du nœud, sélectionnez **Propriétés de l'application**.

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

2. Sélectionnez l'onglet **Diagnostic de dysfonctionnement**.

3. Cliquez sur le bouton **Paramètres** dans le groupe **Paramètres de diagnostic des dysfonctionnements**.

   La fenêtre **Paramètres de diagnostic des dysfonctionnements** s'ouvre.

4. Utilisez la case **Activer la protection des fichiers de vidage et des fichiers de traçage** pour activer ou désactiver la protection des fichiers dump et des fichiers de traçage.

5. Enregistrez vos modifications.

Vous pouvez également activer ou désactiver la protection des fichiers dump et des fichiers de traçage dans le module Interface de diagnostic compacte.

Les fichiers dump et les fichiers de traçage enregistrés alors que la protection étaient activées resteront protégés même après la désactivation de cette fonction.

Obtention des données relatives au système d'exploitation (Kaspersky Get System Info)

Après l'installation de l'application Kaspersky Embedded Systems Security, le système d'exploitation ou l'application peuvent ne pas fonctionner correctement. Il existe un conflit entre l'application et le logiciel ou les pilotes des modules de l'ordinateur.

Afin de déterminer la cause du problème, le Support technique de Kaspersky a besoin d'un rapport créé par l'utilitaire Kaspersky Get System Info (ci-après, GSI). Pour en savoir plus sur l'utilisation de cet utilitaire, consultez la Base des connaissances de Kaspersky.

Sources d'informations sur Kaspersky Embedded Systems Security

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

- Page de Kaspersky Embedded Systems Security sur le site Internet de Kaspersky
- Page de Kaspersky Embedded Systems Security sur le site du Support Technique (Base de connaissances)
- Aide en ligne
- Discussions sur l'application dans le forum

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

Il peut être impossible d'afficher l'aide en ligne dans un navigateur qui ne prend pas en charge les protocoles de chiffrement modernes.

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

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

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

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

Page de Kaspersky Embedded Systems Security dans la base des connaissances

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

La page de Kaspersky Embedded Systems Security dans la Base des connaissances permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la Base de connaissances peuvent répondre à des questions qui concernent non seulement Kaspersky Embedded Systems Security, mais également d'autres applications de Kaspersky. Ces articles peuvent également contenir des actualités du Support technique.

Aide de Kaspersky Embedded Systems Security

L'aide en ligne contient des informations relatives à la configuration et à l'utilisation de Kaspersky Embedded Systems Security.

Discussions sur l'application dans le forum

Si votre question ne requiert pas de réponse urgente, vous pouvez en discuter avec les experts de Kaspersky et d'autres utilisateurs dans notre Forum.

Dans le Forum, vous pouvez afficher les sujets existants, publier vos propres commentaires et créer des sujets de discussion.

Annexes

Cette section contient des informations qui viennent compléter le texte principal.

Extensions de fichier pour analyse rapide

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64 Ko ;

exe : fichier exécutable, archive autoextractible ;

sys : fichier système Microsoft Windows ;

prg : texte du programme dBase™, Clipper ou Microsoft Visual FoxPro®, programme de la suite WAVmaker ;

bin : fichier binaire ;

bat : fichier de paquet ;

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2 ;

dpl : bibliothèque Borland Delphi compressée ;

dll : bibliothèque dynamique ;

scr : fichier d'économiseur d'écran de Microsoft Windows ;

cpl : module du panneau de configuration de Microsoft Windows ;

ocx : objet Microsoft OLE (Object Linking and Embedding) ;

tsp : programme qui fonctionne en mode de partage du temps ;

drv : pilote d'un appareil quelconque ;

vxd : pilote d'un appareil virtuel Microsoft Windows ;

pif : fichier contenant des informations sur un logiciel ;

lnk : fichier lien dans Microsoft Windows ;

reg : fichier d'enregistrement des clés de la base de registre de Microsoft Windows ;

ini : fichier de configuration qui contient les données des paramètres pour Microsoft Windows, Windows NT et pour certaines applications ;

cla : classe Java ;

vbs : script Visual Basic® ;

vbe : extension vidéo BIOS ;

js, jse : texte source JavaScript ;

htm : document hypertexte ;

htt : préparation hypertexte de Microsoft Windows ;

hta : programme hypertexte pour Microsoft Internet Explorer® ;

asp : script Active Server Pages ;

chm : fichier HTML compilé ;

pht : fichier HTML avec scripts PHP intégrés ;

php : script intégré dans les fichiers HTML ;

wsh : fichier Microsoft Windows Script Host ;

wsf : script Microsoft Windows ;

the : fichier du bureau de Microsoft Windows 95 ;

hlp : fichier d'aide au format Win Help ;

msg : email de Microsoft Mail ;

plg : email ;

mbx : email Microsoft Office Outlook enregistré ;

doc* : documents Microsoft Office Word, par exemple, doc : document Microsoft Office Word, docx : document Microsoft Office Word 2007 compatible avec XML, docm : document Microsoft Office Word 2007 compatible avec les macros ;

dot* : modèles de document Microsoft Office Word, par exemple, dot : modèle de document Microsoft Office Word, dotx : modèle de document Microsoft Office Word 2007, dotm : modèle de document Microsoft Office Word 2007 compatible avec les macros ;

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro ;

rtf : document au format Rich Text Format ;

shs : fragment de Windows Shell Scrap Object Handler ;

dwg : base de données de dessins AutoCAD® ;

msi : paquet Microsoft Windows Installer ;

otm : projet VBA pour Microsoft Office Outlook ;

pdf : document Adobe Acrobat ;

swf : objet d'un paquet Shockwave® Flash ;

jpg, jpeg : fichier graphique de conservation de données compressées ;

emf : fichier au format Enhanced Metafile ;

ico : fichier d'icône d'un objet ;

ov? : fichiers exécutables Microsoft Office Word ;

xl* : les documents et les fichiers de Microsoft Office Excel, tels que, xla : extension Microsoft Excel, xlc : schéma, xlt : modèle des documents, xlsx : feuille de calcul Microsoft Office Excel 2007, xltm : feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, xlsb : feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), xltx : modèle Microsoft Office Excel 2007, xlsm : modèle Microsoft Office Excel 2007 compatible avec les macros, xlam : modèle externe Microsoft Office Excel 2007 compatible avec les macros ;

pp* : les documents et les fichiers de Microsoft Office PowerPoint®, tels que, pps : diaporama Microsoft Office PowerPoint, ppt : présentation, pptx : présentation Microsoft Office PowerPoint 2007, pptm : présentation Microsoft Office PowerPoint 2007 compatible avec les macros, potx : modèle de présentation Microsoft Office PowerPoint 2007, potm : modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, ppsx : diaporama Microsoft Office PowerPoint 2007, ppsm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, ppam : module externe Microsoft Office PowerPoint 2007 compatible avec les macros ;

md* : documents et fichiers de Microsoft Office Access® tels que, mda : groupe de travail de Microsoft Office Access, mdb : base de données ;

sldx : diaporama Microsoft Office PowerPoint 2007 ;

sldm : diaporama Microsoft Office PowerPoint 2007 compatible avec les macros ;

thmx : thème Microsoft Office 2007.

Comptes utilisateurs dans les règles des modules d'application

Pour configurer certains modules de l'application, vous devez ajouter des règles spéciales dans lesquelles vous pouvez sélectionner les utilisateurs auxquels l'application appliquera la règle.

Pour la configuration des modules d'application suivants, il est nécessaire d'ajouter des règles :

- Contrôle du lancement des applications
- Contrôle des appareils
- Détection comportementale
- Contrôle de l'intégrité du système

Vous pouvez ajouter des utilisateurs comme suit :

- Sélectionner les utilisateurs dans Active Directory (recommandé)
- Sélectionner les utilisateurs dans la liste des utilisateurs de Kaspersky Security Center
- Ajouter manuellement

Kaspersky recommande l'utilisation de comptes utilisateurs locaux uniquement dans les cas particuliers où il n'est pas possible d'utiliser les comptes utilisateurs du domaine. Pour en savoir plus sur les risques de sécurité liés à l'utilisation de comptes locaux, consultez la Base de connaissances Microsoft. Vous assumez l'entière responsabilité de la sécurité de l'ordinateur en cas d'utilisation de comptes utilisateurs locaux. En particulier, cela inclut la responsabilité de contrôler et de limiter l'accès aux paramètres de l'application.

L'application utilise le SID (Security Identifier) de l'utilisateur pour identifier les utilisateurs. Lors de l'utilisation de comptes utilisateurs depuis Active Directory ou depuis la liste des utilisateurs de Kaspersky Security Center, l'application détermine le SID sur le Serveur d'administration. Cela signifie que l'application n'impose pas de charge supplémentaire à l'ordinateur pour identifier l'utilisateur. Si vous avez ajouté plus de 1 000 comptes utilisateurs locaux à une règle d'application, l'application contacte le contrôleur de domaine pour identifier l'utilisateur. Cela signifie que la charge de l'ordinateur est augmentée. Pour optimiser l'impact sur les performances de l'ordinateur, nous vous recommandons d'utiliser des comptes utilisateurs d'Active Directory ou de la liste des utilisateurs de Kaspersky Security Center.

Kaspersky Embedded Systems Security prend en charge les comptes utilisateurs et les groupes intégrés (par exemple, le groupe « Tout le monde ») dans les règles. En raison des particularités de la détection du SID de l'utilisateur, l'application ne permet d'utiliser que des comptes utilisateurs intégrés ajoutés à partir d'Active Directory ou de la liste des utilisateurs de Kaspersky Security Center. Les règles dans lesquelles le compte intégré est ajouté manuellement ne fonctionnent pas.

Informations légales

À propos des données

Cette section contient des informations sur les données que l'application Kaspersky Embedded Systems Security peut stocker sur l'appareil et transmettre automatiquement à Kaspersky pendant son fonctionnement.

Les informations obtenues par Kaspersky sont protégées conformément à la législation en vigueur et aux politiques de Kaspersky. Les données sont transmises via des canaux de communication chiffrés.

À propos des données dans le cadre du Contrat de licence utilisateur final

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

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

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

Lors de la désinstallation de Kaspersky Embedded Systems Security, toutes les données stockées par Kaspersky Embedded Systems Security sur l'appareil protégé sont supprimées.

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

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

Traitement des données locales

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

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

Traitement et stockage des données contenues dans les rapports

Domaine fonctionnel	Enregistrement des événements
Type d'utilisation	Kaspersky Embedded Systems Security stocke les données localement et les envoie au Serveur d'administration. La base de données du Serveur d'administration stocke des informations sur les événements de l'application qui se produisent sur les appareils protégés administrés.
Stockage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<version du produit>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Base de données du Serveur d'administration
Mesures de sécurité	Liste de contrôle de l'accès.
Période de stockage	Kaspersky Embedded Systems Security stocke les données jusqu'à la désinstallation de Kaspersky Embedded Systems Security. Lors de la désinstallation de Kaspersky Embedded Systems Security, toutes les données stockées par Kaspersky Embedded Systems Security sur l'appareil protégé sont supprimées.
Fonction	Fournir une fonctionnalité principale.

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

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

- Noms, sommes de contrôle (MD5, SHA-256) et attributs des fichiers traités et leurs chemins d'accès complets sur le support numérisé.
- Actions réalisées sur les fichiers analysés par Kaspersky Embedded Systems Security.
- Actions réalisées par l'utilisateur sur les fichiers analysés sur l'appareil protégé.
- Informations sur les comptes d'utilisateurs effectuant des actions sur le réseau protégé ou l'appareil protégé.
- Valeurs du chemin d'accès à l'instance de l'appareil pour les appareils ajoutés aux règles du Contrôle des appareils.
- Informations sur les processus et scripts exécutés sur le système : sommes de contrôle (MD5, SHA-256) et chemins d'accès complets aux fichiers exécutables, informations relatives aux certificats numériques.
- Paramètres du pare-feu Windows.
- Entrées du journal des événements Windows.
- Noms des comptes utilisateur exécutant des actions sur les fichiers analysés sur l'appareil protégé.

- Instances de fichiers exécutables en cours de démarrage et types, noms, sommes de contrôle et attributs de ces fichiers.
- Informations sur l'activité réseau :
  - Adresses IP des appareils externes bloqués.
  - Adresses IP traitées.
- Informations sur l'état du journal Windows USN.

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

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

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

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

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

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

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

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

Kaspersky Embedded Systems Security vous permet de configurer le niveau de protection des données traitées localement. Vous pouvez modifier les privilèges d'accès des utilisateurs aux données traitées, modifier les périodes de conservation de ces données, désactiver entièrement ou partiellement la fonctionnalité qui implique l'enregistrement des événements dans le journal des données et modifier le chemin et les attributs du dossier où les données sont enregistrées.

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

Par défaut, toutes les données traitées localement par l'application en cours de fonctionnement sont supprimées après la désinstallation de Kaspersky Embedded Systems Security de l'appareil protégé.

Les fichiers contenant les informations de diagnostic (fichiers de traçage et fichiers de vidage), les événements de l'application dans le journal des événements Windows et les fichiers contenant les paramètres exportés de Kaspersky Embedded Systems Security constituent une exception. Nous vous recommandons de supprimer ces fichiers manuellement.

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

Vous pouvez supprimer les fichiers du journal des événements Windows contenant les événements des applications Kaspersky Embedded Systems Security à l'aide des outils standard du système d'exploitation.

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

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

- Console de l'application. Le module est un module logiciel enfichable Microsoft Management Console.
- Plug-in d'administration. Ce module assure une intégration complète avec l'application Kaspersky Security Center.

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

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

- Console de l'application : nom de l'appareil protégé hébergeant Kaspersky Embedded Systems Security (adresse IP ou nom de domaine) auquel la Console de l'application s'est connectée à distance la dernière fois ; paramètres d'affichage configurés dans le module logiciel enfichable Microsoft Management Console ; données concernant le dernier dossier dans lequel l'utilisateur a sélectionné des objets via la Console de l'application (à l'aide d'une boîte de dialogue ouverte via le bouton **Parcourir**). Les fichiers de traçage de la Console de l'application peuvent également contenir les données suivantes : nom de l'appareil protégé hébergeant l'application Kaspersky Embedded Systems Security auquel la connexion à distance a été effectuée, nom du compte utilisateur sous lequel la connexion à distance a été établie.
- Le Plug-in d'administration peut traiter et stocker temporairement des données traitées par Kaspersky Embedded Systems Security ; par exemple les paramètres configurés des tâches et des modules de l'application, les paramètres des stratégies de Kaspersky Security Center, les données envoyées dans les listes de réseau.

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

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

- Informations sur les actions effectuées par Kaspersky Embedded Systems Security sur l'appareil protégé.
- Informations relatives aux objets traités par Kaspersky Embedded Systems Security.
- Informations sur l'activité sur l'appareil protégé traitées par Kaspersky Embedded Systems Security.
- Informations relatives aux erreurs survenues lors de l'exécution de Kaspersky Embedded Systems Security.

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

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

Les fichiers de traçage des modules auxiliaires de l'application constituent la seule exception. Nous vous recommandons de supprimer ces fichiers manuellement.

Données dans les fichiers de vidage et de traçage

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

Les fichiers de vidage de Kaspersky Embedded Systems Security sont générés par le système d'exploitation lors des échecs d'application et sont écrasés par l'échec suivant.

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

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

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

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

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

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

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

Les données des fichiers de vidage et de traçage peuvent contenir :

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

Collecte des données dans le cadre de l'utilisation de Kaspersky Security Network

L'ensemble des données que Kaspersky Embedded Systems Security envoie à Kaspersky dépend du type de licence et des paramètres d'utilisation de Kaspersky Security Network.

Utilisation de KSN sous licence sur un maximum de 4 ordinateurs

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

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

Utilisation de KSN sous licence sur 5 ordinateurs ou plus

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

Si la case **Kaspersky Security Network** est cochée alors que la case **Activer le mode étendu de KSN** est décochée, l'application transmet les informations suivantes :

- informations relatives à la mise à jour de la configuration de KSN : identifiant de la configuration active, identifiant de la configuration reçue, code d'erreur de mise à jour de la configuration ;
- informations sur les fichiers et les adresses Internet analysés : sommes de contrôle du fichier analysé (MD5, SHA2-256, SHA1) et profils de fichier (MD5), taille du profil, type de menace détectée et son nom conformément à la classification du Titulaire des droits, identifiant des bases antivirus, adresse Internet pour laquelle la réputation est sollicitée, adresse Internet depuis laquelle l'accès à l'adresse Internet à analyser a eu lieu, identifiant du protocole de connexion et numéro du port utilisé ;
- identifiant de la tâche d'analyse qui a détecté la menace ;

- informations sur les certificats numériques utilisés requises pour vérifier leur authenticité : sommes de contrôle du certificat (SHA256) utilisé pour signer l'objet à analyser, clé publique du certificat ;

- identificateur du module de l'application qui exécute l'analyse ;

- identificateurs des bases antivirus et enregistrements dans les bases antivirus ;

- informations relatives à l'activation de l'application sur l'ordinateur ; en-tête signé du ticket du service d'activation (identificateur du centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identificateur unique du ticket, version du ticket, état de la licence, date et heure du début de fin de validité du ticket, identificateur unique de licence, version de la licence), identificateur du certificat utilisé pour signer les en-têtes du ticket, somme de contrôle (MD5) du fichier clé ;

- informations relatives à l'application du Titulaire des droits : version complète, type, version du protocole utilisé dans le cadre de la connexion aux services de Kaspersky.

Si en plus de la case **Kaspersky Security Network** vous cochez la case **Activer le mode étendu de KSN**, l'application transmet en plus les informations suivantes :

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

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

- informations sur l'état de la protection antivirus de l'Ordinateur : versions, dates et heures de publication des bases antivirus utilisées, identifiant de la tâche et identifiant du Logiciel qui effectue l'analyse ;

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

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

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

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

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

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

- adresses IP de l'ordinateur à l'origine de l'attaque (IPv4 et IPv6), numéro du port de l'Ordinateur cible de l'attaque de réseau, identifiant du protocole du paquet IP contenant l'attaque, cible de l'attaque (nom de l'entreprise, site Web), indicateur de la réaction à l'attaque, poids de l'attaque, niveau de confiance ;

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

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

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

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

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

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

- si un objet potentiellement malveillant est détecté, les informations relatives aux données présentes dans la mémoire des processus (éléments de la hiérarchie système des objets (ObjectManager), données de la mémoire BIOS UEFI, noms et valeurs des clés de Registre) seront fournies ;

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

- informations relatives aux connexions réseau : version et sommes de contrôle (MD5, SHA2-256, SHA1) du fichier à partir desquels le processus qui a ouvert le port a été démarré, chemin d'accès au fichier du processus et sa signature numérique, adresses IP locale et distante, numéros des ports de connexion local et distant, état de la connexion, horodatage de l'ouverture du port ;

- informations sur la date d'installation et d'activation du Logiciel sur l'Ordinateur : identifiant du partenaire qui a vendu la licence, numéro de série de la licence, en-tête signé du ticket du service d'activation (identifiant d'un centre d'activation régional, somme de contrôle du code d'activation, somme de contrôle du ticket, date de création du ticket, identifiant unique du ticket, version du ticket, état de la licence, date et heure de début/fin du ticket, identifiant unique de la licence, version de la licence), identifiant du certificat utilisé pour signer l'en-tête du ticket, somme de contrôle (MD5) du fichier clé, identifiant unique de l'installation du Logiciel sur l'Ordinateur, type et identifiant de l'application qui est mise à jour, identifiant de la tâche de mise à jour ;

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

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

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

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

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

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

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

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

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

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

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

- informations sur l'outil de trace des événements Windows (Event Tracing for Windows, ETW) lors de problèmes de performances de l'application, fournisseurs d'événements SysConfig/SysConfigEx/WinSATAssessment de Microsoft : données sur l'ordinateur (modèle, fabricant, facteur de forme, version), données sur les indicateurs de performance Windows (données de l'évaluation WinSAT, indice de performance Windows), nom du domaine, données sur les processus physiques et logiques (nombre de processeurs physiques et logiques, fabricant, modèle, stepping, nombre de noyaux, fréquence d'horloge, identificateur de processeur (CPUID), caractéristiques du cache, caractéristiques du processeur logique, indice de prise en charge des modes et des instructions), données sur les modules de la mémoire vive (type, facteur de forme, fabricant, modèle, volume, granularité de l'allocation de la mémoire), données sur les interfaces réseau (adresses IP et MAC, nom, description, configuration des interfaces réseau, répartition du nombre et du volume de paquets réseau par type, vitesse de l'échange réseau, distribution du nombre d'erreurs réseau par type), configuration du contrôleur IDE, adresses IP des serveurs DNS, données sur la carte vidéo (modèle, description, fabricant, compatibilité, volume de mémoire vidéo, résolution de l'écran, nombre de bits par pixel, version du BIOS), données sur les appareils Plug-and-Play (nom, description, identificateur d'appareil [PnP, ACPI], données relatives aux disques et supports (nombre de disques ou de clés USB, fabricant, modèle, volume de disque, nombre de tambours, nombre de pistes par tambour, nombre de partitions par piste, volume de secteur, caractéristiques du cache, numéro de séquence, nombre de partitions, configuration du contrôleur SCSI), données sur les disques logiques (numéro de séquence, volume de la partition, taille du volume, lettre du volume, type de partition, type de système de fichiers, nombre de clusters, taille du cluster, nombre de secteurs dans un cluster, nombre de clusters occupés et disponibles, lettre du volume d'amorçage, déplacement de la partition par rapport au début du disque), données sur le BIOS de la carte-mère (fabricant, date de fabrication, version), données sur la mémoire physique (volume total et disponible), données sur les services du système d'exploitation (nom, description, état, tag, données sur les processus [nom et identificateur PID]), paramètres de consommation de l'ordinateur, configuration du contrôleur d'interruptions, chemin d'accès aux dossiers système Windows (Windows et System32), données sur le système d'exploitation (version, build, date d'édition, nom, type, date d'installation), taille du fichier de débogage, données sur les écrans (nombre, fabricant, résolution de l'écran, pouvoir de résolution, type), données sur le pilote de la carte vidéo (fabricant, date de sortie, version) ;

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

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

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

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

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

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

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

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

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

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

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

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

- informations sur le Logiciel du Titulaire des droits : version complète, type, localisation et état de fonctionnement du Logiciel utilisé, versions des modules du Logiciel installés et leur état de fonctionnement, informations sur les mises à jour du Logiciel installé, valeur du filtre TARGET, version du protocole utilisé pour se connecter aux services du Titulaire des droits ;

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

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

- fichiers exécutables et non exécutables, en tout ou en partie ;

- parties de la mémoire RAM de l'Ordinateur ;

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

- les paquets de données du trafic réseau ;

- les pages Web et les emails contenant des objets malveillants et suspects ;

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

- rapports d'activités des applications :

    - nom, taille et version du fichier à envoyer, sa description et ses sommes de contrôle (MD5, SHA2-256, SHA1), identifiant du format, nom de son éditeur, nom du produit associé au fichier, chemin d'accès complet au fichier sur l'Ordinateur et code du modèle de chemin, date et heure de création et de modification du fichier ;

    - date et heure de début et de fin de validité du certificat (si le fichier possède une signature numérique), date et heure de la signature, nom de l'émetteur du certificat, informations relatives au détenteur du certificat, empreinte, clé publique et algorithmes appropriés du certificat, numéro de série du certificat ;

    - nom du compte utilisateur sous lequel le processus a été lancé ;

    - sommes de contrôle (MD5, SHA2-256, SHA1) du nom de l'Ordinateur sur lequel le processus est lancé ;

    - titres des fenêtres du processus ;

- identifiant des bases antivirus, nom de la menace détectée conformément à la classification de Détenteur des droits ;
- données relatives à la licence installée, son identifiant, son type et sa date d'expiration ;
- heure locale de l'Ordinateur au moment de la collecte des informations ;
- noms et chemins d'accès aux fichiers auxquels le processus a accédé ;
- noms des clés du registre, ainsi que leurs valeurs, auxquelles le processus a accédé ;
- URL et adresses IP auxquelles le processus a accédé ;
- URL et adresses IP à partir desquelles le fichier en cours d'exécution a été téléchargé.

Respect de la législation de l'Union européenne (RGPD)

Il se peut que Kaspersky Embedded Systems Security transmette des données à Kaspersky dans les cas suivants :

- Utilisation de Kaspersky Security Network.
- Activation de l'application à l'aide d'un code d'activation.
- Mise à jour des modules d'application et des bases antivirus.
- Consultation de liens dans la Console de l'application.

Indépendamment de la classification des données et du territoire à partir duquel les données sont reçues, Kaspersky adhère à des normes élevées de sécurité des données et emploie diverses mesures juridiques, organisationnelles et techniques pour protéger les données des utilisateurs, pour garantir la sécurité et la confidentialité des données, mais également pour assurer le respect des droits des utilisateurs, conformément à la législation applicable. Le texte de la politique de confidentialité est inclus dans le kit de distribution de l'application et est accessible sur le site de Kaspersky.

Avant d'utiliser Kaspersky Embedded Systems Security, veuillez lire attentivement la description des données transmises dans le Contrat de licence utilisateur final et la Déclaration de Kaspersky Security Network (repris dans la déclaration de Kaspersky Security Network). Si des données particulières transmises par Kaspersky Embedded Systems Security dans l'un des cas de figure décrits peuvent être classées comme des données personnelles selon la législation ou la norme locale, vous devez vous assurer que ces données sont traitées légalement et obtenir le consentement des utilisateurs finaux pour collecter et transmettre ces données.

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

Si vous ne souhaitez pas transmettre de données à Kaspersky, vous pouvez désactiver la collecte de données.

Utilisation de Kaspersky Security Network

En utilisant Kaspersky Security Network, vous acceptez de fournir automatiquement les données mentionnées dans la Déclaration de Kaspersky Security Network. Si vous n'acceptez pas de fournir ces données à Kaspersky, utilisez Kaspersky Private Security Network (KPSN) ou désactivez l'utilisation de KSN.

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

En utilisant un code d'activation, vous acceptez de fournir automatiquement les données mentionnées dans le Contrat de licence utilisateur final. Si vous ne voulez pas fournir ces données à Kaspersky, activez Kaspersky Embedded Systems Security à l'aide du fichier clé.

Mise à jour des modules d'application et des bases antivirus

En utilisant les serveurs de Kaspersky, vous acceptez de fournir automatiquement les données mentionnées dans le Contrat de licence utilisateur final. Kaspersky demande ces informations pour vérifier que Kaspersky Embedded Systems Security est utilisé de manière légitime. Si vous n'acceptez pas de fournir ces informations à Kaspersky, utilisez Kaspersky Security Center pour mettre à jour les bases de données.

Consultation de liens dans la Console de l'application.

En utilisant les liens figurant dans la Console de l'application, vous acceptez de fournir automatiquement les données mentionnées dans le Contrat de licence utilisateur final. La liste exacte des données transmises dans chaque lien concret dépend de l'emplacement exact du lien dans la Console de l'application et du problème qu'il est censé résoudre. Si vous n'acceptez pas la communication de ces informations à Kaspersky, désactivez l'affichage de l'interface de l'application.

Informations sur le code tiers

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le fichier d'installation de l'application.

Notice sur les marques de commerce

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Apache est soit une marque déposée, soit une marque de commerce d'Apache Software Foundation aux États-Unis et/ou dans d'autres pays.

Citrix, XenApp et XenDesktop sont des marques déposées ou des marques de commerce de Cloud Software Group, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays.

CVE est une marque déposée de The MITRE Corporation.

Dell Technologies, Dell, Dell Compellent et les autres marques sont des marques de commerce de Dell Inc. ou de ses filiales.

EMC, Celerra, Isilon, OneFS et VNX sont des marques ou des marques déposées d'EMC Corporation enregistrées aux États-Unis et/ou dans d'autres pays.

Hitachi est une marque de commerce d'Hitachi, Ltd.

Linux est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server et Windows Vista sont des marques de commerce du groupe Microsoft.

NetApp et Data ONTAP sont des marques de commerce ou des marques déposées de NetApp, Inc. aux États-Unis et/ou dans d'autres pays.

Oracle est une marque déposée de la société Oracle et/ou de ses filiales.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, licenciée exclusivement via X/Open Company Limited.