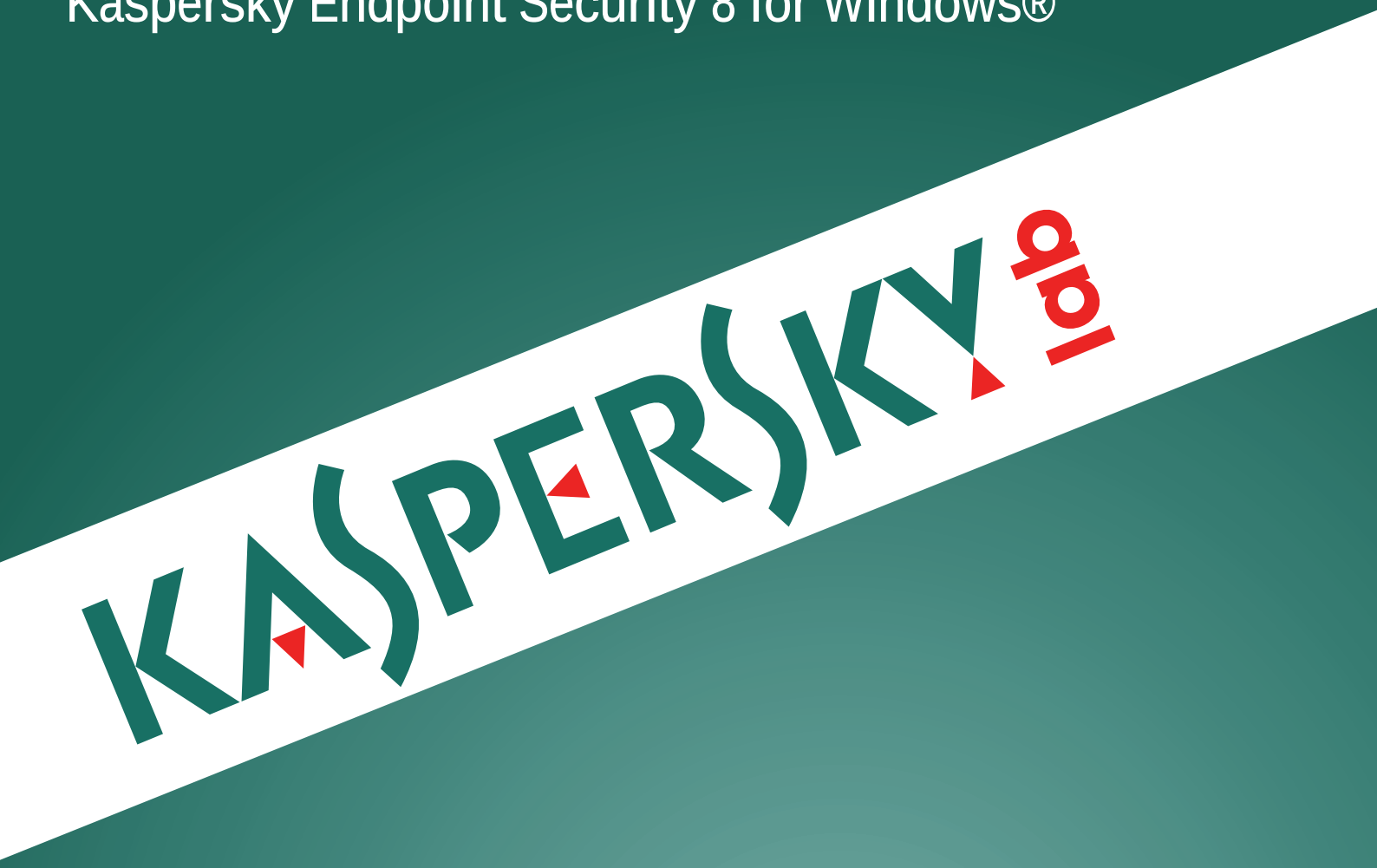
Kaspersky Endpoint Security 8 for Windows®



Manuel d'administrateur

VERSION DE L'APPLICATION : 8.0

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Ce document peut être modifié sans un avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse http://www.kaspersky.fr/docs.

Date d'édition : 30/09/2011

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

TABLE DES MATIERES

PRESENTATION DU GUIDE

Le présent document est un guide de l'administrateur de Kaspersky Endpoint Security 8 for Windows (ci-après : "Kaspersky Endpoint Security").

Ce Guide est un outil pour les administrateurs de réseaux locaux d'entreprise et pour les responsables de protection antivirus. Ce Guide peut aussi aider les utilisateurs qui ont installé l'application Kaspersky Endpoint Security sur leurs postes de travail qui exécutent des tâches spécifiques.

Ce Guide est conçu pour :

- Aider l'utilisateur à installer l'application sur son ordinateur, à l'activer et à la configurer d'une façon optimale en fonction de ses besoins.
- Offrir un accès rapide aux informations pour répondre aux questions liées au fonctionnement de l'application.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

CONTENU DU GUIDE

Ce guide contient les sections suivantes.

Sources d'informations sur l'application (cf. page 13)

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Endpoint Security 8 for Windows (cf. page 15)

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

Installation et suppression de l'application (cf. page 21)

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

Licence de l'application (cf. page 41)

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

Interface de l'application (cf. page 48)

Cette section contient des informations sur les principaux éléments de l'interface graphique : icône de l'application et menu contextuel de l'icône de l'application, fenêtre principale de l'application et fenêtre de configuration de paramètres de l'application.

Lancement et arrêt de l'application (cf. page 53)

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

Tâches types (cf. section "Protection du système de fichiers de l'ordinateur. Antivirus Fichiers" à la page 56)

Ensemble de sections qui décrit les tâches et les modules types de l'application. Les sections expliquent en détail la procédure de configuration des tâches et des modules de l'application.

Administration à distance via Kaspersky Security Center (cf. page 245)

Cette section présente l'administration à distance de Kaspersky Endpoint Security via Kaspersky Security Center.

Participation au Kaspersky Security Network (cf. page 257)

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

Contacter le Service du Support Technique (cf. page 259)

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du service d'assistance technique.

Glossaire (cf. page 264)

Cette section contient une liste des termes qui apparaissent dans le document et leur définition.

Kaspersky Lab (cf. page 268)

Cette section contient des informations sur Kaspersky Lab ZAO.

Index

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

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations ou à la perturbation du fonctionnement de l'ordinateur.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes ou des cas particuliers importants dans le fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
Pour planifier une tâche, procédez comme suit :	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte `help` Les informations suivantes s'affichent : `Indiquez la date au format JJ:MM:AA.`	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
`<Adresse IP de votre ordinateur>`	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page du site du Service d'assistance technique de Kaspersky Lab (ci-après "Service d'assistance technique") (base de connaissances) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la réponse à votre question, il est recommandé de contacter le Support technique de Kaspersky Lab (cf. section "Support Technique par téléphone" à la page 261).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

Page sur le site Internet de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page particulière pour chaque application.

Cette page (http://www.kaspersky.com/fr/endpoint-security-windows) fournit des informations générales sur l'application, ces possibilités et ses particularités.

La page http://www.kaspersky.com/fr/ contient le lien sur la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page sur le site Internet du service d'assistance technique (banque de solutions)

La *Base de connaissances* est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances présente des articles avec des informations pertinentes, des conseils et des réponses de forum aux questions concernant l'achat, l'installation et l'utilisation de Kaspersky Endpoint Security pour les postes de travail http://support.kaspersky.com/fr/kes8wks et les serveurs de fichiers http://support.kaspersky.com/fr/kes8fs.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Endpoint Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est composée de fichiers d'aide.

L'*aide contextuelle* contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et la liste des tâches à effectuer.

La *version complète de l'aide* contient les informations détaillées sur l'administration de la protection de l'ordinateur à l'aide de l'application.

Manuel d'administrateur

Vous pouvez télécharger le Guide de l'administrateur au format PDF depuis la section **Téléchargement** du site de Kaspersky Lab. Ce document vous aidera à installer et à activer l'application sur les ordinateurs du réseau local de la société et à configurer ses paramètres. Le document contient les informations détaillées sur l'administration de la protection de l'ordinateur à l'aide de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum (http://forum.kaspersky.com/index.php?showforum=107).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONTACTER LE GROUPE DE REDACTION DE LA DOCUMENTATION PAR COURRIER ELECTRONIQUE

Pour contacter le Groupe de rédaction de la documentation, il faut envoyer un message par courrier électronique. L'objet du message sera "Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Windows".

KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

DANS CETTE SECTION

NOUVEAUTES

Nouvelles fonctionnalités de Kaspersky Endpoint Security 8 for Windows :

- Le Contrôle des applications permet d'autoriser ou de bloquer le lancement et le fonctionnement des applications spécifiques en fonction de la stratégie du service IT de l'entreprise. Le Contrôle des applications comprend les modules suivants :
  - Le module **Contrôle du lancement des applications** qui s'appuie sur des règles d'autorisation ou d'interdiction définies par l'administrateur du réseau local d'entreprise. Les règles peuvent être créées sur la base des catégories du logiciel fournies par Kaspersky Lab ou sur la base des conditions définies par l'administrateur du réseau local d'entreprise. Grâce à l'intégration avec Active Directory® les règles qui autorisent ou interdisent le lancement d'applications sont définies pour les utilisateurs ou les groupes d'utilisateurs Active Directory.
  - **Le module Contrôle de l'activité des applications** qui permet de bloquer les actions des applications en fonction de leur niveau de danger et de leur réputation. Les informations relatives à la réputation des applications sont fournies par Kaspersky Lab.
  - Le module **Surveillance des vulnérabilités** permet d'identifier les vulnérabilités des applications lancées sur l'ordinateur de l'utilisateur, ainsi que les vulnérabilités de toutes les applications installées sur l'ordinateur de l'utilisateur.
- Le module Contrôle Internet permet de limiter ou d'interdire l'accès utilisateur aux sites Internet selon les règles. En tant que paramètres des règles, vous pouvez indiquer des catégories de contenu des sites Internet, des types de données, des adresses Internet spécifiques ou des groupes d'adresses Internet. Grâce à l'intégration avec Active Directory, les règles du contrôle de l'accès aux sites Internet sont définies pour les utilisateurs ou les groupes d'utilisateurs Active Directory.
- Nouvelle interface de la fenêtre principale de l'application : la fenêtre principale de l'application peut afficher les statistiques relatives au fonctionnement des modules du contrôle et des modules de la protection, ainsi que les statistiques relatives à la réalisation des tâches d'analyse et de mise à jour.

Améliorations :

- Amélioration de la protection antivirus, notamment, grâce à l'intégration avec Kaspersky Security Network. L'intégration au Kaspersky Security Network permet d'obtenir des informations sur la réputation des fichiers et des URL.
- Amélioration de la technologie de désinfection avancée.
- Amélioration de la technologie d'autodéfense contre la modification des fichiers de l'application, des processus dans la mémoire et des valeurs dans la base de registre système.
- Amélioration des technologies de la défense proactive :
  - le module Surveillance du système permet de conserver l'historique de l'activité des applications ;
  - la technologie de la défense proactive BSS (Behavior Stream Signatures) permet d'identifier un comportement malveillant grâce aux signatures actualisées ;
  - une nouvelle fonctionnalité pour annuler les activités malveillantes des applications pendant la désinfection.
- Amélioration du module Pare-feu qui permet de contrôler le trafic entrant/sortant en fonction des ports, des adresses IP, des applications générant le trafic.
- Amélioration de la technologie de prévention des intrusions IDS (Intrusion Detection System) grâce à une prise en charge d'exclusions sur la base des adresses IP définies.
- Amélioration du module Contrôle des périphériques :
  - des plages plus larges des bus et des types de périphériques pris en charge ;
  - la possibilité d'utiliser les numéros de série des périphériques en tant que critères ;
  - une nouvelle fonctionnalité pour limiter l'accès aux périphériques avec système de fichiers au niveau de lecture/écriture ;
  - une nouvelle fonctionnalité pour créer la planification de l'accès aux périphériques pour les utilisateurs ;
  - une intégration avec Active Directory.
- Analyse du trafic via les protocoles IRC, Mail.ru, AIM®.

DISTRIBUTION

Kaspersky Endpoint Security peut être acheté dans la boutique en ligne de Kaspersky Lab (par exemple http://www.kaspersky.com/fr, section **Boutique en ligne**) ou du site d'un partenaire.

Si vous achetez le produit en boîte, vous recevez les éléments suivants :

- Fichiers nécessaires pour l'installation de l'application avec tous les moyens disponibles (cf. section "A propos des méthodes d'installation de l'application" à la page 21).
- Fichier ksn.txt à l'aide duquel vous pouvez faire connaissance avec les conditions de participation à Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 257).
- Fichier license.txt à l'aide duquel vous pouvez faire connaissance avec le contrat de licence. Le contrat de licence reprend les conditions d'utilisation de l'application.

Les informations indispensables à l'activation de l'application vous seront envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et la distribution, contactez le Service Ventes.

MISE EN PLACE DE LA PROTECTION DE L'ORDINATEUR

Kaspersky Internet Security assure une protection intégrale de votre ordinateur contre des menaces connues et nouvelles, des attaques réseau et des escroqueries, des messages non sollicités et d'autres données indésirables.

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

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

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

Les modules suivants sont les modules de l'application :

- **Contrôle du lancement des applications**. Le module surveille les tentatives de lancement d'applications par les utilisateurs et gère le lancement d'applications.

- **Contrôle de l'activité des applications**. Le module enregistre les actions réalisées par les applications dans le système d'exploitation et gère l'activité des applications en fonction du groupe dans lequel le module place cette application. Un ensemble de règles est défini pour chaque groupe d'applications. Ces règles gèrent l'accès aux données personnelles de l'utilisateur et aux ressources du système d'exploitation. Les données personnelles de l'utilisateur sont les fichiers d'utilisateur (dossier **Mes documents**, fichiers cookie, informations sur l'activité utilisateur), ainsi que les fichiers, les dossiers et les clés de registre avec les paramètres de fonctionnement et les informations importantes sur les applications le plus souvent utilisées.

- **Surveillance des vulnérabilités**. Le module Surveillance des vulnérabilités recherche en temps réel la présence éventuelle de vulnérabilités dans les applications exécutées sur l'ordinateur, ainsi que dans les applications au moment de leur lancement.

- **Contrôle des périphériques**. Le module permet de configurer en toute souplesse des restrictions d'accès aux types de périphériques suivants : sources d'information (notamment, disques durs, supports amovibles, lecteurs de bande, CD/DVD), dispositifs de transfert de données (notamment, modems), dispositifs de conversion en sortie papier (notamment, imprimantes) ou interfaces qui permettent de connecter les périphériques à l'ordinateur (notamment, USB, Bluetooth, Infrared).

- **Contrôle Internet**. Le module permet de configurer en toute souplesse des restrictions d'accès aux sites Internet pour différents groupes d'utilisateurs.

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

- Le Contrôle du lancement des applications utilise les règles de contrôle du lancement des applications (cf. section "A propos des règles de contrôle du lancement des applications" à la page 123).

- Le Contrôle de l'activité des applications utilise les règles du contrôle des applications (cf. section "Présentation du Contrôle de l'activité des applications" à la page 135).

- Le Contrôle des périphériques utilise les règles d'accès aux périphériques et les règles d'accès aux bus de connexion (cf. section "A propos des règles d'accès aux périphériques et aux bus de connexion" à la page 150).

- Le Contrôle Internet utilise les règles d'accès aux ressources Internet (cf. section "A propos des règles d'accès aux sites Internet" à la page 162).

Les modules suivants sont les modules de l'application :

- **Antivirus Fichiers**. Ce module permet d'éviter l'infection du système de fichiers de l'ordinateur. Le module est lancé au démarrage de Kaspersky Endpoint Security. Il se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les disques branchés. L'Antivirus Fichiers intercepte toute tentative de s'adresser au fichier et recherche dans ce fichier la présence éventuelle des virus et d'autres applications présentant une menace.

- **Surveillance du système**. Ce module récolte des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent offrir une protection plus efficace de l'ordinateur.

- **Antivirus Courrier**. Le module analyse l'ensemble du courrier entrant et sortant à la recherche d'éventuels virus et d'autres applications présentant une menace.

- **Antivirus Internet**. Le module analyse le trafic qui arrive sur l'ordinateur de l'utilisateur via le protocole HTTP et FTP et définit également si un lien appartient à la base des URL suspectes ou de phishing.

- **Antivirus IM ("Chat")**. Le module analyse le trafic qui arrive sur l'ordinateur via les protocoles de messagerie instantanée. Le module vous protège pendant l'utilisation de nombreux clients de messagerie instantanée.

- **Pare-feu**. Le module assure la protection des informations personnelles stockées sur l'ordinateur de l'utilisateur en bloquant toutes les menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local. Le module filtre toute activité réseau conformément à deux types de règles : règles réseau de l'application et règles pour les paquets réseau (cf. section "A propos des règles réseau" à la page 93).

- **Surveillance du réseau**. Le module est prévu pour consulter en temps réel les informations sur l'activité réseau de l'ordinateur.

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

Kaspersky Endpoint Security prend en charge les tâches suivantes :

- **Analyse complète**. Kaspersky Endpoint Security effectue une analyse minutieuse du système d'exploitation y compris mémoire système, objets chargés au démarrage, sauvegarde du système d'exploitation et tous les disques durs et amovibles.

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

- **Analyse rapide**. Kaspersky Endpoint Security analyse par défaut les objets chargés au démarrage du système d'exploitation, mémoire système et objets potentiellement infectés par les outils de dissimulation d'activité.

- **Mise à jour**. Kaspersky Endpoint Security télécharge les bases actualisées et les modules actualisés de l'application. Cette procédure garantit l'actualité de la protection de l'ordinateur contre de nouveaux virus et d'autres applications présentant une menace.

- **Recherche de vulnérabilités**. Kaspersky Endpoint Security recherche des vulnérabilités éventuelles dans le système d'exploitation et le logiciel installé. Ceci permet de détecter et de résoudre en temps utile des problèmes qui pourraient être exploités par des individus malintentionnés.

Administration à distance via Kaspersky Security Center

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

Services de l'application

Kaspersky Internet Security propose plusieurs services. Les fonctions de service servent à maintenir le logiciel à jour, à élargir les fonctionnalités de l'application et à fournir de l'aide pendant l'utilisation du programme.

- **Journaux**. Pendant le fonctionnement de l'application, celle-ci génère un rapport pour chaque module et chaque tâche de l'application. Ce rapport contient une liste d'évènements pendant toute la période du fonctionnement de Kaspersky Endpoint Security et de toutes les opérations effectuées par cette application. En cas de problème, vous pouvez envoyer ces rapports aux experts de Kaspersky Lab pour qu'ils puissent analyser la situation d'une façon minutieuse.

- **Stockages**. Si l'application détecte des fichiers infectés ou potentiellement infectés lors de la recherche d'éventuels virus ou applications dangereuses sur l'ordinateur, elle bloque les fichiers en question. Kaspersky Endpoint Security déplace les fichiers potentiellement infectés vers un stockage spécial qui est la *quarantaine*. Kaspersky Endpoint Security sauvegarde les copies des fichiers réparés ou supprimés dans le *dossier de sauvegarde*. Kaspersky Endpoint Security met les fichiers qui n'ont pas été traités pour une raison quelconque sur la *liste des fichiers non traités*. Vous pouvez analyser les fichiers, restaurer les fichiers vers leur dossier d'origine, placer vous-mêmes vos fichiers en quarantaine, ainsi que purger les stockages.

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

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

- **Licence**. L'utilisation de la licence permet d'activer toutes les fonctionnalités de l'application, d'assurer l'accès à la mise à jour des bases et des modules de l'application, d'obtenir des informations détaillées sur l'application, ainsi que l'aide des experts du service d'assistance technique de Kaspersky Lab.

- **Assistance technique**. Tous les utilisateurs inscrits de Kaspersky Endpoint Security peuvent bénéficier de l'aide des experts du Support technique de Kaspersky Lab. Vous pouvez envoyer une demande depuis votre Espace Personnel sur le site Internet du service d'assistance technique ou bénéficier d'une consultation téléphonique de nos experts.

SERVICES POUR LES UTILISATEURS ENREGISTRES

L'achat d'une licence vous donne le statut d'utilisateur enregistré tout au long de la durée de sa validité, ce qui vous permet de bénéficier des services suivants :

- mise à jour des bases et nouvelles versions de l'application ;

- support par téléphone et par courrier électronique sur toutes les questions en rapport avec l'installation, la configuration et l'utilisation de l'application ;

- notification sur les nouvelles applications de Kaspersky Lab et les nouveaux virus référencés. Pour bénéficier de ce service, vous devez être abonné à la diffusion d'informations de Kaspersky Lab ZAO sur le site Internet du service d'assistance technique.

Aucun support ne sera apporté sur l'utilisation du système d'exploitation ou des logiciels tiers.

CONFIGURATIONS LOGICIELLE ET MATERIELLE

Afin de garantir un fonctionnement fiable de Kaspersky Internet Security, votre ordinateur doit avoir au minimum la configuration suivante :

Recommandations d'ordre général :

- Espace disponible sur le disque dur : 1 Go.
- CD/DVD-ROM (pour installer l'application depuis un CD).
- Microsoft® Internet Explorer® 7.0 et suivantes.
- Microsoft Windows Installer 3.0 et suivantes.
- Une connexion à Internet pour activer l'application, les mises à jour des bases et des modules de l'application.

Exigences matérielles aux ordinateurs avec des systèmes d'exploitation pour les postes de travail :

- Microsoft Windows XP Professional SP3, Microsoft Windows XP Professional x64 Edition SP2 :
  - Processeur Intel® Pentium® 1 GHz minimum (ou similaire) ;
  - 256 Mo de mémoire vive disponible.
- Microsoft Windows 7 Professional/Enterprise/Ultimate (SP0 ou supérieur), Microsoft Windows 7 Professional/Enterprise/Ultimate (x64 Edition SP0 ou supérieur), Microsoft Windows Vista® SP2, Microsoft Windows Vista x64 Edition SP2 :
  - Processeur Intel Pentium 2 GHz minimum (ou similaire) ;
  - 512 Mo de mémoire vive disponible.
- Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows Embedded Standard 7 x64 Edition SP1, Microsoft Windows Embedded POSReady 2009 dernier SP :
  - Processeur Intel Pentium 800 MHz minimum (ou similaire) ;
  - 256 Mo de mémoire vive disponible.

Exigences matérielles aux ordinateurs avec des systèmes d'exploitation pour les serveurs de fichiers :

Microsoft Windows Small Business Server 2008 Standard x64 Edition, Microsoft Windows Small Business Server 2011 Essentials/Standard (x64 Edition), Microsoft Windows Server® 2008 R2 Standard/Enterprise (x64 Edition SP1), Microsoft Windows Server 2008 Standard/Enterprise SP2, Microsoft Windows Server 2008 Standard/Enterprise SP2 (x64 Edition), Microsoft Windows Server 2003 R2 Standard/Enterprise SP2, Microsoft Windows Server 2003 R2 Standard x64 Edition SP2, Microsoft Windows Server 2003 Standard SP2, Microsoft Windows Server 2003 Standard x64 Edition SP2 :

- Processeur Intel Pentium 2 GHz minimum (ou similaire) ;
- 512 Mo de mémoire vive disponible.

INSTALLATION ET SUPPRESSION DE L'APPLICATION

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

DANS CETTE SECTION

INSTALLATION DE L'APPLICATION

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

DANS CETTE SECTION

A PROPOS DES METHODES D'INSTALLATION DE L'APPLICATION

Il existe plusieurs méthodes pour installer Kaspersky Endpoint Security 8 for Windows sur un ordinateur :

- *Installation locale* : installation de l'application sur un ordinateur individuel. L'installation locale de ce type requiert un accès direct à cet ordinateur. L'installation locale peut être réalisée selon deux modes :
  - *Interactif*, à l'aide de l'Assistant d'installation de l'application (cf. section "Installation de l'application à l'aide de l'assistant d'installation de l'application" à la page 22). Ce mode requiert votre participation au processus d'installation.
  - *Silencieux*, le lancement d'installation de l'application dans ce mode est exécuté depuis la ligne de commande, votre participation à l'installation n'est pas requise (cf. section "Installation de l'application depuis la ligne de commande" à la page 26).
- *Installation à distance* : installation de l'application sur les ordinateurs du réseau réalisée à distance depuis le poste de travail de l'administrateur à l'aide de :

- suite logicielle Kaspersky Security Center (cf. "Manuel d'implantation de Kaspersky Security Center") ;
- stratégies de domaines de groupe de Microsoft Windows Server (cf. section "Installation de l'application à l'aide de l'éditeur d'objets de stratégie de groupe" à la page 27).

Avant de lancer l'installation de Kaspersky Endpoint Security (y compris l'installation à distance), il est conseillé de fermer toutes les applications ouvertes.

INSTALLATION DE L'APPLICATION A L'AIDE DE L'ASSISTANT D'INSTALLATION DE L'APPLICATION

L'interface de l'Assistant d'installation de l'application est composée d'une succession de fenêtres (d'étapes). La navigation entre les fenêtres de l'Assistant d'installation de l'application s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant d'installation de l'application, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant d'installation de l'application à n'importe quelle étape, cliquez sur le bouton **Annuler**.

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

1. Lancez le fichier setup.exe.

   L'Assistant d'installation de l'application sera lancé.

2. Suivez les instructions de l'Assistant d'installation.

DANS CETTE SECTION

ETAPE 1. VERIFICATION DE LA CONFIGURATION DU SYSTEME PAR RAPPORT A LA CONFIGURATION REQUISE

Avant l'installation de Kaspersky Endpoint Security 8 for Windows sur l'ordinateur ou avant la mise à jour de la version précédente de l'application, les conditions suivantes sont vérifiées :

- Correspondance du système d'exploitation et du paquet des mises à jour (Service Pack) aux exigences logicielles pour l'installation (cf. section "Configurations logicielle et matérielle" à la page 19).
- Exécution des exigences logicielles et matérielles (cf. section "Configurations logicielle et matérielle" à la page 19).
- Présences des droits pour l'installation du logiciel.

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

Si l'ordinateur correspond aux pré-requis, l'Assistant d'installation de l'application exécute la recherche des applications de Kaspersky Lab dont l'utilisation commune peut amener à l'apparition de conflits. Si de telles applications sont découvertes, vous devrez les supprimer manuellement.

Si la liste des applications contient Kaspersky Anti-Virus 6.0 for Windows Workstations® MP3/MP4 ou Kaspersky Anti-Virus 6.0 for File Servers MP3/MP4, toutes les données qui peuvent se déplacer (par exemple, les informations sur l'activation, les paramètres de l'application) sont enregistrées et utilisées lors de l'installation de Kaspersky Endpoint Security 8 for Windows, et Kaspersky Anti-Virus 6.0 for Windows Workstations MP3/MP4 ou Kaspersky Anti-Virus 6.0 for File Servers MP3/MP4 sera automatiquement supprimé.

ETAPE 2. FENETRE DE DEPART DE LA PROCEDURE D'INSTALLATION

Si le système d'exploitation de l'ordinateur à installer Kaspersky Endpoint Security 8 for Windows correspond entièrement aux exigences présentées, la fenêtre de départ s'ouvrira sur l'écran après le lancement du paquet d'installation. La fenêtre de départ contient les informations sur le début d'installation de Kaspersky Endpoint Security 8 for Windows sur l'ordinateur.

Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 3. LECTURE DU CONTRAT DE LICENCE

Au cours de cette étape, l'utilisateur doit prendre connaissance du contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le contrat et si vous en acceptez toutes les dispositions, cochez la case **J'accepte les termes du contrat de licence**.

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 4. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape est une invitation à participer au programme Kaspersky Security Network.

Lisez les dispositions relatives à l'utilisation de Kaspersky Security Network :

- Si vous acceptez toutes les dispositions, sélectionnez dans la fenêtre de l'assistant d'installation de l'application l'option **J'accepte de rejoindre le Kaspersky Security Network**.

- Si vous n'êtes pas d'accord aux conditions de participation au Kaspersky Security Network, sélectionnez dans la fenêtre de l'assistant d'installation de l'application l'option **Je n'accepte pas de rejoindre le Kaspersky Security Network**.

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 5. SELECTION DU TYPE D'INSTALLATION

Cette étape de l'installation permet de choisir le type d'installation de Kaspersky Endpoint Security 8 for Windows qui vous convient le mieux :

- *Installation complète*. Si vous sélectionnez ce type d'installation, l'application s'installera en intégralité sur l'ordinateur de l'utilisateur avec les paramètres de protection recommandés par les experts de Kaspersky Lab.

- *Installation personnalisée*. Si vous sélectionnez ce type d'installation, il vous est proposé de sélectionner les modules à installer (cf. section "Etape 6. Sélection des modules de l'application à installer" à la page 24) et d'indiquer le dossier à installer l'application (cf. section "Etape 7. Sélection du dossier pour installer l'application" à la page 25).

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 6. SELECTION DES MODULES DE L'APPLICATION A INSTALLER

Cette étape est exécutée si vous avez sélectionné l'*Installation personnalisée* de l'application.

Cette étape vous permet de sélectionner les modules de Kaspersky Endpoint Security 8 for Windows que vous voulez installer. Par défaut, tous les modules de l'application sont sélectionnés.

Pour sélectionner le module à installer, il faut cliquer sur le bouton gauche de la souris sur l'icône à côté du nom du module pour ouvrir le menu contextuel et sélectionner l'option **Le module sera installé sur un disque dur local**. Pour plus d'informations sur les tâches exécutées par le module sélectionné et sur l'espace libre requis sur le disque dur, veuillez consulter la partie inférieure de la fenêtre actuelle de l'Assistant d'installation de l'application.

Pour en savoir plus d'informations sur l'espace disponible sur les disques durs de l'ordinateur, cliquez sur le bouton **Disque**. Les informations seront proposées dans une nouvelle fenêtre **Espace disque disponible**.

Pour annuler l'installation du module, sélectionnez l'option **Le module sera inaccessible** dans le menu contextuel.

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

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 7. SELECTION DU DOSSIER POUR INSTALLER L'APPLICATION

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

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

Pour consulter les informations sur l'espace disponible sur les disques durs de l'ordinateur, cliquez sur le bouton **Disque**. Les informations seront proposées dans une nouvelle fenêtre **Espace disque disponible**.

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 8. AJOUT D'EXCLUSIONS A L'ANALYSE ANTIVIRUS

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

Cette étape permet de désigner les exclusions de l'analyse antivirus qu'il faut ajouter aux paramètres de l'application.

La case **Exclure de l'analyse antivirus les domaines recommandés par l'entreprise Microsoft/Exclure de l'analyse antivirus les domaines recommandés par l'entreprise Kaspersky Lab** inclut dans la zone de confiance ou en exclut les domaines recommandés par Microsoft/Kaspersky Lab.

Si la case est cochée, Kaspersky Endpoint Security inclut les secteurs recommandés par la société Microsoft® et par Kaspersky Lab dans la zone de confiance. Kaspersky Endpoint Security ne soumet pas ces secteurs à la recherche d'éventuels virus ou autres programmes dangereux.

La case **Exclure de l'analyse antivirus les secteurs recommandés par la société Microsoft** est accessible en cas d'installation de Kaspersky Endpoint Security sur un ordinateur sous Microsoft Windows pour serveurs de fichiers.

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 9. PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Il est conseillé de protéger le processus d'installation, car des applications malveillantes capables de gêner l'installation de Kaspersky Endpoint Security 8 for Windows pourraient être présentes sur l'ordinateur.

Le processus d'installation est activé par défaut.

Il est conseillé de désactiver la protection du processus d'installation s'il est impossible d'exécuter l'installation de l'application (par exemple, lors de l'installation à distance via Windows Remote Desktop). La protection de l'installation de l'application activée peut en être la cause. Dans ce cas, interrompez l'installation et relancez l'assistant d'installation de l'application dès le début. A l'étape 8 (Préparatifs pour l'installation de l'application), décochez la case **Protéger l'installation de l'application**.

La case **Ajouter le chemin au fichier avp.com dans la variable système %PATH%** active ou désactive la fonction qui ajoute la variable système de chemin %PATH% au fichier avp.com.

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

Pour revenir à l'étape antérieure de l'Assistant d'installation de l'application, cliquez sur le bouton **Précédent**. Pour installer l'application, cliquez sur le bouton **Installer**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

La rupture des connexions réseau actuelles est possible lors de l'installation de l'application sur l'ordinateur. La majorité des connexions interrompues seront rétablies automatiquement après quelques secondes.

ETAPE 10. INSTALLATION DE L'APPLICATION

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

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

Après une installation réussie de Kaspersky Endpoint Security 8 for Windows l'Assistant de configuration initiale de l'application est lancé (cf. section "Configuration initiale de l'application" à la page 32).

INSTALLATION DE L'APPLICATION DEPUIS LA LIGNE DE COMMANDE

- *Pour lancer l'assistant d'installation de l'application depuis la ligne de commande,*

  saisissez dans la ligne de commande `setup.exe` ou `msiexec /i <nom du paquet d'installation>`.

- *Pour installer l'application ou mettre à jour la version précédente de l'application en mode silencieux (sans lancer l'Assistant d'installation de l'application),*

  saisissez dans la ligne de commande `setup.exe /pEULA=1 /pKSN=1|0 /pALLOWREBOOT=1|0 /s` ou

  `msiexec /i <nom du paquet d'installation> EULA=1 KSN=1|0 ALLOWREBOOT=1|0 /qn`,

  où :

  - `EULA=1` signifie que vous acceptez les dispositions du contrat de licence. Le contrat de licence fait partie de la distribution de Kaspersky Endpoint Security 8 for Windows (cf. section "Distribution" à la page 16). L'acceptation des dispositions du contrat de licence est une condition indispensable pour installer l'application ou pour actualiser la version précédente de l'application.

  - `KSN=1|0` signifie l'acceptation ou le refus de participer à Kaspersky Security Network (par la suite "KSN"). Paramètre optionnel. Si la commande ne reprend pas la valeur du paramètre `KSN`, le système considère par défaut que vous avez refusé à participer à KSN. Le texte du règlement sur participation à KSN fait partie de la distribution de Kaspersky Endpoint Security 8 for Windows (cf. section "Distribution" à la page 16).

  - `ALLOWREBOOT=1|0` signifie l'acceptation ou l'interdiction de redémarrer automatiquement l'ordinateur en cas de besoin après l'installation de l'application ou la mise à jour de la version précédente de l'application. Paramètre optionnel. Si la commande ne reprend pas la valeur du paramètre `ALLOWREBOOT`, le système considère par défaut que vous interdisez le redémarrage de l'ordinateur après l'installation de l'application ou la mise à jour de la version antérieure de l'application.

    Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour de la version précédente de l'application ou si pendant la procédure de l'installation, Kaspersky Endpoint Security a détecté et supprimé un logiciel antivirus tiers.

    Le redémarrage automatique de l'ordinateur peut être exécuté uniquement en mode d'installation silencieuse (avec la clé/qn).

- *Pour installer l'application ou mettre à jour la version précédente de l'application en activant un mot de passe pour confirmer le droit de modification des paramètres de l'application et d'utilisation de l'application,*

  saisissez dans la ligne de commande :

  - `setup.exe /pKLPASSWD=***** /pKLPASSWDAREA=<zone d'action du mot de passe>` ou

    `msiexec /i <nom du paquet d'installation> KLPASSWD=***** KLPASSWDAREA=<zone d'action du mot de passe>` pour installer l'application ou mettre à jour la version précédente de l'application en mode interactif.

  - `setup.exe /pEULA=1 /pKSN=1|0 /pKLPASSWD=***** /pKLPASSWDAREA=<zone d'action du mot de passe> /s` ou

    `msiexec /i <nom du paquet d'installation>` EULA=1 KSN=1|0 `KLPASSWD=***** KLPASSWDAREA=<zone d'action du mot de passe> ALLOWREBOOT=1|0/qn` pour installer l'application ou mettre à jour la version précédente de l'application en mode silencieux.

  Où vous pouvez saisir en tant que `<zone d'action du mot de passe>` une ou plusieurs valeurs suivantes du paramètre `KLPASSWDAREA` séparées par un ";" :

  - `SET`. Application d'un mot de passe sur la modification des paramètres de l'application.
  - `EXIT`. Application d'un mot de passe sur l'arrêt du fonctionnement de l'application.
  - `DISPROTECT`. Application d'un mot de passe sur l'activation des modules de la protection et sur l'arrêt des tâches d'analyse.
  - `DISPOLICY`. Application d'un mot de passe sur la désactivation de la stratégie de Kaspersky Security Center.
  - `UNINST`. Application d'un mot de passe sur la suppression de l'application.
  - `DISCTRL`. Définition d'un mot de passe pour désactiver les modules du contrôle (Contrôle du lancement des applications, Contrôle de l'activité des applications, Surveillance des vulnérabilités, Contrôle des périphériques, Contrôle Web).
  - `REMOVELIC`. Application d'un mot de passe sur la suppression de la licence de l'application.

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

- setup.ini (cf. section "Description des paramètres du fichier setup.ini" à la page 28) qui contient les paramètres généraux d'installation de l'application ;
- fichier configuration install.cfg ;
- setup.reg.

Les fichiers setup.ini, install.cfg et setup.reg doivent se situer dans le même dossier que le paquet d'installation de Kaspersky Endpoint Security for Windows.

INSTALLATION DE L'APPLICATION A L'AIDE DE L'EDITEUR D'OBJETS DE STRATEGIE DE GROUPE

A l'aide du rédacteur des objets de la stratégie de groupe, vous pouvez installer Kaspersky Endpoint Security sur les postes de travail de l'entreprise qui font partie du domaine sans utiliser Kaspersky Security Center.

Pour installer Kaspersky Endpoint Security à l'aide du rédacteur des objets de la stratégie de groupe, procédez comme suit :

1. Créez un dossier partagé de réseau sur l'ordinateur qui est le contrôleur de domaine.

2. Placez la distribution de la nouvelle version de Kaspersky Endpoint Security au format MSI dans le dossier réseau partagé créé à l'étape précédente des instructions.

   De plus, vous pouvez placer dans ce dossier partagé de réseau le fichier setup.ini (cf. section "Description des paramètres du fichier setup.ini" à la page 28) qui contient la liste des paramètres d'installation de Kaspersky Endpoint Security, le fichier de configuration install.cfg, ainsi que le fichier clé.

3. Ouvrez le rédacteur des objets de la stratégie de groupe via la console d'administration (MMC) (pour plus d'informations sur le travail avec le rédacteur des objets de la stratégie de groupe, lisez le *Système d'aide de Microsoft Windows Server*).

4. Créez un nouveau paquet d'installation du rédacteur des objets de la stratégie de groupe. Pour ce faire, procédez comme suit :

   a. Dans l'arborescence de la console, sélectionnez **Objet de la stratégie de groupe** → **Configuration de l'ordinateur** → **Configuration des applications** → **Installation du logiciel**.

   b. Cliquez-droit afin d'ouvrir le menu contextuel du nœud **Installation du logiciel**.

   c. Dans le menu contextuel, sélectionnez l'option **Créer** → **Paquet**.

      La fenêtre standard de Microsoft Windows Server **Ouvrir** s'ouvre.

   d. Dans la fenêtre standard Microsoft Windows Server **Ouvrir**, indiquez le chemin vers la distribution de Kaspersky Endpoint Security au format MSI.

   e. Dans la boîte de dialogue **Déploiement de l'application**, sélectionnez le paramètre **Désigné**.

   f. Cliquez sur le bouton **OK**.

La stratégie de groupe sera appliquée pour chaque poste de travail lors de l'enregistrement suivant des ordinateurs dans le domaine. Kaspersky Endpoint Security sera installé sur tous les ordinateurs du domaine.

DESCRIPTION DES PARAMETRES DU FICHIER SETUP.INI

Le fichier setup.ini intervient dans l'installation de l'application via la ligne de commande ou l'éditeur d'objets de la stratégie de groupe. Le fichier setup.ini se trouve dans le dossier d'installation du paquet Kaspersky Endpoint Security.

Le fichier setup.ini contient les paramètres suivants :

[Setup] – paramètres généraux d'installation de l'application :

- `InstallDir` – chemin d'accès à l'installation de l'application.
- `ActivationCode` – code d'activation Kaspersky Endpoint Security.
- `Eula` – accepter ou refuser les dispositions du contrat de licence. Valeurs possibles du paramètre `Eula` :
  - `1`. La sélection de cette valeur signifie l'acceptation des dispositions du contrat de licence.
  - `0`. La sélection de cette valeur signifie le refus des dispositions du contrat de licence.
- `KSN` – accord ou désaccord de participer à Kaspersky Security Network. Valeurs possibles du paramètre `KSN` :
  - `1`. La sélection de cette valeur signifie l'acceptation de participer à Kaspersky Security Network.
  - `0`. La sélection de cette valeur signifie le refus de participer à Kaspersky Security Network.
- `Password` – installer le mot de passe pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security.
- `PasswordArea` – définir la zone d'action du mot de passe pour accéder à l'administration des fonctions et des paramètres de Kaspersky Endpoint Security. Valeurs possibles du paramètre `PasswordArea` :
  - `SET`. Application d'un mot de passe sur la modification des paramètres de l'application.
  - `EXIT`. Application d'un mot de passe sur l'arrêt du fonctionnement de l'application.
  - `DISPROTECT`. Application d'un mot de passe sur l'activation des modules de la protection et sur l'arrêt des tâches d'analyse.
  - `DISPOLICY`. Application d'un mot de passe sur la désactivation de la stratégie de Kaspersky Security Center.
  - `UNINST`. Application d'un mot de passe sur la suppression de l'application.
  - `DISCTRL`. Définition d'un mot de passe pour désactiver les modules du contrôle (Contrôle du lancement des applications, Contrôle de l'activité des applications, Surveillance des vulnérabilités, Contrôle des périphériques, Contrôle Web).
  - `REMOVELIC`. Application d'un mot de passe sur la suppression de la licence de l'application.
- `SelfProtection` – faut-il activer le mécanisme d'autodéfense de Kaspersky Endpoint Security lors de l'installation de l'application. Valeurs possibles du paramètre `SelfProtection` :
  - `1`. Cette valeur indique que le mécanisme d'autodéfense est activé.
  - `0`. Cette valeur indique que le mécanisme d'autodéfense est désactivé.

- `Reboot` – faut-il redémarrer l'ordinateur après l'installation de l'application en cas de besoin. Valeurs possibles du paramètre `Reboot` :

  - `1`. La sélection de cette valeur signifie que l'ordinateur redémarrera après l'installation de l'application le cas échéant.

  - `0`. La sélection de cette valeur signifie que, le cas échéant, l'ordinateur ne sera redémarrera pas à la fin de l'installation de l'application.

- `MSExclusions` – ajouter dans les exclusions de l'analyse les applications recommandées par la société Microsoft. Le paramètre est accessible uniquement pour les serveurs de fichiers administrés par le système d'exploitation Microsoft Windows Server (cf. section "Configurations logicielle et matérielle" à la page 19). Valeurs possibles du paramètre `MSExclusions` :

  - `1`. La sélection de cette valeur signifie que les applications recommandées par la société Microsoft sont ajoutées aux exclusions de l'analyse.

  - `0`. La sélection de cette valeur signifie que les applications recommandées par la société Microsoft ne sont pas ajoutées aux exclusions de l'analyse.

- `KLExclusions` – ajouter dans les exclusions de l'analyse les applications recommandées par la société Kaspersky Lab. Valeurs possibles du paramètre `KLExclusions` :

  - `1`. La sélection de cette valeur signifie que les applications de la société Kaspersky Lab sont ajoutées aux exclusions de l'analyse.

  - `0`. La sélection de cette valeur signifie que les applications de la société Kaspersky Lab ne sont pas ajoutées aux exclusions de l'analyse.

- `NoKLIM5` – annuler ou pas l'installation des pilotes réseau de Kaspersky Endpoint Security lors de l'installation de l'application. Les pilotes réseau sont installés par défaut. Les pilotes réseau de Kaspersky Endpoint Security concernant le groupe des pilotes NDIS et répondant de l'interception du trafic de réseau pour les modules de l'application, tels que le Contrôle des périphériques, le Contrôle Internet, l'Antivirus Courrier, l'Antivirus Internet, le Pare-feu et la Protection contre les attaques réseau, peuvent mener aux conflits avec d'autres applications et le matériel installé sur l'ordinateur de l'utilisateur. Il est possible de refuser l'installation des pilotes de réseau pour résoudre des conflits éventuels sur les ordinateurs sous l'administration de Microsoft Windows XP Professional x86 et Microsoft Windows Server 2003 x86. Valeurs possibles du module `NoKLIM5` :

  - `1`. Cette valeur signifie que l'installation des pilotes réseau de Kaspersky Endpoint Security est annulée lors de l'installation de l'application.

  - `0`. Cette valeur signifie que l'installation des pilotes réseau de Kaspersky Endpoint Security n'est pas annulée lors de l'installation de l'application.

- `AddEnviroment` – ajouter dans la variable système %PATH% le chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security. Valeurs possibles du paramètre `AddEnviroment` :

  - `1`. La sélection de cette valeur signifie qu'un chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security est ajouté à la variable %PATH%.

  - `0`. La sélection de cette valeur signifie qu'un chemin d'accès aux fichiers exécutables stockés dans le dossier d'installation de Kaspersky Endpoint Security n'est pas ajouté à la variable %PATH%

[Components] – ensemble des modules de l'application pour installer. Si aucun module n'a été désigné, tous les modules disponibles pour le système d'exploitation sont installés.

- `ALL` – installation de tous les modules.
- `MailAntiVirus` – installation du module Antivirus Courrier.
- `FileAntiVirus` – installation du module Antivirus Fichiers.
- `IMAntiVirus` – installation du module Antivirus IM.
- `WebAntiVirus` – installation du module Antivirus Internet.
- `ApplicationPrivilegeControl` – installation du module Contrôle de l'activité des applications.
- `SystemWatcher` – installation du module Surveillance du système.
- `Firewall` – installation du module Pare-feu.
- `NetworkAttackBlocker` – installation du module Prévention des intrusions.
- `WebControl` – installation du module Contrôle Internet.
- `DeviceControl` – installation du module Contrôle des périphériques.
- `ApplicationStartupControl` – installation du module Contrôle de l'activité des applications.
- `VulnerabilityAssessment` – installation des fonctions pour rechercher les vulnérabilités.
- `AdminKitConnector` – installation du module externe de l'Agent d'administration pour administrer à distance l'application via Kaspersky Security Center.

  Valeurs possibles des paramètres :

- 1. Cette valeur indique que le module va être installé.
- `0`. Cette valeur indique que le module ne va pas être installé.

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

- `ScanMyComputer` – tâche d'analyse complète.
- `ScanCritical` – tâche d'analyse rapide.
- `Updater` – tâche de mise à jour.

  Valeurs possibles des paramètres :

- `1`. La sélection de cette valeur signifie que la tâche de mise à jour est ajoutée à la liste des tâches de Kaspersky Endpoint Security.
- `0`. La sélection de cette valeur signifie que la tâche de mise à jour n'est pas ajoutée à la liste des tâches de Kaspersky Endpoint Security.

A la place de la valeur `1`, les valeurs `yes`, `on`, `enable`, `enabled` peuvent être utilisées. A la place de la valeur `0`, les valeurs `no`, `off`, `disable`, `disabled` peuvent être utilisées.

CONFIGURATION INITIALE DE L'APPLICATION

L'Assistant de configuration initiale de l'application de Kaspersky Endpoint Security démarre à la fin de la procédure d'installation de l'application. L'Assistant de configuration initiale de l'application permet d'activer l'application et effectue la collecte d'informations sur les applications comprises dans le système d'exploitation. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système d'exploitation.

L'interface de l'Assistant de configuration initiale de l'application est composée d'une succession de fenêtres (d'étapes). La navigation entre les fenêtres de l'Assistant de configuration initiale de l'application s'effectue via les boutons **Précédent** et **Suivant**. Le bouton **Terminer** permet de terminer l'assistant de configuration initiale de l'application. Le bouton **Annuler** sert à arrêter l'assistant de configuration initiale de l'application à tout moment.

Si pour des raisons quelconques le fonctionnement de l'assistant de configuration initiale de l'application a été interrompu, les valeurs des paramètres déjà établis ne sont pas sauvegardées. Ensuite, lors de la tentative de commencer le travail avec l'application, l'Assistant de configuration initiale de l'application se relance, et la configuration des paramètres est requise de nouveau.

DANS CETTE SECTION

FIN DE LA MISE A JOUR JUSQU'A KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS

Cette étape est disponible si vous exécutez la mise à jour d'une des versions précédentes de l'application (cf. section "A propos des modes de mise à jour de la version précédente de l'application" à la page 35) jusqu'à Kaspersky Endpoint Security 8 for Windows.

Cette étape propose de redémarrer l'ordinateur. Pour terminer la mise à jour de la version précédente de l'application et pour passer à la configuration initiale de Kaspersky Endpoint Security 8 for Windows, cliquez sur le bouton **Terminer**.

ACTIVATION DE L'APPLICATION

Pour activer l'application, la connexion de l'ordinateur à Internet est requise.

Cette étape permet de sélectionner une des méthodes d'activation de Kaspersky Endpoint Security.

- **Activer à l'aide du code d'activation**. Choisissez cette option et saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 42) si vous souhaitez activer l'application à l'aide d'un code d'activation.

- **Activer à l'aide du fichier de licence**. Sélectionnez cette option pour activer l'application à l'aide du fichier de licence.

- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez activer une version d'évaluation de l'application. L'utilisateur peut utiliser toutes les fonctionnalités de l'application pendant la période définie par la licence de la version d'évaluation. Une fois la durée de validité de la licence expirée, les fonctionnalités de l'application deviennent inopérationnelles et il est impossible d'activer une nouvelle fois la version d'évaluation.

- **Activer plus tard**. Choisissez cette option si vous souhaitez passer cette étape de l'activation de Kaspersky Endpoint Security. L'utilisateur pourra uniquement utiliser les modules Antivirus Fichiers et Pare-feu. L'utilisateur pourra actualiser les bases et les modules de Kaspersky Endpoint Security une fois seulement après l'installation de l'application. L'option **Activer plus tard** est accessible uniquement au premier lancement de l'Assistant de configuration initiale, juste après l'installation de l'application.

Pour poursuivre le fonctionnement de l'Assistant de configuration initiale de l'application, sélectionnez l'option d'activation de l'application et cliquez sur **Suivant**. Pour arrêter l'Assistant de configuration initiale de l'application, cliquez sur **Annuler**.

ACTIVATION EN LIGNE

Cette étape est proposée uniquement lors de l'activation de l'application à l'aide d'un code d'activation. Si vous activez la version d'évaluation de l'application ou si vous réalisez l'activation à l'aide d'un fichier de licence, cette étape est ignorée.

Au cours de cette étape, Kaspersky Endpoint Security envoie les données au serveur d'activation afin de vérifier le code d'activation saisi.

- Si le code d'activation passe la vérification, l'Assistant de configuration initiale de l'application reçoit le fichier de licence qui est installé automatiquement. L'Assistant de configuration initiale de l'application passe automatiquement à l'étape suivante.

- Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, il faut contacter la société où vous avez acheté la licence de Kaspersky Endpoint Security afin d'obtenir des informations.

- Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. L'Assistant de configuration initiale est interrompu et l'application vous propose de contacter le service d'assistance technique de Kaspersky Lab.

Pour revenir à l'étape précédente de l'Assistant de configuration initiale de l'application, cliquez sur **Précédent**. Pour arrêter l'Assistant de configuration initiale de l'application, cliquez sur **Annuler**.

ACTIVATION A L'AIDE D'UN FICHIER DE LICENCE

Cette étape est proposée uniquement lors de l'activation de la version commerciale de l'application à l'aide d'une clé de licence.

Il faut indiquer la clé de licence à cette étape. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier portant l'extension .key.

Après que vous avez sélectionné le fichier de licence, les informations relatives à la licence s'affichent dans la partie inférieure de la fenêtre :

- numéro de la licence ;
- type de licence et nombre d'ordinateurs couvert par celle-ci ;
- date d'activation de l'application ;
- date de fin de validité de la licence.

Pour revenir à l'étape précédente de l'Assistant de configuration initiale de l'application, cliquez sur **Précédent**. Pour continuer l'Assistant de configuration initiale de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant de configuration initiale de l'application, cliquez sur **Annuler**.

FIN DE L'ACTIVATION DE L'APPLICATION

A cette étape, l'Assistant de configuration initiale de l'application vous signale la réussite de l'activation de Kaspersky Endpoint Security. Les informations relatives à la licence sont également affichées :

- type de licence (commerciale ou évaluation) et nombre d'ordinateurs couverts par la licence ;
- date de fin de validité de la licence.

Pour continuer l'Assistant de configuration initiale de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant de configuration initiale de l'application, cliquez sur **Annuler**.

ANALYSE DU SYSTEME D'EXPLOITATION

Cette étape correspond à la collecte d'informations sur les applications reprises dans le système d'exploitation. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système d'exploitation.

L'analyse des autres applications est effectuée après leur première exécution qui suit l'installation de Kaspersky Endpoint Security.

Pour arrêter l'Assistant de configuration initiale de l'application, cliquez sur **Annuler**.

FIN DE L'ASSISTANT DE CONFIGURATION INITIALE DE L'APPLICATION

La dernière fenêtre de l'Assistant de configuration initiale contient des informations sur la fin du processus d'installation de Kaspersky Endpoint Security.

Pour lancer Kaspersky Endpoint Security, cliquez sur **Terminer**.

Pour quitter l'Assistant de configuration initiale de l'application sans lancer Kaspersky Endpoint Security, décochez la case **Lancer Kaspersky Endpoint Security 8 for Windows** et cliquez sur **Terminer**.

MISE A JOUR D'UNE VERSION ANTERIEURE DE L'APPLICATION

Cette section explique comment réaliser la mise à jour d'une version antérieure de l'application.

DANS CETTE SECTION

A PROPOS DES MODES DE MISE A JOUR DE LA VERSION PRECEDENTE DE L'APPLICATION

Vous pouvez mettre à jour les applications suivantes jusqu'à la version Kaspersky Endpoint Security 8 for Windows :

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP3 ;
- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP3 ;
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ;

Vous pouvez mettre à jour la version précédente de l'application à l'aide des manières suivantes :

- de manière locale en mode interactif à l'aide de l'Assistant d'installation de l'application (cf. section "Installation de l'application à l'aide de l'assistant d'installation de l'application" à la page 22) ;
- de manière locale en mode silencieux depuis la ligne de commande (cf. section "Installation de l'application depuis la ligne de commande" à la page 26) ;
- à distance à l'aide de la suite logicielle Kaspersky Security Center (les informations sont fournies dans le *Manuel d'implantation de Kaspersky Security Center*) ;
- à distance à l'aide de l'éditeur d'objets de stratégie de groupe (cf. section "Mise à jour de la version précédente de l'application via le rédacteur des objets de la stratégie de groupe" à la page 36).

Pour actualiser la version précédente jusqu'à Kaspersky Endpoint Security 8 for Windows, il ne faut pas supprimer la version précédente de l'application. Avant de commencer la mise à jour de la version précédente de l'application, il est conseillé de fermer toutes les applications ouvertes.

Lors de la mise à jour de n'importe quelle application énumérée au-dessus jusqu'à Kaspersky Endpoint Security 8 for Windows, le contenu de la quarantaine et du stockage n'est pas transféré.

MISE A JOUR DE LA VERSION PRECEDENTE DE L'APPLICATION VIA LE REDACTEUR DES OBJETS DE LA STRATEGIE DE GROUPE

A l'aide du rédacteur des objets de la stratégie de groupe, vous pouvez mettre à jour la version précédente de Kaspersky Endpoint Security sur les postes de travail de l'entreprise qui font partie du domaine sans utiliser Kaspersky Security Center.

Pour mettre à jour la version précédente de Kaspersky Endpoint Security à l'aide du rédacteur des objets de la stratégie de groupe, procédez comme suit :

1. Créez un dossier partagé de réseau sur l'ordinateur qui est le contrôleur de domaine.
2. Placez la distribution de la nouvelle version de Kaspersky Endpoint Security au format MSI dans le dossier réseau partagé créé à l'étape précédente des instructions.

   De plus, vous pouvez placer dans ce dossier partagé de réseau le fichier setup.ini (cf. section "Description des paramètres du fichier setup.ini" à la page 28) qui contient la liste des paramètres d'installation de Kaspersky Endpoint Security, le fichier de configuration install.cfg, ainsi que le fichier clé.

3. Ouvrez le rédacteur des objets de la stratégie de groupe via la console d'administration (MMC) (pour plus d'informations sur le travail avec le rédacteur des objets de la stratégie de groupe, lisez le *Système d'aide de Microsoft Windows Server*).
4. Créez un nouveau paquet d'installation du rédacteur des objets de la stratégie de groupe. Pour ce faire, procédez comme suit :
   a. Dans l'arborescence de la console, sélectionnez **Objet de la stratégie de groupe** → **Configuration de l'ordinateur** → **Configuration des applications** → **Installation du logiciel**.
   b. Cliquez-droit afin d'ouvrir le menu contextuel du nœud **Installation du logiciel**.
   c. Dans le menu contextuel, sélectionnez l'option **Créer** → **Paquet**.

      La fenêtre standard de Microsoft Windows Server **Ouvrir** s'ouvre.

   d. Dans la fenêtre standard Microsoft Windows Server **Ouvrir**, indiquez le chemin vers la distribution de la nouvelle version de Kaspersky Endpoint Security au format MSI.
   e. Dans la boîte de dialogue **Déploiement de l'application**, sélectionnez le paramètre **Désigné**.
   f. Cliquez sur le bouton **OK**.
5. Dans la liste des paquets d'installation du rédacteur des objets de la stratégie de groupe, sélectionnez le paquet d'installation du rédacteur des objets de la stratégie de groupe créé à l'étape précédente des instructions.
6. Cliquez-droit pour ouvrir menu contextuel du paquet d'installation du rédacteur des objets de la stratégie de groupe.
7. Dans le menu contextuel, choisissez l'option **Propriétés**.

   La fenêtre des propriétés du paquet d'installation du rédacteur des objets de la stratégie de groupe s'ouvrira.

8. Dans la fenêtre des propriétés du paquet d'installation du rédacteur des objets de la stratégie de groupe, sélectionnez l'onglet **Mises à jour**.

9. Sous l'onglet **Mises à jour**, ajoutez le paquet d'installation du rédacteur des objets de la stratégie de groupe qui contient la distribution de la version précédente de Kaspersky Endpoint Security.

10. Sélectionnez l'option d'installation par-dessus du paquet d'installation du rédacteur des objets de la stratégie de groupe pour installer la version actualisée de Kaspersky Endpoint Security, en sauvegardant les paramètres de la version précédente.

La stratégie de groupe sera appliquée pour chaque poste de travail lors de l'enregistrement suivant des ordinateurs dans le domaine. Finalement, la version de l'application sera mise à jour sur tous les ordinateurs du domaine.

SUPPRESSION DE L'APPLICATION

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

DANS CETTE SECTION

A PROPOS DES METHODES DE SUPPRESSION DE L'APPLICATION

Suite à la suppression de Kaspersky Endpoint Security 8 for Windows l'ordinateur et les données de l'utilisateur ne seront plus protégés.

Il existe plusieurs méthodes pour supprimer Kaspersky Endpoint Security 8 for Windows d'un ordinateur :

- de manière locale en mode interactif à l'aide de l'Assistant d'installation de l'application (cf. section "Suppression de l'application à l'aide de l'assistant d'installation de l'application" à la page 37) ;
- de manière locale en mode silencieux depuis la ligne de commande ;
- à distance à l'aide de la suite logicielle Kaspersky Security Center (les informations sont fournies dans le *Manuel d'implantation de Kaspersky Security Center*) ;
- suppression à l'aide de l'éditeur d'objets de stratégie de groupe de Microsoft Windows Server (cf. section "Suppression de l'application à l'aide de l'éditeur d'objets de stratégie de groupe" à la page 40).

SUPPRESSION DE L'APPLICATION A L'AIDE DE L'ASSISTANT D'INSTALLATION DE L'APPLICATION

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

1. Sélectionnez dans le menu **Démarrer** l'option **Programmes → Kaspersky Endpoint Security 8 for Windows → Modification, restauration ou suppression**.

   L'Assistant d'installation de l'application sera lancé.

2. Dans la fenêtre de l'Assistant d'installation de l'application **Modification, restauration ou suppression de l'application**, cliquez sur le bouton **Suppression**.

3. Suivez les instructions de l'Assistant d'installation.

DANS CETTE SECTION

ETAPE 1. ENREGISTREMENT DE DONNEES POUR UNE REUTILISATION

Cette étape vous invite à supprimer complètement l'application ou à enregistrer les objets de l'application. Vous pouvez indiquer les données de l'application que vous voulez enregistrer pour l'utilisation suivante lors de la réinstallation de l'application (par exemple, sa version plus récente).

L'option **Supprimer complètement l'application** est l'option sélectionnée par défaut. Dans ce cas, les paramètres de fonctionnement de l'application, les informations relatives à l'activation de l'application, les objets de la sauvegarde et de la quarantaine seront supprimés et inaccessibles pour l'utilisateur.

Pour enregistrer les données de l'application en vue de leur réutilisation, procédez comme suit :

1. Choisissez l'option **Enregistrer les objets de l'application**.

2. Cochez les cases en regard des données à enregistrer :

   - **Informations sur l'activation** : données permettant de ne pas activer ultérieurement l'application à installer, mais d'utiliser automatiquement la licence actuelle, à condition qu'elle soit toujours valable au moment de l'installation.

   - **Objets de la sauvegarde ou de la quarantaine** : fichiers analysés par l'application et placés dans la sauvegarde ou en quarantaine.

     L'accès aux objets de la sauvegarde ou de la quarantaine qui ont survécu à la suppression de l'application ne peut être fourni que par la version de l'application utilisée pour leur sauvegarde.

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

   - **Paramètres de fonctionnement de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.

Pour continuer l'Assistant d'installation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'installation de l'application, cliquez sur **Annuler**.

ETAPE 2. CONFIRMATION DE LA SUPPRESSION DU PROGRAMME

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

Vous pouvez à tout moment annuler cette action, en cliquant sur le bouton **Annuler**.

ETAPE 3. SUPPRESSION DE L'APPLICATION. FIN DE LA SUPPRESSION

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

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

SUPPRESSION DE L'APPLICATION DEPUIS LA LIGNE DE COMMANDE

Pour supprimer l'application de la ligne de commande, procédez comme suit :

- Saisissez dans la ligne de commande `setup.exe /x` ou

  `msiexec.exe /x {D72DD679-A3EC-4FCF-AFAF-12E2552450B6}` afin de supprimer l'application en mode interactif.

  L'Assistant d'installation de l'application sera lancé. Suivez les instructions de l'Assistant d'installation (cf. section "Suppression de l'application à l'aide de l'assistant d'installation de l'application" à la page 37).

- Saisissez dans la ligne de commande `setup.exe /s/x` ou

  `msiexec.exe /x {D72DD679-A3EC-4FCF-AFAF-12E2552450B6} /qn` pour supprimer l'application en mode silencieux (sans lancer l'Assistant d'installation de l'application).

SUPPRESSION DE L'APPLICATION A L'AIDE DE L'EDITEUR D'OBJETS DE STRATEGIE DE GROUPE

Pour supprimer Kaspersky Endpoint Security à l'aide du rédacteur des objets de la stratégie de groupe, procédez comme suit :

1. Ouvrez le rédacteur des objets de la stratégie de groupe via la console d'administration (MMC) (pour plus d'informations sur le travail avec le rédacteur des objets de la stratégie de groupe, lisez le *Système d'aide de Microsoft Windows Server*).

2. Dans l'arborescence de la console, sélectionnez **Objet de la stratégie de groupe** → **Configuration de l'ordinateur** → **Configuration des applications** → **Installation du logiciel**.

3. Dans la liste des paquets d'installation, choisissez celui de Kaspersky Endpoint Security 8 for Windows.

4. Cliquez-droit pour ouvrir le menu contextuel de l'installation, puis choisissez l'option **Toutes les tâches** → **Supprimer**.

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

5. Dans la boîte de dialogue **Suppression des applications**, choisissez l'option **Suppression immédiate de cette application des ordinateurs de tous les utilisateurs**.

La stratégie de groupe sera appliquée pour chaque poste de travail lors de l'enregistrement suivant des ordinateurs dans le domaine. En conséquence, la version de l'application sera supprimée sur tous les ordinateurs du domaine.

LICENCE DE L'APPLICATION

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

DANS CETTE SECTION

A PROPOS DU CONTRAT DE LICENCE

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

Il est conseillé de lire attentivement le contrat de licence avant de commencer à utiliser l'application.

Vous pouvez faire connaissances avec les conditions du contrat de licence, en utilisant les moyens suivants :

- Lors de l'installation de l'application de Kaspersky Lab en mode interactif (cf. section "A propos des méthodes d'installation de l'application" à la page 21).
- En lisant le document license.txt. Ce document figure dans la distribution de l'application (cf. section "Distribution" à la page 16).

En marquant votre accord avec le texte du contrat de licence pendant l'installation de l'application, vous acceptez le contrat de licence.

Si vous rejetez les termes du contrat, vous devez interrompre l'installation de l'application.

PRESENTATION DES DONNEES

En acceptant les conditions du contrat de licence, vous acceptez de transférer de manière automatique les informations relatives aux sommes de contrôle des fichiers traités (MD5) ainsi que les informations requises pour définir la réputation des URL. Ces informations ne contiennent aucune donnée personnelle ou autre donnée confidentielle. Kaspersky Lab protège les informations obtenues conformément aux dispositions juridiques en vigueur. Pour obtenir de plus amples informations, consultez le site Internet http://support.kaspersky.com/fr/corporate.

A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence. La licence contient le code d'activation unique de votre copie de Kaspersky Endpoint Security.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs périphériques.

  Ce nombre de périphériques, indiqué dans le Contrat de licence, sur lesquels vous pouvez utiliser l'application.

- Recours au service d'assistance technique de Kaspersky Lab.

- Accès à l'ensemble des services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence (cf. section "Services pour les utilisateurs enregistrés" à la page 19).

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

Les types de licence suivants existent :

- *Evaluation* : licence gratuite à validité limitée qui permet de découvrir les fonctionnalités de l'application.

  Une fois que la validité de la licence d'évaluation est écoulée, Kaspersky Endpoint Security arrête de remplir toutes ces fonctions. Pour pouvoir continuer à utiliser l'application, il faut acheter une licence commerciale.

- *Commerciale* : licence payante à durée de validité limitée délivrée lors de l'achat de l'application.

  Une fois que la licence commerciale arrive à échéance, l'application continue à fonctionner, mais ses fonctionnalités sont réduites. Vous pouvez continuer à rechercher la présence éventuelle de virus sur l'ordinateur et à utiliser d'autres modules de l'application, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour continuer à utiliser l'ensemble des fonctionnalités de Kaspersky Endpoint Security, il faut renouveler la licence commerciale.

  Il est conseillé de renouveler la validité de la licence avant la date d'expiration de la licence active afin de garantir la protection antivirus maximale pour l'ordinateur.

PRESENTATION DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence commerciale pour Kaspersky Endpoint Security. Ce code est nécessaire pour obtenir le fichier de licence et pour activer l'application en installant le fichier de licence.

Le code d'activation est une suite de 20 caractères alphanumériques (alphabet latin) au format xxxxx-xxxxx-xxxxx-xxxxx.

Le décompte de la durée de validité de la licence débute à partir de l'activation de l'application. Si vous avez acheté une licence permettant d'utiliser Kaspersky Endpoint Security sur plusieurs ordinateurs, le décompte de la validité de la licence commence à l'activation de l'application sur le premier ordinateur.

En cas de perte ou de suppression accidentelle du code après l'activation, vous devez envoyer une demande au service d'assistance technique via Mon Espace Personnel pour le récupérer (cf. section "Obtention de l'Assistance technique via Mon Espace Personnel" à la page 262).

A PROPOS DU FICHIER DE LICENCE

Le *fichier de licence* est un fichier qui se présente sous la forme xxxxxxxx.key et qui permet d'utiliser une application de Kaspersky Lab selon les termes d'une licence d'évaluation ou commerciale. Kaspersky Lab octroie le fichier de licence sur la base du code d'activation, en cas d'activation de l'application à l'aide du code d'activation ou lors de l'achat de Kaspersky Endpoint Security. Le fichier de licence est indispensable à l'utilisation de l'application.

En cas de suppression accidentelle du fichier de licence, vous devez procéder comme suit pour le restaurer :

- envoyer une demande au Service d'assistance technique (cf. section "Appel au Service d'assistance technique" à la page 259) ;
- récupérer le fichier de licence sur la base du code d'activation sur le site Internet (https://activation.kaspersky.com/fr/).

Un *fichier de licence d'évaluation* est un fichier de licence prévu pour explorer les fonctionnalités de l'application pendant une période déterminée. Le fichier de licence d'évaluation donne droit à l'utilisation de l'application dès le jour de l'installation. Kaspersky Lab offre le fichier de licence d'évaluation gratuitement lors de l'activation de la version d'évaluation.

Un *fichier de licence commerciale* est un fichier de licence qui contient les informations indispensables à l'utilisation de l'application dans le respect des conditions de la licence commerciale. Le fichier de licence commerciale donne droit à l'utilisation de l'application dès le jour de l'installation. Kaspersky Lab propose le fichier de licence commerciale sur la base du code d'activation obtenu à l'achat de l'application.

Le fichier de licence contient les informations suivantes relatives à la licence :

- Le numéro de licence, un numéro unique utilisé, par exemple, pour obtenir l'assistance technique de Kaspersky Lab.
- Restriction sur le nombre d'ordinateurs : le nombre maximal d'ordinateurs sur lesquels vous pouvez activer l'application à l'aide de ce fichier de licence.
- Durée de validité du fichier de licence : délai défini à compter de la création du fichier de licence. Ce délai est déterminé par l'application en fonction de la durée de validité de la licence (cf. section "Présentation de la licence" à la page 42).
- Date de création du fichier de licence : la date de création du fichier de licence sur la base du code d'activation utilisé pour le décompte de la durée de validité du fichier de licence.
- Durée de conservation de la licence : durée établie à partir de la création de la licence par les experts de Kaspersky Lab. La durée de validité de la licence peut être de plusieurs années. L'application peut être activée uniquement avant l'expiration de ce délai.
- Date de fin de validité du fichier de licence : date après laquelle il est impossible d'utiliser le fichier de licence pour activer l'application. La date de fin de validité du fichier de licence est calculée à partir de la date d'utilisation du fichier de licence, augmentée du délai de validité du fichier de licence, mais pas au-delà de la fin de la conservation de la licence.

  Si la date de fin de validité du fichier de licence est antérieure à la fin de validité de la licence, la durée de conservation de la licence est limitée à la date de fin de validité du fichier de licence.

- Renseignements sur l'assistance technique.

A PROPOS DES MODES D'ACTIVATION DE L'APPLICATION

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

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

- Lors de l'installation de l'application, à l'aide de l'Assistant de configuration initiale de l'application (cf. section "Configuration initiale de l'application" à la page 32).
- Localement, via l'interface de l'application à l'aide de l'Assistant d'activation de l'application (cf. section "Assistant d'activation de l'application" à la page 45).
- A distance à l'aide de Kaspersky Security Center en créant une tâche d'installation du fichier de licence (cf. section "Gestion des tâches" à la page 247).
- A distance via la diffusion automatique sur les postes client de licences stockées dans le référentiel des licences du serveur d'administration Kaspersky Security Center (les informations à ce sujet sont reprises dans le *Guide de l'administrateur de Kaspersky Security Center*).

ADMINISTRATION DE LA LICENCE

Cette section contient des informations sur les actions que vous pouvez exécuter dans le cadre de l'octroi des licences.

DANS CETTE SECTION

ACTIVATION DE L'APPLICATION A L'AIDE DE L'ASSISTANT D'ACTIVATION DE L'APPLICATION

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

1. Exécutez une des actions suivantes :

   - Cliquez sur le lien **Veuillez activer l'application** dans la fenêtre de notification de Kaspersky Endpoint Security dans la zone de notifications de la barre des tâches.
   - Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application. Dans la fenêtre **Gestionnaire de licences** qui s'ouvre, cliquez sur le bouton **Activer l'application avec une nouvelle licence**.

   L'Assistant d'activation de l'application démarre (cf. page 45).

2. Suivez les instructions de l'Assistant d'activation de l'application.

ACHAT DE LA LICENCE

Vous pouvez acheter une licence après avoir installé l'application. L'achat de la licence vous permet de recevoir un code d'activation ou un fichier de licence pour activer l'application (cf. section "Activation de l'application à l'aide de l'Assistant d'activation de l'application" à la page 44).

Pour acheter une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Gestionnaire de licences**.
3. Dans la fenêtre **Gestionnaire de licences**, réalisez une des opérations suivantes :
   - Cliquez sur le bouton **Acheter une licence** si aucune licence n'est installée ou si vous utilisez une licence d'évaluation.
   - Cliquez sur le bouton **Renouveler la durée de validité de la licence** si vous avez installé une licence commerciale.

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

PROLONGEMENT DE LA LICENCE

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

Pour renouveler la licence, procédez comme suit :

1. Achetez un nouveau code d'activation de l'application ou une nouvelle clé de licence (cf. section "Achat de la licence" à la page 45).
2. Activez l'application à l'aide du code d'activation ou du fichier de licence que vous avez acheté (cf. section "Activation de l'application à l'aide de l'Assistant d'activation de l'application" à la page 44).

Une nouvelle licence, appelée licence complémentaire, est ajoutée. Elle entrera en vigueur automatiquement à l'expiration de la licence active de Kaspersky Endpoint Security.

CONSULTATION DES INFORMATIONS RELATIVES A LA LICENCE

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

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Cliquez sur le lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application.

La fenêtre **Gestionnaire de licences** s'ouvre. Les informations relatives à la licence apparaissent dans le groupe situé dans la partie supérieure de la fenêtre **Gestionnaire de licences**.

ASSISTANT D'ACTIVATION DE L'APPLICATION

L'interface de l'Assistant d'activation de l'application est composée d'une succession de fenêtres (d'étapes). La navigation entre les fenêtres de l'Assistant d'activation de l'application s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant d'activation de l'application, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant d'activation de l'application à n'importe quelle étape, cliquez sur le bouton **Annuler**.

DANS CETTE SECTION

ACTIVATION DE L'APPLICATION

Pour activer l'application, la connexion de l'ordinateur à Internet est requise.

Cette étape permet de sélectionner une des méthodes d'activation de Kaspersky Endpoint Security.

- **Activer à l'aide du code d'activation**. Choisissez cette option et saisissez le code d'activation (cf. section "Présentation du code d'activation" à la page 42) si vous souhaitez activer l'application à l'aide d'un code d'activation.
- **Activer à l'aide du fichier de licence**. Sélectionnez cette option pour activer l'application à l'aide du fichier de licence.
- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez activer une version d'évaluation de l'application. L'utilisateur peut utiliser toutes les fonctionnalités de l'application pendant la période définie par la licence de la version d'évaluation. Une fois la durée de validité de la licence expirée, les fonctionnalités de l'application deviennent inopérationnelles et il est impossible d'activer une nouvelle fois la version d'évaluation.

Pour continuer à utiliser l'Assistant d'activation de l'application, choisissez le mode d'activation de l'application, puis cliquez sur **Suivant**. Pour arrêter l'Assistant d'activation de l'application, cliquez sur **Annuler**.

ACTIVATION EN LIGNE

Cette étape est proposée uniquement lors de l'activation de l'application à l'aide d'un code d'activation. Si vous activez la version d'évaluation de l'application ou si vous réalisez l'activation à l'aide d'un fichier de licence, cette étape est ignorée.

Au cours de cette étape, Kaspersky Endpoint Security envoie les données au serveur d'activation afin de vérifier le code d'activation saisi.

- Si le code d'activation passe la vérification, l'Assistant d'activation de l'application reçoit le fichier de licence qui est installé automatiquement. L'Assistant d'activation de l'application passe automatiquement à l'étape suivante.
- Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, il faut contacter la société où vous avez acheté la licence de Kaspersky Endpoint Security afin d'obtenir des informations.
- Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. L'Assistant d'activation de l'application est interrompu et un message vous invite à contacter le Service du Support Technique de Kaspersky Lab.

Pour revenir à l'étape antérieure de l'Assistant d'activation de l'application, cliquez sur le bouton **Précédent**. Pour arrêter l'Assistant d'activation de l'application, cliquez sur **Annuler**.

ACTIVATION A L'AIDE D'UN FICHIER DE LICENCE

Cette étape est proposée uniquement lors de l'activation de la version commerciale de l'application à l'aide d'une clé de licence.

Il faut indiquer la clé de licence à cette étape. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier portant l'extension .key.

Après que vous avez sélectionné le fichier de licence, les informations relatives à la licence s'affichent dans la partie inférieure de la fenêtre :

- numéro de la licence ;
- type de licence et nombre d'ordinateurs couvert par celle-ci ;
- date d'activation de l'application ;
- date de fin de validité de la licence.

Pour revenir à l'étape antérieure de l'Assistant d'activation de l'application, cliquez sur le bouton **Précédent**. Pour continuer l'Assistant d'activation de l'application, cliquez sur **Suivant**. Pour arrêter l'Assistant d'activation de l'application, cliquez sur **Annuler**.

FIN DE L'ACTIVATION DE L'APPLICATION

A cette étape, l'Assistant d'activation de l'application vous signale la réussite de l'activation de Kaspersky Endpoint Security. Les informations relatives à la licence sont également affichées :

- type de licence (commerciale ou évaluation) et nombre d'ordinateurs couverts par la licence ;
- date de fin de validité de la licence.

Pour quitter l'Assistant d'activation de l'application, cliquez sur le bouton **Terminer**.

INTERFACE DE L'APPLICATION

Cette section contient des informations sur les principaux éléments de l'interface graphique : icône de l'application et menu contextuel de l'icône de l'application, fenêtre principale de l'application et fenêtre de configuration de paramètres de l'application.

DANS CETTE SECTION

ICONE DE L'APPLICATION DANS LA ZONE DE NOTIFICATION

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

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

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

Indication du fonctionnement de l'application

L'icône de l'application indique l'état de fonctionnement de l'application. Elle renseigne l'état de la protection de l'ordinateur et affiche les actions que l'application exécute actuellement :

- L'icône  indique que tous les modules de la protection de l'application sont activés.
- L'icône  indique que Kaspersky Endpoint Security analyse le courrier.
- L'icône  indique que Kaspersky Endpoint Security vérifie le trafic de réseau entrant ou sortant.
- L'icône  indique que Kaspersky Endpoint Security met à jour les bases et les modules de l'application.
- L'icône  indique que des événements importants se sont déroulés dans Kaspersky Endpoint Security et qu'il faut y prêter attention. Par exemple, l'Antivirus Fichiers est désactivé ou les bases de l'application sont dépassées.
- L'icône  indique que des événements critiques se sont produits durant le fonctionnement de Kaspersky Endpoint Security. Par exemple, échec d'un ou de plusieurs des modules, bases endommagées.

Par défaut, l'animation de l'icône de l'application est activée : par exemple, lorsque Kaspersky Endpoint Security analyse un message électronique, une petite icône représentant une enveloppe clignote sur le fond de l'icône de l'application. Lorsque Kaspersky Endpoint Security met à jour des bases et des modules de l'application, l'icône d'une mappemonde apparaît sur le fond de l'icône de l'application.

MENU CONTEXTUEL DE L'ICONE DE L'APPLICATION

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

- **Kaspersky Endpoint Security 8 for Windows**. Ouvre la fenêtre principale de l'application à l'onglet **Centre de gestion**. L'onglet **Centre de gestion** vous permet de gérer le fonctionnement des modules et des tâches de l'application, et de consulter les statistiques relatives aux fichiers traités et aux menaces détectées.

- **Configuration** dans la partie supérieure de la fenêtre. Ouvre la fenêtre principale de l'application à l'onglet **Configuration**. L'onglet **Configuration** vous permet de modifier les paramètres par défaut de l'application.

- **Suspension de la protection et du contrôle/Rétablissement de la protection et du contrôle**. Désactive temporairement ou rétablit le fonctionnement des modules de protection et des modules de contrôle de l'application. Cette option du menu contextuel n'a aucune incidence sur l'exécution de la tâche de mise à jour et des tâches d'analyse.

- **Désactivation de la stratégie/Activation de la stratégie**. Désactive ou active la stratégie de Kaspersky Security Center. Cette option est accessible si Kaspersky Endpoint Security fonctionne dans le cadre d'une stratégie et que le mot de passe pour la désactivation d'une stratégie de Kaspersky Security Center a été défini dans les paramètres de la stratégie.

- **A propos du programme**. Ouvre une fenêtre contenant des informations sur l'application.

- **Quitter**. Entraîne l'arrêt de Kaspersky Endpoint Security. Si vous choisissez cette option du menu contextuel, l'application est déchargée de la mémoire vive de l'ordinateur.

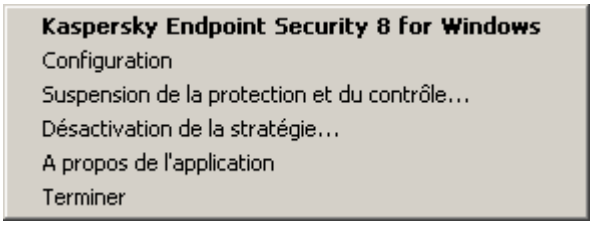


Illustration 1. Menu contextuel de l'icône de l'application

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

FENETRE PRINCIPALE DE L'APPLICATION

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

La fenêtre principale de l'application contient trois parties (cf. ill. ci-après) :

- La partie supérieure de la fenêtre contient les éléments de l'interface qui permettent d'accéder aux informations suivantes :
  - informations sur l'application ;
  - statistiques des bases de données de réputation ;
  - liste des fichiers non traités ;
  - liste des vulnérabilités détectées ;
  - liste des fichiers placés en quarantaine ;

- dossier de sauvegarde des fichiers infectés supprimés lors du fonctionnement de l'application ;
- rapports sur les événements survenus pendant le fonctionnement de l'application dans son ensemble, de modules distincts et des tâches.

- L'onglet **Centre de gestion** permet de réglementer le fonctionnement des modules et des tâches de l'application. Lorsque vous ouvrez la fenêtre principale de l'application, l'onglet **Centre de gestion** s'affiche.
- L'onglet **Configuration** permet de modifier les paramètres de l'application définis par défaut.

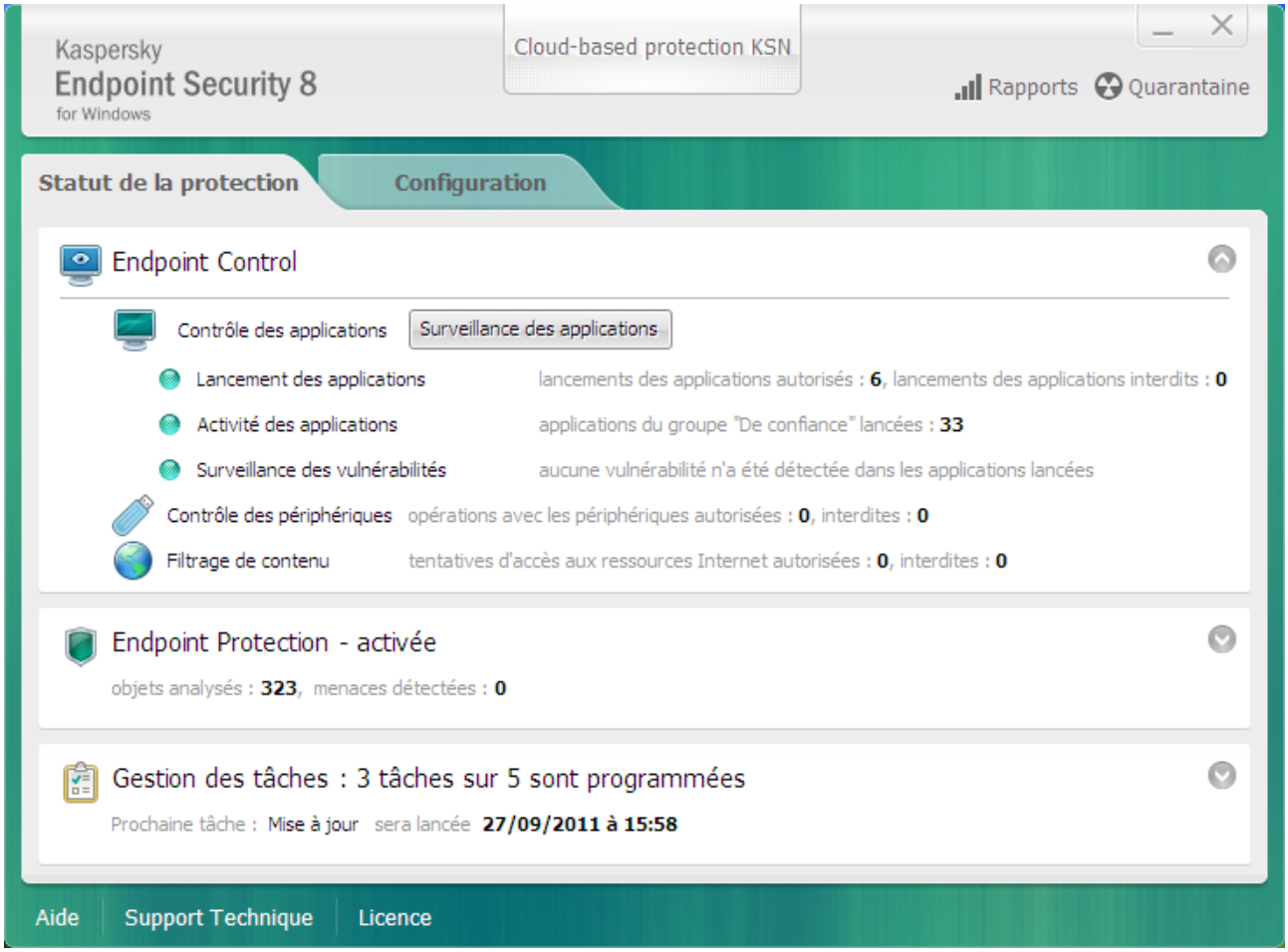


Illustration 2. Fenêtre principale de l'application

Vous pouvez cliquer sur les liens suivants :

- **Aide**. Cliquez sur ce lien pour accéder à l'aide de Kaspersky Endpoint Security.
- **Assistance technique**. Cliquez sur ce lien pour ouvrir la fenêtre **Assistance technique** contenant les informations relatives au système d'exploitation, à la version actuelle de Kaspersky Endpoint Security et des liens vers des ressources d'informations de Kaspersky Lab.
- **Licence**. Cliquez sur ce lien pour ouvrir la fenêtre **Gestionnaire de licences** contenant les informations relatives à la licence utilisée.

Vous pouvez ouvrir la fenêtre principale de Kaspersky Endpoint Security d'une des manières suivantes :

- En positionnant le curseur sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et en cliquant avec le bouton gauche de la souris.
- En choisissant l'option **Kaspersky Endpoint Security** dans le menu contextuel de l'application (cf. section "Menu contextuel de l'icône de l'application" à la page 49).

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

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

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

- Le volet gauche de la fenêtre contient des modules de l'application, des tâches et d'autres éléments qui peuvent être configurés.
- Le volet droit de la fenêtre contient des éléments de gestion qui permettent de configurer le fonctionnement de l'élément sélectionné dans le volet gauche.

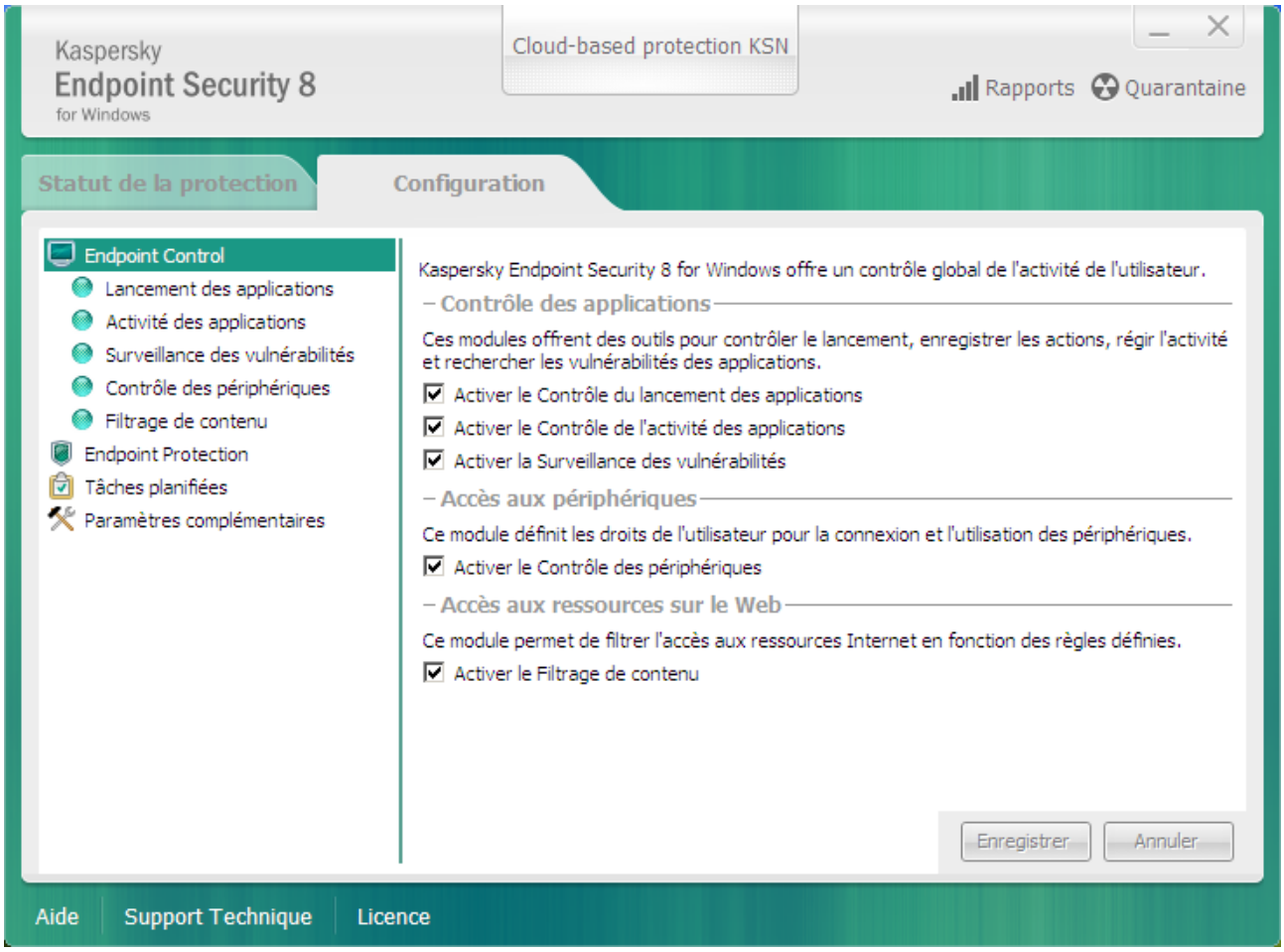


Illustration 3. Fenêtre de configuration des paramètres de l'application

A l'instar de la fenêtre principale de l'application, cette fenêtre propose les liens suivants :

- **Aide**. Cliquez sur ce lien pour accéder à l'aide de Kaspersky Endpoint Security.
- **Assistance technique**. Cliquez sur ce lien pour ouvrir la fenêtre **Assistance technique** contenant les informations relatives au système d'exploitation, à la version actuelle de Kaspersky Endpoint Security et des liens vers des ressources d'informations de Kaspersky Lab.
- **Licence**. Cliquez sur ce lien pour ouvrir la fenêtre **Gestionnaire de licences** contenant les informations relatives à la licence utilisée.

Vous avez le choix entre deux méthodes pour ouvrir la fenêtre de configuration des paramètres de l'application :

- Via l'onglet **Configuration** dans la fenêtre principale de l'application (cf. section "Ouvrez la fenêtre principale de l'application" à la page 49).
- Via l'option **Configuration** du menu contextuel de l'application (cf. section "Menu contextuel de l'icône de l'application" à la page 49).

LANCEMENT ET ARRET DE L'APPLICATION

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

DANS CETTE SECTION

ACTIVATION ET DESACTIVATION DU LANCEMENT AUTOMATIQUE DE L'APPLICATION

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

La première fois, Kaspersky Endpoint Security est lancé automatiquement après son installation. Ensuite, l'application est lancée automatiquement après le démarrage du système d'exploitation.

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

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Lancer Kaspersky Endpoint Security au démarrage de l'ordinateur** si vous souhaitez activer le lancement automatique de l'application.
   - Décochez la case **Lancer Kaspersky Endpoint Security au démarrage de l'ordinateur** si vous souhaitez désactiver le lancement automatique de l'application.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

LANCEMENT ET ARRET MANUELS DE L'APPLICATION

Les experts de Kaspersky Lab déconseillent de quitter Kaspersky Endpoint Security car cela exposerait votre ordinateur et ses données à des risques. Le cas échéant, vous pouvez suspendre la protection de l'ordinateur pendant l'intervalle que vous souhaitez, sans quitter l'application (cf. section "Suspension et rétablissement de la protection et du contrôle de l'ordinateur" à la page 54).

Le lancement manuel de Kaspersky Endpoint Security s'impose si vous avez désactivé le lancement automatique de l'application (cf. section "Activation et désactivation du lancement automatique de l'application" à la page 53).

Pour lancer l'application manuellement,

ouvrez le menu Pour lancer l'application manuellement, sélectionnez dans le menu **Démarrer** l'option **Programmes** → **Kaspersky Endpoint Security 8 for Windows**.

Pour arrêter l'application manuellement, procédez comme suit :

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

2. Sélectionnez **Quitter** dans le menu contextuel.

SUSPENSION ET RETABLISSEMENT DE LA PROTECTION ET DU CONTROLE DE L'ORDINATEUR

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

L'icône dans la zone de notification de la barre des tâches indique le fonctionnement de l'application (cf. section "Icône de l'application dans la zone de notification" à la page 48) :

- L'icône  indique la suspension de la protection et du contrôle de l'ordinateur.

- L'icône  indique le rétablissement de la protection et du contrôle de l'ordinateur.

La suspension et le rétablissement de la protection et du contrôle de l'ordinateur 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 de la protection et du contrôle de l'ordinateur, un message s'affiche pour indiquer l'interruption de ces connexions.

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

1. Si vous souhaitez suspendre la protection et le contrôle de l'ordinateur, procédez comme suit :

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

   b. Sélectionnez **Suspension de la protection et du contrôle** dans le menu contextuel.

      La fenêtre **Suspension de la protection et du contrôle** s'ouvre.

   c. Choisissez l'une des options suivantes :

      - **Suspendre pendant la période indiquée** : la protection et le contrôle de l'ordinateur seront activés à l'issue de l'intervalle de temps défini dans la liste déroulante en dessous. Vous pouvez sélectionner l'intervalle requis dans la liste déroulante.

      - **Suspendre jusqu'au redémarrage** : la protection et le contrôle de l'ordinateur sont activés après le redémarrage de l'application ou du système d'exploitation. Pour pouvoir utiliser cette fonction, le lancement automatique de l'application doit être activé.

      - **Interrompre** : la protection et le contrôle de l'ordinateur sont activés quand vous décidez de les rétablir.

2. Si vous souhaitez rétablir la protection et le contrôle de l'ordinateur, vous pouvez le faire à tout moment, quelle que soit la variante de suspension que vous aviez sélectionnée. Pour rétablir la protection et le contrôle de l'ordinateur, procédez comme suit :

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

   b. Sélectionnez l'option **Rétablissement de la protection et du contrôle** dans le menu contextuel.

PROTECTION DU SYSTEME DE FICHIERS DE L'ORDINATEUR. ANTIVIRUS FICHIERS

Cette section contient des informations sur l'Antivirus Fichiers et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DE L'ANTIVIRUS FICHIERS

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. L'Antivirus Fichiers est lancé par défaut au démarrage de Kaspersky Endpoint Security. Il se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur ainsi que sur tous les disques montés. Il recherche des virus et d'autres applications présentant une menace.

L'Antivirus Fichiers utilise les méthodes de l'analyse sur la base de signatures et de l'analyse heuristique, ainsi que les technologies iChecker et iSwift.

Lorsque l'utilisateur ou une application sollicite le fichier protégé, l'Antivirus Fichiers recherche les données relatives à celui-ci dans les bases iChecker et iSwift et, sur la base des données obtenues, décide d'analyser ou de ne pas analyser le fichier.

Lorsque Kaspersky Endpoint Security détecte une menace dans le fichier, il attribue au fichier un des états suivants :

- Etat qui désigne le type de l'application malveillante détectée (par exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si le fichier est infecté ou non. Le fichier contient peut-être une séquence de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

Ensuite, l'application bloque le message électronique, affiche sur l'écran une notification (cf. page 215) sur la menace détectée (si cela a été défini dans les paramètres des notifications) et exécute l'action définie dans les paramètres de l'Antivirus Courrier (cf. section "Modification de l'action sur les fichiers infectés" à la page 60).

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS FICHIERS

Par défaut, l'Antivirus Fichiers est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Fichiers le cas échéant.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver l'Antivirus Fichiers sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Antivirus Fichiers.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Fichiers.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Fichiers**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Fichiers.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Fichiers**, sera modifiée sur l'icône .

Pour activer ou désactiver l'Antivirus Fichiers depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'Antivirus Fichiers** pour activer l'Antivirus Fichiers.
   - Décochez la case **Activer l'Antivirus Fichiers** pour désactiver l'Antivirus Fichiers.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ARRET AUTOMATIQUE DE L'ANTIVIRUS FICHIERS

Vous pouvez configurer l'arrêt automatique de fonctionnement du module à l'heure indiquée ou en cas d'utilisation d'applications spécifiques.

La suspension de l'Antivirus Fichiers en cas de conflit avec certaines applications est une mesure extrême. Si des conflits se manifestent pendant l'utilisation du module, veuillez contacter le Support technique de Kaspersky Lab (http://support.kaspersky.com/fr). Les experts vous aideront à garantir le fonctionnement de Kaspersky Endpoint Security avec d'autres applications sur votre ordinateur.

Pour configurer l'arrêt automatique de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.
5. Dans le groupe **Suspension de la tâche**, procédez comme suit :

   - Cochez la case **Selon la programmation** et cliquez sur le bouton **Programmation** pour configurer l'arrêt automatique de l'Antivirus Fichiers à l'heure indiquée.

     La fenêtre **Suspension de la tâche** s'ouvre.
   - Cochez la case **Au lancement du programme** et cliquez sur le bouton **Sélectionner** pour configurer l'arrêt automatique de l'Antivirus Fichiers au lancement des applications indiquées.

     La fenêtre **Applications** s'ouvre.
6. Exécutez une des actions suivantes :

   - Pour configurer l'arrêt automatique de l'Antivirus Fichiers à l'heure indiquée dans la fenêtre **Suspension de la tâche**, indiquez la période (au format hh:mm) pendant laquelle il faut suspendre le fonctionnement de l'Antivirus Fichiers dans les champs **Pause à partir de** et **Reprendre à**. Cliquez sur le bouton **OK**.
   - Pour configurer l'arrêt automatique de l'Antivirus Fichiers au lancement des applications indiquées, composez la liste des applications dont l'utilisation nécessite la suspension de l'Antivirus Fichiers dans la fenêtre **Applications** à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Cliquez sur le bouton **OK**.
7. Dans la fenêtre **Antivirus Fichiers**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE L'ANTIVIRUS FICHIERS

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Fichiers :

- Modifier le niveau de protection des fichiers.

  Vous pouvez sélectionner un des niveaux de protection prédéfinis pour les fichiers ou personnaliser les paramètres du niveau de protection des fichiers. Après avoir modifié les paramètres du niveau de protection des fichiers, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de protection des fichiers.

- Modifier l'action que l'Antivirus Fichiers exécute en cas de découverte d'un fichier infecté.

- Constituer la zone de protection de l'Antivirus Fichiers.

  Vous pouvez élargir ou restreindre la zone de protection en ajoutant ou en supprimant des objets ou en modifiant le type de fichiers à analyser.

- Configurer l'utilisation de l'analyse heuristique.

  L'Antivirus Fichiers utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, l'Antivirus Fichiers compare l'objet trouvé aux signatures des bases. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, l'Antivirus Fichiers analyse l'activité des objets dans le système. L'Analyse heuristique permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases.

- Sélectionner les technologies d'analyse.

  Vous pouvez activer les technologies iChecker et iSwift qui permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers avec l'Antivirus Fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

- Configurer l'analyse des fichiers composés.

- Modifier le mode d'analyse des fichiers.

DANS CETTE SECTION

MODIFICATION DU NIVEAU DE PROTECTION DES FICHIERS

Pour protéger le système de fichiers de l'ordinateur, l'Antivirus Fichiers utilise de différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de protection des fichiers*. Il existe trois niveaux prédéfinis de protection des fichiers : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de protection des fichiers **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky Lab.

Afin de modifier le niveau de protection des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, exécutez une des actions suivantes :

   - Pour définir un des niveaux prédéfinis de protection des fichiers (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de protection des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Fichiers** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de protection des fichiers, le nom du niveau de protection des fichiers dans le groupe **Niveau de protection** devient **Autre**.
   - Pour sélectionner le niveau de protection des fichiers **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DE L'ACTION SUR LES FICHIERS INFECTES

Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Action en cas de découverte d'une menace** sélectionnez l'option requise :
   - **Sélectionner l'action automatiquement**.
   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible**.
   - **Exécuter l'action : Réparer**.
   - **Exécuter l'action : Supprimer**.
   - **Exécuter l'action : Bloquer**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS FICHIERS

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection de l'Antivirus Fichiers sont l'emplacement et le type des fichiers analysés. Par défaut, Antivirus Fichiers analyse uniquement les fichiers pouvant être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau de l'ordinateur.

Pour former la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers** sous l'onglet **Général** dans le groupe **Types de fichiers**, indiquez le type de fichiers que vous voulez analyser à l'aide de l'Antivirus Fichiers :
   - Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.
   - Sélectionnez **Fichiers analysés selon le format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.
   - Sélectionnez **Fichiers analysés selon l'extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

Au moment de choisir le type d'objet à analyser, il convient de ne pas oublier les éléments suivants :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, les formats EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

- Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Un tel fichier est scrupuleusement analysé sur les virus et sur d'autres applications présentant une menace.

5. La liste **Zone d'analyse** permet d'effectuer une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** pour ajouter un nouvel objet à la liste des objets analysés.

   - Pour modifier l'emplacement de l'objet, sélectionnez-le dans la liste des objets analysés et cliquez sur le bouton **Modifier**.

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

   - Pour supprimer l'objet de la liste des objets analysés, sélectionnez-le dans la liste des objets analysés et cliquez sur le bouton **Supprimer**.

     La fenêtre de confirmation de suppression s'ouvrira.

6. Exécutez une des actions suivantes :

   - Pour ajouter un nouvel objet ou modifier l'emplacement de l'objet de la liste des objets analysés, sélectionnez-le dans la fenêtre **Sélection de l'objet à analyser** et cliquez sur le bouton **Ajouter**.

     Tous les objets sélectionnés dans la fenêtre **Sélection de l'objet à analyser** seront affichés dans la liste **Zone de protection** dans la fenêtre **Antivirus Fichiers**.

     Cliquez sur le bouton **OK**.

   - Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

7. Le cas échéant, répétez les points 5-6 pour ajouter, modifier l'emplacement ou supprimer les objets de la liste des objets à analyser.

8. Pour exclure l'objet de la liste des objets analysés, décochez la case en regard de l'objet dans la liste **Zone d'analyse**. Avec cela, l'objet reste dans la liste des objets analysés mais sera exclu de l'analyse par l'Antivirus Fichiers.

9. Dans la fenêtre **Antivirus Fichiers**, cliquez sur **OK**.

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

UTILISATION DE L'ANALYSE HEURISTIQUE LORS DU FONCTIONNEMENT DE L'ANTIVIRUS FICHIERS

Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Performance**.
5. Dans le groupe **Méthodes d'analyse** procédez comme suit :

   - Si vous voulez que l'Antivirus Fichiers utilise l'analyse heuristique, cochez la case **Analyse heuristique**, et à l'aide du curseur définissez le niveau de spécification de l'analyse heuristique : spécifications de l'analyse heuristique : **Superficiel**, **Moyen** ou **Profond**.

   - Si vous voulez que l'Antivirus Fichiers n'utilise pas l'analyse heuristique, décochez la case **Analyse heuristique**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

UTILISATION DES TECHNOLOGIES D'ANALYSE DANS LE FONCTIONNEMENT DE L'ANTIVIRUS FICHIERS

Pour configurer l'utilisation des technologies d'analyse dans le fonctionnement de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.

5. Dans le groupe **Technologies d'analyse** procédez comme suit :

   - Cochez les cases à côté des noms des technologies que vous voulez utiliser dans le fonctionnement de l'Antivirus Fichiers.

   - Décochez les cases à côté des noms des technologies que vous ne voulez pas utiliser dans le fonctionnement de l'Antivirus Fichiers.

6. Cliquez sur le bouton **OK**.

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

OPTIMISATION DE L'ANALYSE DES FICHIERS

Pour optimiser l'analyse des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.

4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Performance**.

5. Dans le groupe **Optimisation de l'analyse**, cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

6. Cliquez sur le bouton **OK**.

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

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour détecter les virus dissimulés et les autres applications présentant une menace de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limites le cercle des fichiers composés analysés pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre **Antivirus Fichiers** s'ouvre.

4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Performance**.

5. Dans le groupe **Analyse des fichiers composés**, indiquez les types des fichiers composés à vérifier : archives, paquets d'installation ou objets OLE incorporés.

6. Si dans le groupe **Optimisation de l'analyse** la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est décochée, vous pouvez indiquer pour chaque type de fichier composé s'il faut analyser tous les fichiers de ce type ou uniquement les nouveaux fichiers. Pour réaliser la sélection, cliquez sur le lien **tous/nouveaux**, situé à côté du nom de type du fichier composé. Le lien change de valeur lorsque vous appuyez sur le bouton gauche de la souris.

   Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée, l'application analyse uniquement les nouveaux fichiers.

7. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

8. Dans le groupe **Analyse en arrière-plan**, exécutez une des actions suivantes :

   - Si vous ne souhaitez pas décompacter les fichiers composés en arrière-plan par l'Antivirus Fichiers, décochez la case **Décompacter les fichiers composés en arrière-plan**.

   - Si vous ne souhaitez pas décompacter les fichiers composés de grande taille en arrière-plan par l'Antivirus Fichiers, cochez la case **Décompacter les fichiers composés en arrière-plan**, indiquez la valeur requise dans le champ **Taille minimum de fichier**.

9. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Si vous ne souhaitez que l'Antivirus Fichiers décompacte les fichiers composés de grande taille, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

   - Si vous souhaitez décompacter les fichiers composés de grande taille par l'Antivirus Fichiers, décochez la case **Ne pas décompacter les fichiers composés de grande taille**.

     Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

   L'Antivirus Fichiers analyse les fichiers de grande taille extraits de l'archive, que la case **Ne pas décompacter les fichiers composés de grande taille** soit cochée ou non.

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

11. Dans la fenêtre **Antivirus Fichiers**, cliquez sur **OK**.

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

MODIFICATION DU MODE D'ANALYSE DES FICHIERS

Le *mode d'analyse* désigne la condition dans laquelle l'Antivirus Fichier va commencer l'analyse des fichiers. Par défaut, Kaspersky Endpoint Security utilise le mode intelligent d'analyse des fichiers. Dans ce mode d'analyse des fichiers, l'Antivirus Fichiers prend une décision sur la base de l'analyse des opérations exécutées par l'utilisateur, par l'application au nom de l'utilisateur (sous les données duquel l'entrée dans le système d'exploitation a eu lieu, ou sous les données d'un autre utilisateur) ou par le système d'exploitation sur les fichiers. Par exemple, dans le cas d'un fichier Microsoft Office Word, Kaspersky Endpoint Security analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Afin de modifier le mode d'analyse des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Fichiers**.

   Les paramètres du module Antivirus Fichiers s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Fichiers** s'ouvre.
4. Dans la fenêtre **Antivirus Fichiers**, sélectionnez l'onglet **Avancé**.
5. Dans le groupe **Mode d'analyse**, sélectionnez le mode requis :
   - **Mode intelligent**.
   - **Accès et modification**.
   - **Accès**.
   - **Exécution**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

SURVEILLANCE DU SYSTEME

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur la Surveillance du système et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DE LA SURVEILLANCE DU SYSTEME

La Surveillance du système récolte des données sur l'activité des applications sur l'ordinateur et offre ces informations aux autres modules afin qu'ils puissent offrir une protection plus efficace.

Modèles de comportement dangereux

Les modèles de comportement dangereux BSS (Behavior Stream Signatures) (ci-après : modèles de comportement dangereux) contiennent les séquences d'actions des applications que Kaspersky Endpoint Security juge dangereuses. Lorsque l'activité de l'application est identique à un modèle de comportement dangereux, Kaspersky Endpoint Security exécute l'action définie. La fonction de Kaspersky Endpoint Security qui repose sur les modèles de comportement dangereux garantit la protection proactive de l'ordinateur.

Par défaut, lorsque l'activité de l'application est parfaitement identique à un modèle de comportement dangereux, la Surveillance du système place le fichier exécutable de cette application en quarantaine (cf. section "Utilisation de la quarantaine et du dossier de sauvegarde" à la page 218).

Annulation des actions exécutées par des applications malveillantes

Sur la base des informations recueillies par la Surveillance du système, Kaspersky Endpoint Security peut annuler les actions exécutées par les programmes malveillants dans le système d'exploitation lors de la réparation des programmes malveillants.

L'annulation des actions des applications malveillantes peut être initiée par la défense proactive, l'Antivirus Fichier (cf. section "Protection du système de fichiers de l'ordinateur. Antivirus Fichiers" à la page 56) et pendant la recherche des virus (cf. section "Analyse de l'ordinateur" à la page 181).

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

ACTIVATION ET DESACTIVATION DE LA SURVEILLANCE DES VULNERABILITES

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

Il est déconseillé de désactiver la Surveillance du système sans raison valable, parce que cela entraîne une baisse d'efficacité des modules de la protection qui peuvent avoir besoin des informations recueillies par la Surveillance du système pour identifier avec une plus grande précision toute menace éventuelle détectée.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver la Surveillance du système, sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez-droit pour ouvrir le menu contextuel de la ligne avec les informations sur le module Surveillance du système.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer la Surveillance du système.

     L'icône du statut du fonctionnement du module , qui s'affiche à gauche dans la ligne **Surveillance du système**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver la Surveillance du système.

     L'icône du statut du fonctionnement du module , qui s'affiche à gauche dans la ligne **Surveillance du système**, sera modifiée sur l'icône .

Pour activer ou désactiver la Surveillance du système depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer la Surveillance du système** si vous souhaitez activer la Surveillance du système.

   - Décochez la case **Activer la Surveillance du système** si vous souhaitez désactiver la Surveillance du système.

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

UTILISATION DES MODELES DE COMPORTEMENT DANGEREUX

Pour utiliser les modèles de comportement dangereux, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Défense proactive**, cochez la case **Utiliser les modèles actualisés de comportement dangereux (BSS)**.

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

   - **Sélectionner l'action automatiquement**. Si cet élément est sélectionné, Kaspersky Endpoint Security exécute l'action définie comme action par défaut par les experts de Kaspersky Lab. en cas de détection d'une activité malveillante de l'application. Par défaut, Kaspersky Endpoint Security place le fichier exécutable du programme malveillant en quarantaine.

   - **Placer le fichier en quarantaine**. Si cet élément est sélectionné, Kaspersky Endpoint Security place le fichier exécutable de l'application en quarantaine en cas de détection d'une activité malveillante de l'application.

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

   - **Ignorer**. Si cet élément est sélectionné, Kaspersky Endpoint Security n'exécute aucune action sur le fichier exécutable de l'application en cas de détection d'une activité malveillante de l'application.

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

ANNULATION DES ACTIONS DES APPLICATIONS MALVEILLANTES LORS DE LA REPARATION

Pour activer ou désactiver l'annulation des actions des applications malveillantes, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance du système**.

   Les paramètres du module **Surveillance du système** s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cocher la case **Annuler les actions des applications malveillantes lors de la réparation**, si vous souhaitez que Kaspersky Endpoint Security annule les actions exécutées par les applications malveillantes dans votre système d'exploitation lors de leur réparation.

   - Décocher la case **Annuler les actions des applications malveillantes lors de la réparation**, si vous souhaitez que Kaspersky Endpoint Security n'annule pas les actions exécutées par les applications malveillantes dans votre système d'exploitation lors de leur réparation.

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

PROTECTION DU COURRIER. ANTIVIRUS COURRIER

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur l'Antivirus Courrier et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DE L'ANTIVIRUS COURRIER

L'Antivirus Courrier analyse l'ensemble du courrier entrant et sortant à la recherche de virus et d'autres applications présentant une menace. Il démarre au lancement de Kaspersky Endpoint Security, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages reçus ou envoyés via les protocoles POP3, SMTP, IMAP, MAPI et NNTP.

L'icône dans la zone de notification de la barre des tâches indique le fonctionnement de l'Antivirus Courrier. L'icône prend cette apparence  chaque fois qu'un message électronique est analysé. 

L'Antivirus Courrier intercepte et analyse chaque message reçu ou envoyé par l'utilisateur. Si aucune menace n'a été découverte dans le message, le message devient accessible à l'utilisateur.

En cas de découverte d'une menace dans le fichier, Kaspersky Endpoint Security attribue au fichier un des états suivants :

- Etat qui désigne le type de l'application malveillante détectée (par exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* (suspect) lorsqu'il est impossible d'affirmer avec certitude si le message est infecté ou non. Le message contient peut-être une séquence de code propre aux virus et aux autres applications présentant une menace ou la modification d'un code de virus connu.

Ensuite, l'application bloque le message électronique, affiche une notification (cf. page 215) (si cela a été défini dans les paramètres des notifications) sur la menace détectée à l'écran et exécute l'action définie dans les paramètres de l'Antivirus Courrier (cf. section "Modification de l'action sur les messages infectés" à la page 75).

Pour les applications Microsoft Office Outlook® et The Bat!, il existe des modules d'extension (ci-après plug-ins) permettant de réaliser une configuration plus détaillée des paramètres d'analyse du courrier. Le plug-in de l'Antivirus Courrier est intégré aux clients de la messagerie Microsoft Office Outlook et The Bat! lors de l'installation de Kaspersky Endpoint Security.

L'Antivirus Courrier ne prend pas en charge les protocoles qui assurent le transfert sécurisé des données.

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS COURRIER

Par défaut, l'Antivirus Courrier est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Courrier le cas échéant.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver l'Antivirus Courrier sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Antivirus Courrier.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Courrier.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Courrier**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Courrier.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Courrier**, sera modifiée sur l'icône .

Pour activer ou désactiver l'Antivirus Courrier depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans le groupe Protection antivirus qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'Antivirus Courrier** pour activer l'Antivirus Courrier.
   - Décochez la case **Activer l'Antivirus Courrier** pour désactiver l'Antivirus Courrier.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE L'ANTIVIRUS COURRIER

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Courrier :

- Modifier le niveau de protection du courrier.

  Vous pouvez sélectionner un des niveaux de protection prédéfinis pour le courrier ou personnaliser le niveau de protection du courrier.

  Après avoir modifié les paramètres du niveau de protection du courrier, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de protection du courrier.

- Modifier l'action que Kaspersky Endpoint Security exécute sur les messages infectés.

- Constituer la zone de protection de l'Antivirus Courrier.

- Configurer l'analyse des fichiers composés joints aux messages.

  Vous pouvez activer ou désactiver l'analyse des archives jointes aux messages, limiter la taille maximale des objets analysés joints aux messages et la période maximale d'analyse des objets joints aux messages.

- Configurer le filtrage selon le type des pièces jointes présentes dans les messages.

  Le filtrage selon le type des pièces jointes dans les messages permet de renommer ou de supprimer automatiquement les fichiers des types indiqués.

- Configurer l'utilisation de l'analyse heuristique.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier dans les messages de nouvelles menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

- Configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook.

  Vous pouvez intégrer dans le client de messagerie Microsoft Office Outlook le plug-in qui permet de personnaliser la configuration des paramètres de l'analyse du courrier.

- Configurer les paramètres de l'analyse du courrier dans l'application The Bat!.

  Vous pouvez intégrer dans le client de messagerie The Bat! le plug-in qui permet de personnaliser la configuration des paramètres de l'analyse du courrier.

  S'agissant des autres clients de messagerie (dont Microsoft Outlook Express®, Windows Mail et Mozilla™ Thunderbird™), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

  Lorsqu'il s'agit du client de messagerie Mozilla Thunderbird, l'Antivirus Courrier ne soumet pas à la recherche de virus et d'autres applications présentant une menace, des messages transmis via le protocole IMAP en cas d'utilisation de filtres triant les messages du dossier **Boîte aux lettres**.

DANS CETTE SECTION

MODIFICATION DU NIVEAU DE PROTECTION DU COURRIER

L'Antivirus Courrier utilise de différents ensembles de paramètres afin de protéger votre courrier. Ces ensembles de paramètres sont appelés *niveaux de protection du courrier*. Il existe trois niveaux prédéfinis de protection du courrier : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de protection du courrier **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky Lab.

Afin de modifier le niveau de protection du courrier, exécutez l'opération suivante :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, exécutez une des actions suivantes :
   - Pour définir un des niveaux prédéfinis de protection du courrier (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de protection des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Courrier** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de protection du courrier, le nom du niveau de protection du courrier dans le groupe **Niveau de protection** devient **Autre**.
   - Pour sélectionner le niveau de protection du courrier **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DE L'ACTION SUR LES MESSAGES INFECTES

Pour modifier l'action à exécuter sur les messages infectés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un message infecté :
   - **Sélectionner l'action automatiquement**.
   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible**.
   - **Exécuter l'action : Réparer**.
   - **Exécuter l'action : Supprimer**.
   - **Exécuter l'action : Bloquer**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS COURRIER

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. Les propriétés de la zone de protection de l'Antivirus Courrier sont les paramètres d'intégration de l'Antivirus Courrier aux clients de messagerie, le type de messages et les protocoles de courrier électronique dont le trafic est analysé par l'Antivirus Courrier. Par défaut, Kaspersky Endpoint Security analyse l'ensemble du courrier entrant et sortant, le trafic des protocoles de courrier électronique POP3, SMTP, NNTP et IMAP, et s'intègre aux clients de messagerie Microsoft Office Outlook et The Bat!.

Pour former la zone de protection de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   L'onglet **Général** de la fenêtre **Antivirus Courrier** s'ouvre.

4. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :

   - Sélectionnez l'option **Analyser le courrier entrant et sortant**, si vous souhaitez que l'Antivirus Courrier analyse tout le courrier entrant et sortant sur votre ordinateur.

   - Sélectionnez l'option **Analyser uniquement le courrier entrant**, si vous souhaitez que l'Antivirus Courrier analyse uniquement le courrier entrant sur votre ordinateur.

   Si vous sélectionnez l'analyse du courrier entrant uniquement, il est recommandé d'analyser une fois le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

5. Dans le groupe **Intégration au système** procédez comme suit :

   - Cochez la case **Trafic POP3/SMTP/NNTP/IMAP**, si vous souhaitez que l'Antivirus Courrier analyse les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur.

     Cochez la case **Trafic POP3/SMTP/NNTP/IMAP**, si vous souhaitez que l'Antivirus Courrier n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP avant qu'ils n'atteignent l'ordinateur de l'utilisateur. Dans ce cas, les messages analysent les plug-ins de l'Antivirus Courrier intégrés à Microsoft Office Outlook et The Bat! après leur réception sur l'ordinateur de l'utilisateur.

   Si vous utilisez un autre programme de messagerie que Microsoft Office Outlook et The Bat!, si la case **Trafic POP3/SMTP/NNTP/IMAP** est décochée, l'Antivirus Courrier n'analyse pas les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP.

   Si les cases **Avancé : plugin dans Microsoft Office Outlook** et **Avancé : plugin dans The Bat**! sont décochées, l'Antivirus Courrier ignore également les messages transmis via les protocoles POP3, SMTP, NNTP et IMAP.

   - Cochez la case **Avancé : plugin dans Microsoft Office Outlook**, si vous souhaitez donner l'accès à la configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et activer l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur du côté du plug-in intégré à l'application Microsoft Office Outlook.

   - Cochez la case **Avancé : plugin dans The Bat!**, si vous souhaitez activer l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur du côté du plug-in intégré à l'application The Bat!

     Décochez la case **Avancé : plugin dans The Bat!**, si vous souhaitez désactiver l'analyse des messages transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI après leur réception sur l'ordinateur de l'utilisateur du côté du plug-in intégré dans l'application The Bat!.

   Le plug-in de l'Antivirus Courrier est intégré aux clients de la messagerie Microsoft Office Outlook et The Bat! lors de l'installation de Kaspersky Endpoint Security.

6. Cliquez sur le bouton **OK**.

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

ANALYSE DES FICHIERS COMPOSES JOINTS AUX MESSAGES

Pour configurer l'analyse des fichiers composés joints aux messages, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
4. Sous l'onglet **Général** dans le groupe **Analyse des fichiers composés**, procédez comme suit :
   - Décochez la case **Analyser les archives jointes** si vous souhaitez que l'Antivirus Courrier n'analyse pas les archives jointes aux messages.
   - Cochez la case **Ne pas analyser les archives jointes de plus de N Mo** si vous souhaitez que l'Antivirus Courrier n'analyse pas les objets joints aux messages dont la taille dépasse N Mo. Si vous avez coché cette case, indiquez la taille maximale des archives dans le champ à côté du nom de la case.
   - Cochez la case **Ne pas analyser les archives plus de** si vous souhaitez que l'Antivirus Courrier n'analyse pas les archives jointes aux messages plus de N secondes.
5. Cliquez sur le bouton **OK**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

FILTRAGE DES PIECES JOINTES DANS LES MESSAGES

Les applications malveillantes peuvent se diffuser via le courrier électronique sous forme de pièces jointes dans les messages. Vous pouvez configurer le filtrage selon le type des pièces jointes présentes dans les messages permettant ainsi de renommer automatiquement ou de supprimer les fichiers des types indiqués.

Pour configurer le filtrage des pièces jointes, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Courrier** s'ouvre.
4. Dans la fenêtre **Antivirus Courrier** sélectionnez l'onglet **Filtre des pièces jointes**.

5. Exécutez une des actions suivantes :

   - Sélectionnez le paramètre **Désactiver le filtrage** si vous souhaitez que l'Antivirus Courrier ne filtre pas les pièces jointes dans les messages.

   - Sélectionnez le paramètre **Renommer les pièces jointes du type indiqué** si vous souhaitez que l'Antivirus Courrier change les noms des fichiers des types indiqués joints aux messages.

   - Sélectionnez le paramètre **Supprimer les pièces jointes du type indiqué**, si vous souhaitez que l'Antivirus Courrier supprime les fichiers des types indiqués joints aux messages.

6. Exécutez une des actions suivantes :

   - Si dans le paragraphe 5 de l'instruction vous avez sélectionné le paramètre **Désactiver le filtrage**, passez au paragraphe 7.

   - Si dans le paragraphe 5 de l'instruction vous avez sélectionné le paramètre **Renommer les pièces jointes du type indiqué** ou le paramètre **Supprimer les pièces jointes du type indiqué**, la liste des types de fichiers devient active. Cochez les cases en regard des types requis de fichiers.

     Vous pouvez modifier la liste des types de fichiers avec les boutons **Ajouter**, **Modifier**, **Supprimer**.

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

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

UTILISATION DE L'ANALYSE HEURISTIQUE

Afin d'utiliser l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus**, sélectionnez la section **Antivirus Courrier**.

   Les paramètres du module Antivirus Courrier s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre **Antivirus Courrier** s'ouvre.

4. Dans la fenêtre **Antivirus Courrier**, sélectionnez l'onglet **Avancé**.

5. Sous l'onglet **Avancé** dans le groupe **Méthodes d'analyse**, cochez la case **Analyse heuristique**.

6. Sélectionnez à l'aide du curseur le niveau de détail des tests en l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.

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

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

ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Lors de l'installation de Kaspersky Endpoint Security, un plug-in spécial est intégré à l'application Microsoft Office Outlook. Il permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier depuis l'application Microsoft Office Outlook et d'indiquer le moment à analyser les messages sur la présence de virus et d'autres applications présentant une menace. Le plug-in de messagerie Microsoft Office Outlook peut analyser les messages entrants et sortants transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI.

La configuration de l'Antivirus Courrier depuis Microsoft Office Outlook est disponible dans le cas, si la case **Avancé : plugin dans Microsoft Office Outlook** est cochée dans l'interface de l'application Kaspersky Endpoint Security.

Les messages entrants et sortants dans Microsoft Office Outlook sont tout d'abord vérifiés par l'Antivirus Courrier (si la case **Trafic POP3/SMTP/NNTP/IMAP** est cochée), puis par le plug-in de messagerie de Microsoft Office Outlook. Lorsque l'Antivirus Courrier détecte un objet malveillant dans un message électronique, il vous en avertit.

D'après l'action sélectionnée dans la fenêtre de notification dépend qui élimine la menace dans le message : l'Antivirus Courrier ou le plug-in de messagerie Microsoft Office Outlook :

- Si l'utilisateur a sélectionné dans la fenêtre de notification de l'Antivirus Courrier l'action **Réparer** ou **Supprimer**, l'action liée à la suppression de la menace sera exécutée par l'Antivirus Courrier.

- Si l'utilisateur a sélectionné dans la fenêtre de notification de l'Antivirus Courrier l'action **Ignorer**, l'action liée à la suppression de la menace sera exécutée par le plug-in de messagerie de l'application Microsoft Office Outlook.

Le courrier sortant est analysé d'abord par le plug-in de messagerie de l'application Microsoft Office Outlook et ensuite par l'Antivirus Courrier.

Pour configurer les paramètres de l'analyse du courrier dans l'application Microsoft Office Outlook, procédez comme suit :

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.

2. Dans le menu de l'application, sélectionnez l'option **Service** → **Paramètres**.

   La fenêtre **Paramètres** s'ouvre.

3. Dans la fenêtre **Paramètres**, sélectionnez l'onglet **Protection du courrier**.

VOIR EGALEMENT

Formation de la zone de protection de l'Antivirus Courrier 75

ANALYSE DU COURRIER DANS THE BAT!

Lors de l'installation de Kaspersky Endpoint Security un plug-in spécifique est intégré dans l'application The Bat!. Il permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier depuis l'application The Bat! et de définir le moment à analyser les messages sur la présence de virus et d'autres applications présentant une menace. Le plug-in de messagerie The Bat! peut analyser les messages entrants et sortants transmis via les protocoles POP3, SMTP, NNTP, IMAP et MAPI.

La configuration des paramètres de l'Antivirus Courrier depuis The Bat! est disponible dans le cas, si la case **Avancé : plugin dans The Bat!** est cochée dans l'interface de l'application Kaspersky Endpoint Security.

Dans l'application The Bat!, les messages du courrier entrant sont d'abord analysés par l'Antivirus Courrier (si la case **Trafic POP3/SMTP/NNTP/IMAP** est cochée dans l'interface de Kaspersky Endpoint Security), puis ils sont analysés par le plug-in de messagerie de The Bat!. Lorsque l'Antivirus Courrier détecte un objet malveillant dans un message électronique, il vous en avertit.

D'après l'action sélectionnée dans la fenêtre de notification dépend qui élimine la menace dans le message : l'Antivirus Courrier ou le plug-in de messagerie The Bat! :

- Si l'utilisateur sélectionne dans la fenêtre de notification l'action **Réparer** ou **Supprimer**, l'action de suppression de la menace sera exécutée par l'Antivirus Courrier.

- Si l'utilisateur a sélectionné dans la fenêtre de notification l'action **Ignorer**, l'action liée à la suppression de la menace sera exécutée par le plug-in de messagerie de l'application The Bat!.

Le courrier sortant est analysé d'abord par le plug-in de messagerie de l'application The Bat! et ensuite par l'Antivirus Courrier.

L'application The Bat! a ses propres outils pour les actions à exécuter sur le courrier infecté. Vous pouvez configurer les paramètres suivants :

- sélectionner le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant) ;

- définir le moment de l'analyse du courrier (avant d'ouvrir le message, avant d'enregistrer le message sur un disque) ;

- déterminer l'action que l'application The Bat! exécute en cas de détection des messages électroniques infectés :

  - **Tenter de réparer les parties infectées**. Si vous avez sélectionné cette option, l'application The Bat! tente de réparer les messages électroniques infectés. Si la réparation s'est avérée impossible, l'application The Bat! ne modifie rien aux messages électroniques.

  - **Supprimer les parties infectées**. Si vous avez sélectionné cette option, l'application The Bat! supprime les messages électroniques infectés ou les messages électroniques potentiellement infectés.

  Par défaut, l'application The Bat! place tous les messages électroniques infectés en quarantaine sans tentative de réparation.

  L'application The Bat! ne marque pas les messages électroniques infectés par un en-tête spécifique.

Pour configurer les paramètres de l'analyse du courrier dans l'application The Bat!, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application The Bat!.
2. Dans le menu **Propriétés**, sélectionnez l'option **Configuration**.
3. Dans l'arborescence des paramètres, choisissez l'objet **Protection contre les virus**.

VOIR EGALEMENT

Formation de la zone de protection de l'Antivirus Courrier 75

PROTECTION DE L'ORDINATEUR SUR L'INTERNET. ANTIVIRUS INTERNET

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur l'Antivirus Internet et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DE L'ANTIVIRUS INTERNET

Chaque fois que l'utilisateur travaille sur Internet, les informations enregistrées sur son ordinateur sont exposées à un risque d'infection par des virus et par d'autres applications présentant une menace. Ces menaces peuvent s'introduire dans l'ordinateur lors du téléchargement d'applications gratuites ou lors de la consultation de sites Internet, attaqués par des pirates, avant la visite de l'utilisateur. De plus, les vers de réseau peuvent s'introduire sur l'ordinateur des utilisateurs avant l'ouverture des pages Internet ou le téléchargement d'un fichier, directement à l'ouverture de la connexion Internet.

L'Antivirus Internet protège les informations qui arrivent sur l'ordinateur des utilisateurs et qui sont envoyées depuis celui-ci via les protocoles HTTP et FTP. Il permet également de déterminer si un lien est suspect ou s'il mène à un site d'hameçonnage.

Chaque page Internet ou fichier qu'accède l'utilisateur ou une application via le protocole HTTP ou FTP sont interceptés et analysés par l'Antivirus Internet pour découvrir la présence éventuelle de virus et d'autres applications présentant une menace :

- Si aucun code malveillant n'a été détecté sur la page Internet ou dans le fichier, ils deviennent immédiatement accessibles à l'utilisateur.
- Si la page Internet ou le fichier que souhaite ouvrir l'utilisateur contient un code malveillant, l'application exécute l'action définie dans les paramètres de l'Antivirus Internet (cf. section "Modification de l'action à réaliser sur les objets malveillants du trafic Internet" à la page 84).

L'Antivirus Internet ne prend pas en charge les protocoles qui assurent le transfert sécurisé des données.

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS INTERNET

Par défaut, l'Antivirus Internet est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus Internet le cas échéant.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver l'Antivirus Internet sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Antivirus Internet.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer l'Antivirus Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Internet**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver l'Antivirus Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus Internet**, sera modifiée sur l'icône .

Pour activer ou désactiver l'Antivirus Internet depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'Antivirus Internet** pour activer l'Antivirus Internet.
   - Décochez la case **Activer l'Antivirus Internet** pour désactiver l'Antivirus Internet.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE L'ANTIVIRUS INTERNET

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus Internet :

- Modifier le niveau de protection du trafic Internet.

  Vous pouvez sélectionner un des niveaux prédéfinis de protection du trafic Internet reçus ou envoyés via les protocoles HTTP et FTP, ou personnaliser le niveau de protection du trafic Internet.

  Après avoir modifié les paramètres du niveau de protection du trafic Internet, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de protection du trafic Internet.

- Modifier l'action que Kaspersky Endpoint Security exécutera sur les objets infectés du trafic Internet.

  Si l'analyse d'un objet du trafic Internet par l'Antivirus Internet détermine la présence d'un code malveillant, la suite des opérations de l'Antivirus Internet dépendra de l'action que vous aurez spécifiée.

- Configurer l'Analyse par Antivirus Internet des liens par rapport aux bases d'URL de phishing ou suspectes.

- Configurer l'utilisation de l'analyse heuristique lors de la recherche d'éventuels virus dans le trafic Internet et d'autres applications présentant une menace.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier de nouvelles menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

- Configurer l'utilisation de l'analyse heuristique lors de la recherche d'éventuels liens de phishing sur les pages Internet.

- Optimiser l'analyse par l'Antivirus Internet du trafic Internet sortant et entrant via les protocoles HTTP et FTP.

- Composer la liste des URL de confiance.

  Vous pouvez composer une liste des URL dont vous faites confiance au contenu. Antivirus Internet ne recherche pas la présence éventuelle des virus et d'autres applications présentant une menace dans les informations en provenance des URL de confiance. Cette fonctionnalité peut être utilisée, par exemple, si l'Antivirus Internet empêche le téléchargement d'un fichier depuis un site Internet que vous connaissez.

Le terme URL signifie à la fois l'URL d'une page Internet et celle d'un site Internet.

DANS CETTE SECTION

MODIFICATION DU NIVEAU DE PROTECTION DU TRAFIC INTERNET

Pour protéger les données reçues ou envoyées via les protocoles HTTP et FTP, l'Antivirus Internet utilise de différents ensembles de paramètres. Ces ensembles de paramètres sont appelés *niveaux de protection du trafic Internet*. Il existe trois niveaux prédéfinis de protection du trafic Internet : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de protection de protection du trafic Internet **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky Lab.

Afin de modifier le niveau de protection du trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, exécutez une des actions suivantes :
   - Pour définir un des niveaux prédéfinis de protection du trafic Internet (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de protection du trafic Internet, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre **Antivirus Internet** qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de protection du trafic Internet, le nom du niveau de protection du trafic Internet dans le groupe **Niveau de protection** devient **Autre**.
   - Pour sélectionner le niveau de protection du trafic Internet **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS MALVEILLANTS DU TRAFIC INTERNET

Pour modifier l'action sur les objets malveillants du trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Action en cas de découverte d'une menace**, sélectionnez l'action que Kaspersky Endpoint Security exécutera sur les objets malveillants du trafic Internet :
   - **Sélectionner l'action automatiquement**.
   - **Interdire le chargement**.
   - **Autoriser le chargement**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ANALYSE DES LIENS PAR RAPPORT AUX BASES D'URL DE PHISHING OU SUSPECTES

La vérification des liens pour voir s'ils appartiennent aux URL de phishing permet d'éviter les *attaques d'hameçonnage (phishing)*. L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel de la banque. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse du site s'affiche, toutefois vous vous trouvez sur un site fictif. Toutes vos actions sur ce site sont surveillées et pourraient servir au vol de votre argent.

Dans la mesure où le lien vers un site d'hameçonnage (phishing) peut figurer non seulement dans un courrier, mais également dans un message ICQ, l'Antivirus Internet contrôle les tentatives d'accès à un site d'hameçonnage (phishing) au niveau de l'analyse du trafic Internet et bloque l'accès à ces sites Internet. La liste des adresses de phishing est reprise dans la distribution de Kaspersky Endpoint Security.

Pour configurer l'analyse par l'Antivirus Internet des liens en fonction des bases d'URL suspectes ou de phishing, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Méthodes d'analyse** procédez comme suit :

   - Cochez la case **Analyser les liens selon la base des URL suspectes**, si vous souhaitez que l'Antivirus Internet analyse les liens selon la base des URL suspectes.
   - Cochez la case **Analyser les liens selon la base des URL de phishing**, si vous souhaitez que l'Antivirus Internet analyse les liens selon la base des URL de phishing.

   Pour analyser les liens, vous pouvez également utiliser les bases de données de réputation de Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 257).
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

UTILISATION DE L'ANALYSE HEURISTIQUE DANS L'ANTIVIRUS INTERNET

Pour configurer l'utilisation de l'analyse heuristique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Méthodes d'analyse**, procédez comme suit :

   - Si vous souhaitez que l'Antivirus Internet utilise l'analyse heuristique lors de la recherche d'éventuels virus et d'autres applications présentant une menace dans le trafic Internet, cochez la case **Analyse heuristique pour la recherche des virus** et sélectionnez le niveau de détail de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse** à l'aide du curseur.

   - Si vous souhaitez que l'Antivirus Internet utilise l'analyse heuristique lors de la recherche d'éventuels liens de phishing sur les pages Internet, cochez la case **Analyse heuristique pour la recherche des liens de phishing** et sélectionnez le niveau de détail de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse** à l'aide du curseur.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE LA DUREE DE LA MISE EN CACHE DU TRAFIC INTERNET

Afin d'augmenter l'efficacité de la détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. En utilisant la mise en cache, l'Antivirus Internet analyse les objets uniquement après qu'ils aient été entièrement reçus sur l'ordinateur.

Le recours à la mise en cache augmente la durée de traitement des objets et retarde leur transfert à l'utilisateur. De plus, la mise en cache peut entraîner des problèmes lors du téléchargement et du traitement de grands objets en raison de l'expiration du délai d'attente de la connexion du client HTTP.

Pour résoudre ce problème, la possibilité de limiter la durée de la mise en cache des fragments des objets envoyés via Internet est prévue. Une fois le délai écoulé, chaque partie de l'objet reçue sera transmise à l'utilisateur sans vérification et l'objet sera analysé complètement une fois qu'il aura été copié. Ceci permet d'accélérer le transfert de l'objet à l'utilisateur et de résoudre le problème de la déconnexion. Le niveau de protection de l'utilisation d'Internet ne sera pas réduit pour la cause.

La levée de la restriction sur la durée de la mise en cache du trafic Internet améliore l'efficacité de l'analyse antivirus mais provoque en même temps un ralentissement de l'accès aux objets.

Pour configurer la durée de la mise en cache du trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Dans la fenêtre **Antivirus Internet**, sélectionnez l'onglet **Général**.
5. Dans le groupe **Avancé**, exécutez une des actions suivantes :
   - Cochez la case **Limiter la durée de mise en cache du trafic Internet** pour limiter la durée de mise en cache du trafic Internet et pour accélérer l'analyse.
   - Décochez la case **Limiter la durée de mise en cache du trafic Internet** pour supprimer la limite de la durée de mise en cache du trafic Internet.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONSTITUTION D'UNE LISTE DES URL DE CONFIANCE

Pour composer une liste d'URL de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus Internet**.

   Les paramètres du module Antivirus Internet s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration**.

   La fenêtre **Antivirus Internet** s'ouvre.
4. Sélectionnez l'onglet **Sites de confiance**.
5. Cochez la case **Ne pas analyser le trafic Internet en provenance des URL de confiance**.
6. Formez la liste des sites Internet/pages Internet dont vous considérez le contenu comme étant fiable. Pour ce faire, procédez comme suit :
   a. Cliquez sur le bouton **Ajouter**.

      La fenêtre **Adresse/Masque d'adresse** s'ouvrira.

   b. Saisissez l'adresse du site Internet/de la page Internet ou le masque d'adresse du site Internet/de la page Internet.

   c. Cliquez sur le bouton **OK**.

      Un nouvel enregistrement apparaîtra dans la liste des adresses Internet de confiance.

   d. Répétez les paragraphes a–c de l'instruction si nécessaire.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

PROTECTION DU TRAFIC DES CLIENTS DE MESSAGERIES INSTANTANEES. ANTIVIRUS IM ("CHAT")

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur l'Antivirus IM et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DE L'ANTIVIRUS IM

L'Antivirus IM est prévu pour analyser le trafic transmis par les *clients de messagerie instantanée*.

Les messages transmis via les clients de messagerie instantanée peuvent contenir les types suivants de menaces contre la sécurité de l'ordinateur :

- Des liens dont l'activation déclenche le téléchargement d'une application malveillante sur l'ordinateur de la victime.
- Des liens sur les applications et les pages Internet malveillantes que les individus malintentionnés utilisent pour les attaques d'hameçonnage (phishing).

  Le but des attaques de phishing est de voler les informations personnelles des utilisateurs, notamment les numéros des cartes de crédit, les informations sur leurs passeports, les mots de passe pour les systèmes de payement des établissements bancaires ou pour d'autres services en ligne (par exemple, les réseaux sociaux ou les services de messagerie en ligne).

Les clients de messagerie instantanée permettent la transmission des fichiers. Pendant la tentative d'enregistrement de ces fichiers, ils sont analysés par le module Antivirus Fichiers (cf. section "A propos de l'Antivirus Fichiers" à la page 56).

L'Antivirus IM intercepte chaque message envoyé ou reçu via un client de messagerie instantanée et recherche dans ceux-ci la présence éventuelle d'objets dangereux pour l'ordinateur :

- En l'absence d'objets présentant une menace, le message devient accessible à l'utilisateur.
- Si le message contient des objets présentant une menace, l'Antivirus IM remplace le message par les informations sur la menace détectée dans la fenêtre des messages du client de messagerie instantanée.

L'Antivirus IM ne prend pas en charge les protocoles qui assurent le transfert sécurisé des données. L'Antivirus IM n'analyse pas le trafic transmis via les clients de messagerie instantanée qui utilisent une connexion sécurisée.

ACTIVATION ET DESACTIVATION DE L'ANTIVIRUS IM

Par défaut, l'Antivirus IM est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Vous pouvez désactiver l'Antivirus IM le cas échéant.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver l'Antivirus IM sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez-droit sur la ligne **Antivirus IM** pour ouvrir le menu contextuel des actions du module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu contextuel l'option **Arrêter** si vous voulez désactiver l'Antivirus IM.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus IM**, sera modifiée sur l'icône .
   - Sélectionnez l'option **Désactiver** dans le menu contextuel si vous voulez désactiver l'Antivirus IM.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Antivirus IM**, sera modifiée sur l'icône .

Pour activer ou désactiver l'Antivirus IM depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'Antivirus IM** pour activer l'Antivirus IM.
   - Décochez la case **Activer l'Antivirus IM** pour désactiver l'Antivirus IM.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE L'ANTIVIRUS IM

Vous pouvez exécuter les opérations suivantes pour configurer l'Antivirus IM :

- Constituer la zone de protection.

  Vous pouvez élargir ou restreindre la zone de protection en modifiant le type de messages à analyser reçus par les clients de messagerie instantanée.

- Configurer l'Analyse par Antivirus IM des liens dans les messages des clients de messagerie instantanée par rapport aux bases d'URL suspectes ou de phishing.

- Configurer l'utilisation de l'analyse heuristique.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des applications dans le système d'exploitation. L'analyse heuristique permet d'identifier dans les messages des clients de messagerie instantanée de nouvelles menaces qui ne figurent pas encore dans les bases de Kaspersky Endpoint Security.

DANS CETTE SECTION

FORMATION DE LA ZONE DE PROTECTION DE L'ANTIVIRUS IM

La zone de protection fait référence aux objets analysés par le module. Les propriétés de la zone de protection des modules différents peuvent varier. La propriété de la zone de protection de l'Antivirus IM est le type des messages analysés reçus et envoyés via les clients de messagerie instantanée. L'Antivirus IM analyse par défaut le courrier entrant et le courrier sortant. Vous pouvez vous passer de l'analyse des messages sortants.

Pour former la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Zone de protection**, exécutez une des actions suivantes :

   - Sélectionnez l'option **Analyser le courrier entrant et sortant**, si vous souhaitez que l'Antivirus IM analyse tout le courrier entrant et sortant des clients de messagerie instantanée.

   - Sélectionnez l'option **Analyser uniquement le courrier entrant**, si vous souhaitez que l'Antivirus IM analyse uniquement le courrier entrant des clients de messagerie instantanée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ANALYSE PAR L'ANTIVIRUS IM DES LIENS PAR RAPPORT AUX BASES D'URL DE PHISHING OU SUSPECTES

Pour configurer l'analyse par l'Antivirus IM des liens en fonction des bases d'URL suspectes ou de phishing, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Méthodes d'analyse** cochez les cases à côté des noms des méthodes que vous souhaitez utiliser lors du fonctionnement de l'Antivirus IM :
   - Cochez la case **Analyser les liens selon la base des URL suspectes**, si vous voulez analyser les liens dans les messages des clients de messagerie instantanée par rapport à la base des URL suspectes.
   - Cochez la case **Analyser les liens selon la base des URL de phishing**, si vous voulez analyser les liens dans les messages des clients de messagerie instantanée par rapport à la base des URL de phishing.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

UTILISATION DE L'ANALYSE HEURISTIQUE DANS L'ANTIVIRUS IM ("CHAT")

Pour configurer l'utilisation de l'analyse heuristique dans le fonctionnement de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Antivirus IM**.

   Les paramètres du module Antivirus IM s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Méthodes d'analyse**, procédez comme suit :
   a. Cochez la case **Analyse heuristique**.
   b. Sélectionnez à l'aide du curseur le niveau de détail de l'analyse heuristique : **superficielle**, **moyenne** ou **minutieuse**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

PROTECTION DU RESEAU

Cette section contient les informations sur les principes de fonctionnement et sur la configuration des modules Pare-feu et Prévention des intrusions, ainsi que sur le contrôle du trafic de réseau.

DANS CETTE SECTION

PARE-FEU

Cette section contient des informations sur le Pare-feu et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DU PARE-FEU

Tout ordinateur connecté aux réseaux locaux et à l'Internet risque non seulement une infection par des virus et d'autres applications présentant une menace, mais il est aussi ouvert aux différentes attaques qui exploitent les vulnérabilités des systèmes d'exploitation et du logiciel.

Le Pare-feu garantit la protection des données personnelles stockées sur l'ordinateur de l'utilisateur, car il bloque toutes les menaces éventuelles pour le système d'exploitation lorsque l'ordinateur est connecté à l'Internet ou au réseau local. Le Pare-feu permet de détecter toutes les connexions réseau sur l'ordinateur de l'utilisateur et d'afficher une liste de leurs adresses IP en indiquant l'état de la connexion réseau par défaut.

Le module Pare-feu filtre toute activité réseau conformément aux règles réseau (cf. section "A propos des règles réseau" à la page 93). La configuration des règles réseau permet de définir le niveau de la protection de l'ordinateur qui peut varier entre un blocage complet de l'accès Internet et l'autorisation de l'accès illimité.

ACTIVATION ET DESACTIVATION DU PARE-FEU

Par défaut, le Pare-feu est activé et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver le Pare-feu.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver le Pare-feu sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez-droit sur la ligne **Pare-feu** et ouvrez le menu contextuel des actions du Pare-feu.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu contextuel l'option **Arrêter** si vous voulez désactiver le Pare-feu.

     L'icône de l'état du fonctionnement du module  , qui s'affiche à gauche dans la ligne **Pare-feu**, sera modifiée sur l'icône  .
   - Sélectionnez l'option **Désactiver** dans le menu contextuel si vous voulez désactiver le Pare-feu.

     L'icône de l'état du fonctionnement du module  , qui s'affiche à gauche dans la ligne **Pare-feu**, sera modifiée sur l'icône  .

Pour activer ou désactiver le Pare-feu depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer le Pare-feu** pour activer le Pare-feu.
   - Décochez la case **Activer le Pare-feu** pour désactiver le Pare-feu.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A PROPOS DES REGLES RESEAU

La règle réseau est une action d'autorisation ou d'interdiction que le Pare-feu exécute lorsqu'il détecte une tentative de connexion réseau.

Le Pare-feu réalise la protection contre les différents types d'attaques réseau sur deux niveaux : niveau de réseau et niveau appliqué. La protection au niveau de réseau est assurée par l'application des règles pour les paquets réseau. La protection au niveau appliqué est garantie grâce à l'application de règles d'utilisation des ressources de réseau pour les applications installées sur l'ordinateur de l'utilisateur.

Les deux niveaux de protection du Pare-feu vous permettent de créer :

- *Règles pour les paquets réseau*. Elles sont utilisées pour définir des restrictions pour les paquets réseau quelles que soient les applications. Ces règles limitent l'activité réseau entrante et sortante pour des ports spécifiques du protocole de transfert des données sélectionné. Le Pare-feu définit certaines règles pour les paquets réseau par défaut.
- *Règles réseau des applications*. Elles sont utilisées pour limiter l'activité réseau d'une application spécifique. Elles tiennent compte non seulement des caractéristiques du paquet réseau, mais aussi de l'application spécifique destinataire ou expéditeur de ce paquet réseau. Ces règles permettent de configurer en détail le filtrage de l'activité réseau lorsque, par exemple, un type déterminé des connexions réseau est interdit pour certaines applications mais autorisé pour d'autres.

Les règles pour les paquets réseau ont une priorité plus élevée que les règles réseau des applications. Si des règles pour les paquets réseau et des règles réseau des applications sont définies pour la même activité réseau, celle-ci sera traitée selon les règles pour les paquets réseau.

Vous pouvez définir pour chacune des règles pour les paquets réseau et chacune des règles réseau des applications une priorité d'exécution spécifique.

A PROPOS DES STATUTS DE LA CONNEXION RESEAU

Le Pare-feu contrôle toutes les connexions réseau sur l'ordinateur de l'utilisateur et attribue automatiquement un état à toutes les connexions détectées.

Il existe les états suivant de la connexion réseau :

- **Réseau public**. Cet état a été développé pour les réseaux non protégés par des applications antivirus quelconques, des pare-feu, des filtres (ex : pour les réseaux des café Internet). Pour ce genre de réseau, le Pare-feu empêche l'utilisateur d'accéder aux fichiers et aux imprimantes de cet ordinateur. D'autres utilisateurs sont également incapables d'accéder aux informations via les dossiers partagés et l'accès à distance au bureau de cet ordinateur. Le Pare-feu filtre l'activité réseau de chaque application conformément aux règles réseau définies pour cette application.

  Par défaut, le Pare-feu attribue l'état *Réseau public* au réseau Internet. Vous ne pouvez pas modifier l'état du réseau Internet.
- **Réseau local**. Cet état a été développé pour les réseaux aux utilisateurs desquels vous faites suffisamment confiance pour autoriser l'accès aux fichiers et aux imprimantes de cet ordinateur (par exemple, réseau local d'entreprise ou réseau domestique).
- **Réseau de confiance**. Cet état a été développé pour un réseau sûr dont l'utilisation n'expose pas l'ordinateur au risque d'attaque ou d'accès non autorisé aux données. Le Pare-feu autorise aux réseaux avec cet état toute activité réseau dans le cadre de ce réseau.

MODIFICATION DE L'ETAT DE LA CONNEXION RESEAU

Pour modifier l'état d'une connexion réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Réseaux disponibles**.

   La fenêtre **Pare-feu** sous l'onglet **Réseaux** s'ouvre.

4. Sous l'onglet **Réseaux**, sélectionnez la connexion réseau dont vous souhaitez modifier l'état.
5. Ouvrez le menu contextuel de la connexion réseau en cliquant avec le bouton droit de la souris.
6. Dans le menu contextuel, choisissez l'option état de la connexion réseau (cf. section "A propos des statuts de la connexion réseau" à la page 94) :
   - **Réseau public**.
   - **Réseau local**.
   - **Réseau de confiance**.
7. Cliquez sur **OK** dans la fenêtre **Pare-feu**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

APPLICATION DES REGLES POUR LES PAQUETS RESEAU

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles pour les paquets réseau :

- Créer une nouvelle règle pour les paquets réseau.

  Vous pouvez une nouvelle règle pour les paquets réseau en sélectionnant un ensemble des conditions et des actions relatives aux paquets réseau et aux flux de données.

- Activer et désactiver la règle pour les paquets réseau.

  Toutes les règles pour les paquets réseau créés par défaut par le Pare-feu possèdent l'état *Activé*. Si la règle pour les paquets réseau est activée, le Pare-feu applique cette règle.

  Vous pouvez activer toute règle pour les paquets réseau, sélectionnée dans la liste des règles pour les paquets réseau. Si la règle pour les paquets réseau est désactivée, le Pare-feu suspend temporairement l'application de la règle.

  La nouvelle règle pour les paquets réseau créée par l'utilisateur est par défaut ajoutée à la liste des règles pour les paquets réseau avec l'état *Activé*.

- Modifier les paramètres de la règle pour les paquets réseau.

  Après avoir créé une nouvelle règle pour les paquets réseau, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle pour les paquets réseau.

  Dans la liste des règles pour les paquets réseau, vous pouvez modifier l'action que le Pare-feu exécute en cas de découverte d'une activité réseau de la règle pour les paquets réseau indiquée.

- Modifier la priorité de la règle pour les paquets réseau.

  Vous pouvez augmenter ou diminuer la priorité de la règle pour les paquets réseau sélectionnée dans la liste.

- Supprimer la règle pour les paquets réseau.

  Vous pouvez supprimer la règle pour les paquets réseau si vous ne souhaitez pas que le Pare-feu applique cette règle en cas de découverte d'une activité réseau et qu'elle soit affichée dans la liste des règles pour les paquets réseau avec le statut *Désactivé*.

DANS CETTE SECTION

CREATION ET MODIFICATION D'UNE REGLE POUR LES PAQUETS RESEAU

Au moment de créer des règles pour les paquets réseau, il ne faut pas oublier qu'elles ont priorité sur les règles réseau des applications.

Pour créer ou modifier une règle pour les paquets réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

   Cet onglet contient la liste des règles pour les paquets réseau que le Pare-feu a définies par défaut.
4. Exécutez une des actions suivantes :
   - Si vous voulez créer une nouvelle règle pour les paquets réseau, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle pour les paquets réseau, sélectionnez-la dans la liste des règles pour les paquets réseau et cliquez sur le bouton **Modifier**.
5. La fenêtre **Règle réseau** s'ouvre.
6. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**.
   - **Interdire**.
   - **Selon les règles de l'application**.
7. Indiquez dans le champ **Nom** le nom du service de réseau d'une des manières suivantes :
   - Cliquez sur l'icône  qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service de réseau.

     Kaspersky Endpoint Security contient des services de réseau qui décrivent les connexions réseau les plus souvent utilisées.
   - Dans le champ **Noms**, saisissez manuellement le nom du service de réseau.

     Service de réseau est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle.

8. Indiquez le protocole de transfert des données :

   a. Cochez la case **Protocole**.

   b. Sélectionnez dans la liste déroulante le type de protocole dont il faut contrôler l'activité réseau.

      Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

      La case **Protocole** est désélectionnée par défaut.

      Si le service de réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service de réseau sélectionné.

9. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

   Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

   - **Entrant**.
   - **Entrant (flux)**.
   - **Entrant/Sortant**.
   - **Sortant**.
   - **Sortant (flux)**.

10. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type CMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code CMP** et sélectionnez dans la liste déroulante le code ICMP.

11. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de l'ordinateur de l'utilisateur et de l'ordinateur distant pour contrôler la connexion entre eux :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de l'ordinateur de l'utilisateur.

12. Au besoin, indiquez l'adresse de réseau dans le champ **Adresse**.

    En guise d'adresse de réseau, vous pouvez utiliser l'adresse IP ou indiquer l'état de la connexion réseau. Dans le dernier cas, les adresses de réseau proviennent de toutes les connexions réseau actives avec l'état sélectionné.

    Vous pouvez sélectionner une des catégories d'adresses réseau suivantes :

    - **Adresse quelconque**.
    - **Adresse de sous-réseau**.
    - **Adresse de la liste**.

13. Cochez la case **Consigner dans le rapport**, si vous souhaitez que l'action d'autorisation ou d'interdiction de la règle réseau soit consignée dans le rapport (cf. section "Utilisation des rapports" à la page 208).

14. Cliquez sur **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau, elle apparaît sous l'onglet **Règles pour les paquets réseau** de la fenêtre **Pare-feu**. Par défaut, la nouvelle règle réseau est placée en fin de liste.

15. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

ACTIVATION ET DESACTIVATION DE LA REGLE POUR LES PAQUETS RESEAU

Pour activer ou désactiver la règle pour les paquets réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle requise pour les paquets réseau.

5. Exécutez une des actions suivantes :

   - Cochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle pour les paquets réseau si vous souhaitez désactiver la règle.

6. Cliquez sur le bouton **OK**.

   La fenêtre **Pare-feu** se ferme.

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

MODIFICATION DE L'ACTION DU PARE-FEU POUR LA REGLE POUR LES PAQUETS RESEAU

Pour modifier l'action du Pare-feu pour la règle pour les paquets réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle pour les paquets réseau dont vous souhaitez modifier l'action.

5. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Selon la règle de l'application**.
   - **Consigner dans le rapport**.

6. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

   La fenêtre **Pare-feu** se ferme.

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

MODIFICATION DE LA PRIORITE DE LA REGLE POUR LES PAQUETS RESEAU

La priorité d'exécution de la règle pour les paquets réseau est définie par l'emplacement de la règle dans la liste des règles pour les paquets réseau. La première règle pour les paquets réseau dans la liste des règles pour les paquets réseau possède la priorité la plus élevée.

Chaque règle pour les paquets réseau que vous avez créée est ajoutée à la fin de la liste des règles pour les paquets réseau et possède la priorité la plus faible.

Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles pour les paquets réseau haut/bas. Suivant chacune des règles pour les paquets réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Pour modifier la priorité de la règle pour les paquets réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.

4. Sélectionnez dans la liste des règles pour les paquets réseau la règle pour les paquets réseau dont vous souhaitez modifier la priorité.
5. A l'aide des boutons **Haut** et **Bas**, déplacez la règle pour les paquets réseau vers la position requise dans la liste des règles pour les paquets réseau.
6. Cliquez sur le bouton **OK**.
7. La fenêtre **Pare-feu** se ferme.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

APPLICATION DES REGLES RESEAU DU GROUPE D'APPLICATIONS

Kaspersky Endpoint Security regroupe par défaut toutes les applications installées selon le nom de l'éditeur de l'application dont il contrôle l'activité de réseau ou de fichiers. Les groupes d'applications sont à leur tour regroupés en groupes de confiance. Toutes les applications et tous les groupes d'applications héritent des propriétés de leur groupe parent : règles du contrôle des applications, règles réseau de l'application, ainsi que la priorité de leur exécution.

Kaspersky Endpoint Security répartit toutes les applications lancées sur l'ordinateur en groupes de confiance. Les applications sont réparties en groupes de confiance selon le niveau de danger que ces applications peuvent représenter pour le système d'exploitation.

Les zones de confiances suivantes sont :

- **De confiance**. Ce groupe reprend les applications qui satisfont à une ou plusieurs des conditions suivantes :
  - Les applications sont dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network contient des enregistrements relatifs à ces applications.
  - L'utilisateur a placé les applications dans le groupe "De confiance".

  Il n'existe aucune opération interdite pour ces applications.
- **Restrictions faibles**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
  - L'indice de danger de ces applications est inférieur à 50.
  - L'utilisateur a placé les applications dans le groupe "Restrictions faibles".

  Il existe des restrictions minimes sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.
- **Restrictions élevées**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
  - L'indice de danger ces applications est compris entre 51 et 71.
  - L'utilisateur a placé les applications dans le groupe "Restrictions élevées".

  Il existe des restrictions considérables sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.
- **Douteuses**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.

- L'indice de danger ces applications est compris entre 71 et 100.
- L'utilisateur a placé les applications dans le groupe "Douteuses".

Il existe des restrictions considérables sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.

A l'instar du module Contrôle de l'activité des applications, le module Pare-feu applique par défaut les règles réseau du groupe d'applications afin de filtrer l'activité réseau de toutes les applications appartenant à ce groupe (cf. page 135). Les règles réseau du groupe d'applications définissent les droits d'accès aux différentes connexions réseau attribués aux applications qui font partie du groupe.

Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Endpoint Security a identifié sur l'ordinateur. Vous avez deux options pour modifier l'action du Pare-feu pour les règles réseau du groupe d'applications créées par défaut. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau du groupe d'applications créées par défaut, ni modifier leur priorité.

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles réseau du groupe d'applications :

- Créer une nouvelle règle réseau du groupe d'applications.

  Vous pouvez créer une règle réseau du groupe d'applications selon laquelle le Pare-feu va régir l'activité réseau des applications qui font partie du groupe sélectionné.

- Activer et désactiver la règle réseau du groupe d'applications.

  Toutes les règles réseau du groupe d'application sont ajoutées à la liste des règles réseau du groupe d'applications avec l'état *Activé*. Si la règle réseau du groupe d'applications est activée, le Pare-feu applique cette règle.

  Vous pouvez activer la règle réseau du groupe d'applications que vous avez créée manuellement. Si la règle réseau du groupe d'application est désactivée, le Pare-feu suspend temporairement l'application de la règle.

- Modifier les paramètres de la règle réseau du groupe d'applications.

  Après avoir créé une nouvelle règle réseau du groupe d'applications, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle réseau du groupe d'applications.

  Dans la liste des règles réseau du groupe d'applications, vous pouvez modifier l'action pour la règle réseau du groupe d'applications que le Pare-feu exécute lors de la détection de l'activité réseau de ce groupe d'applications.

- Modifier la priorité de la règle réseau du groupe d'applications.

  Vous pouvez augmenter ou diminuer la priorité de la règle réseau du groupe d'applications que vous avez créée manuellement.

- Supprimer la règle réseau du groupe d'applications.

  Vous pouvez supprimer la règle réseau du groupe d'applications que vous avez créée manuellement si vous ne souhaitez pas que le Pare-feu applique cette règle réseau au groupe sélectionné d'applications lors de la détection de l'activité réseau et qu'elle soit affichée sur la liste des règles réseau du groupe d'applications.

DANS CETTE SECTION

CREATION ET MODIFICATION D'UNE REGLE RESEAU DU GROUPE DES APPLICATIONS

Pour activer ou désactiver la règle réseau du groupe d'applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications pour lequel vous souhaitez créer ou modifier une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles du contrôle du groupe d'applications** s'ouvre.
6. Dans la fenêtre **Règles du contrôle du groupe d'application** qui s'ouvre, sélectionnez l'onglet **Règles réseau**.
7. Exécutez une des actions suivantes :
   - Si vous voulez créer une nouvelle règle réseau du groupe des applications, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle réseau du groupe des applications, sélectionnez-la dans la liste des règles réseau et cliquez sur le bouton **Modifier**.
8. La fenêtre **Règle réseau** s'ouvre.
9. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**.
   - **Interdire**.
10. Indiquez dans le champ **Nom** le nom du service de réseau d'une des manières suivantes :
    - Cliquez sur l'icône  qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service de réseau.

      Kaspersky Endpoint Security contient des services de réseau qui décrivent les connexions réseau les plus souvent utilisées.
    - Dans le champ **Noms**, saisissez manuellement le nom du service de réseau.

    Service de réseau est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle réseau.
11. Indiquez le protocole de transfert des données :
    a. Cochez la case **Protocole**.
    b. Sélectionnez dans la liste déroulante le type de protocole à utiliser pour le contrôle de l'activité réseau.

       Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

       La case **Protocole** est désélectionnée par défaut.

Si le service de réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service de réseau sélectionné.

12. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

    Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

    - **Entrant**.
    - **Entrant (flux)**.
    - **Entrant/Sortant**.
    - **Sortant**.
    - **Sortant (flux)**.

13. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type CMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code CMP** et sélectionnez dans la liste déroulante le code ICMP.

14. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de l'ordinateur de l'utilisateur et de l'ordinateur distant dont l'interconnexion doit être contrôlée :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de l'ordinateur de l'utilisateur.

15. Au besoin, indiquez l'adresse de réseau dans le champ **Adresse**.

    En guise d'adresse de réseau, vous pouvez utiliser l'adresse IP ou indiquer l'état de la connexion réseau. Dans le dernier cas, les adresses de réseau proviennent de toutes les connexions réseau actives avec l'état sélectionné.

    Vous pouvez sélectionner une des catégories d'adresses réseau suivantes :

    - **Adresse quelconque**.
    - **Adresse de sous-réseau**.
    - **Adresse de la liste**.

16. Cochez la case **Consigner dans le rapport**, si vous souhaitez que l'action d'autorisation ou d'interdiction de la règle réseau soit consignée dans le rapport (cf. section "Utilisation des rapports" à la page 208).

17. Cliquez sur **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau pour un groupe d'applications, elle apparaît sous l'onglet **Règles réseau** de la fenêtre **Règles de contrôle du groupe d'applications**.

18. Cliquez sur **OK** dans la fenêtre **Règles du contrôle du groupe d'applications**.

19. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

ACTIVATION ET DESACTIVATION DE LA REGLE RESEAU DU GROUPE D'APPLICATIONS

Pour activer ou désactiver la règle réseau du groupe d'applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications requis.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles du contrôle du groupe d'applications** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau du groupe d'applications la règle réseau du groupe d'applications requise.
8. Exécutez une des actions suivantes :

   - Cochez la case à côté du nom de la règle réseau du groupe d'applications si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle réseau du groupe d'applications si vous souhaitez désactiver la règle.

   Vous ne pouvez pas désactiver la règle réseau du groupe d'applications si elle a été créée par le Pare-feu par défaut.
9. Cliquez sur **OK** dans la fenêtre **Règles du contrôle du groupe d'applications**.
10. Cliquez sur **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFIER LES ACTIONS DU PARE-FEU POUR LA REGLE RESEAU DU GROUPE D'APPLICATIONS

Vous pouvez modifier l'action du Pare-feu pour les règles réseau de tout le groupe des applications qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle spécifique du groupe d'applications qui a été créée manuellement.

Pour modifier l'action du Pare-feu pour les règles réseau de tout le groupe des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau du groupe créées par défaut. Les règles réseau du groupe des applications, créées manuellement, resteront sans modification.
5. Dans la colonne **Réseau**, cliquez avec le bouton gauche de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :
   - **Hériter**.
   - **Autoriser**.
   - **Interdire**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Pour modifier l'action du Pare-feu pour une règle réseau du groupe des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications le groupe d'applications requis.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles du contrôle du groupe d'applications** s'ouvre.
6. Dans la fenêtre **Règles du contrôle du groupe d'application** qui s'ouvre, sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau du groupe d'applications, sélectionnez la règle réseau du groupe d'applications pour lequel vous souhaitez modifier l'action du Pare-feu.

8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Consigner dans le rapport**.

9. Cliquez sur **OK** dans la fenêtre **Règles du contrôle du groupe d'applications**.

10. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

MODIFICATION DE LA PRIORITE DE LA REGLE RESEAU DU GROUPE D'APPLICATIONS

La priorité d'exécution de la règle réseau pour le groupe d'applications est définie par l'emplacement de la règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Suivant chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau du groupe d'application créées manuellement ont une priorité plus élevée que les règles réseau du groupe d'application créées par défaut.

Vous ne pouvez pas modifier la priorité des règles réseau pour le groupe d'applications créées par défaut. Afin de modifier la priorité d'une règle réseau du groupe d'applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.

4. Sélectionnez dans la liste des applications le groupe d'applications requis.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel, puis sélectionnez l'option **Règles pour le groupe**.

   La fenêtre **Règles du contrôle du groupe d'applications** s'ouvre.

6. Dans la fenêtre **Règles du contrôle du groupe d'application** qui s'ouvre, sélectionnez l'onglet **Règles réseau**.

7. Sélectionnez dans la liste des règles réseau du groupe d'applications, sélectionnez la règle réseau du groupe d'applications pour lequel vous souhaitez modifier la priorité.

8. A l'aide des boutons **Haut** et **Bas**, déplacez la règle réseau du groupe d'applications vers la position requise dans la liste des règles réseau du groupe d'applications.

9. Cliquez sur **OK** dans la fenêtre **Règles du contrôle du groupe d'applications**.

10. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

APPLICATION DES REGLES RESEAU DE L'APPLICATION

Conformément aux règles réseau de l'application, le Pare-feu réglementer l'accès de l'application aux différentes connexions réseau.

Par défaut, le Pare-feu crée un ensemble de règles réseau pour chaque groupe d'applications que Kaspersky Endpoint Security a identifié sur l'ordinateur. Les applications qui appartiennent à ce groupe héritent de ces règles réseau. Vous pouvez modifier les actions du Pare-feu pour les règles réseau des applications héritées. Vous ne pouvez pas modifier, supprimer ou désactiver les règles réseau des applications héritées du groupe parent, ni modifier leur priorité.

Vous pouvez exécuter les opérations suivantes pendant l'utilisation des règles réseau de l'application :

- Créer une nouvelle règle réseau de l'application.

  Vous pouvez créer une nouvelle règle réseau de l'application que le Pare-feu utilise pour réglementer l'activité réseau de cette application.

- Activer et désactiver la règle réseau de l'application.

  Toutes les règles réseau de l'application sont ajoutées à la liste des règles réseau de l'application avec l'état *Activé*. Si la règle de l'application est activée, le Pare-feu applique cette règle.

  Vous pouvez désactiver toute règle réseau de l'application que vous avez créée manuellement. Si la règle de l'application est désactivée, le Pare-feu suspend temporairement l'application de la règle.

- Modifier les paramètres de la règle réseau de l'application.

  Après avoir créé une nouvelle règle de l'application, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Modifier l'action du Pare-feu pour la règle réseau de l'application.

  Dans la liste des règles de l'application, vous pouvez modifier l'action pour la règle réseau de l'application que le Pare-feu exécute lors de la détection de l'activité réseau de cette application.

- Modifier la priorité de la règle réseau de l'application.

  Vous pouvez augmenter ou diminuer la priorité de la règle réseau de l'application que vous avez créée manuellement.

- Supprimer la règle réseau de l'application.

  Vous pouvez supprimer la règle réseau de l'application que vous avez créée manuellement si vous ne souhaitez pas que le Pare-feu applique cette règle réseau à l'application sélectionnée lors de la détection de l'activité réseau et qu'elle soit affichée sur la liste des règles réseau de l'application.

DANS CETTE SECTION

CREATION ET MODIFICATION D'UNE REGLE RESEAU DE L'APPLICATION

Pour créer ou modifier une règle réseau de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications l'application pour laquelle vous souhaitez créer une règle réseau.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles de l'application**.

   La fenêtre **Règles du contrôle de l'application** s'ouvre.
6. Dans la fenêtre **Règles du contrôle de l'application qui s'ouvre**, sélectionnez l'onglet **Règles réseau**.
7. Exécutez une des actions suivantes :
   - Si vous voulez créer une nouvelle règle réseau de l'application, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier la règle réseau de l'application, sélectionnez-la dans la liste des règles réseau de l'application et cliquez sur le bouton **Modifier**.
8. La fenêtre **Règle réseau** s'ouvre.
9. Sélectionnez, dans la liste déroulante **Action**, l'action qui sera exécutée par le Pare-feu après avoir détecté ce type d'activité réseau :
   - **Autoriser**.
   - **Interdire**.
10. Indiquez dans le champ **Nom** le nom du service de réseau d'une des manières suivantes :
    - Cliquez sur l'icône  qui se trouve à droite du champ **Nom** et sélectionnez dans la liste déroulante le nom du service de réseau.

      Kaspersky Endpoint Security contient des services de réseau qui décrivent les connexions réseau les plus souvent utilisées.
    - Dans le champ **Noms**, saisissez manuellement le nom du service de réseau.

    Service de réseau est un ensemble de paramètres qui caractérise l'activité réseau pour laquelle vous définissez la règle.
11. Indiquez le protocole de transfert des données :
    a. Cochez la case **Protocole**.
    b. Sélectionnez dans la liste déroulante le type de protocole à utiliser pour le contrôle de l'activité réseau.

       Le pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE.

La case **Protocole** est désélectionnée par défaut.

Si le service de réseau est sélectionné dans la liste déroulante **Nom**, la case **Protocole** est cochée automatiquement et la liste déroulante à côté de la case est remplie avec le type de protocole qui correspond au service de réseau sélectionné.

12. Sélectionnez dans la liste déroulante **Direction** la direction de l'activité réseau contrôlée.

    Le Pare-feu contrôle les connexions réseau avec des directions suivantes :

    - **Entrant**.
    - **Entrant (flux)**.
    - **Entrant/Sortant**.
    - **Sortant**.
    - **Sortant (flux)**.

13. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP :

    a. Cochez la case **Type CMP** et sélectionnez dans la liste déroulante le type du paquet ICMP.

    b. Cochez la case **Code CMP** et sélectionnez dans la liste déroulante le code ICMP.

14. Si vous avez sélectionné le protocole TCP ou UDP, vous pouvez définir les ports de l'ordinateur de l'utilisateur et de l'ordinateur distant pour contrôler la connexion entre eux :

    a. Saisissez dans le champ **Ports distants** les ports de l'ordinateur distant.

    b. Saisissez dans le champ **Ports locaux** les ports de l'ordinateur de l'utilisateur.

15. Au besoin, indiquez l'adresse de réseau dans le champ **Adresse**.

    En guise d'adresse de réseau, vous pouvez utiliser l'adresse IP ou indiquer l'état de la connexion réseau. Dans le dernier cas, les adresses de réseau proviennent de toutes les connexions réseau actives avec l'état sélectionné.

    Vous pouvez sélectionner une des catégories d'adresses réseau suivantes :

    - **Adresse quelconque**.
    - **Adresse de sous-réseau**.
    - **Adresse de la liste**.

16. Cochez la case **Consigner dans le rapport**, si vous souhaitez que l'action d'autorisation ou d'interdiction de la règle réseau soit consignée dans le rapport (cf. section "Utilisation des rapports" à la page 208).

17. Cliquez sur **OK** dans la fenêtre **Règle réseau**.

    Si vous avez créé une règle réseau pour une application, elle apparaît sous l'onglet **Règles réseau** de la fenêtre **Règles pour l'application**.

18. Cliquez sur **OK** dans la fenêtre **Règles du contrôle de l'application**.

19. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

ACTIVATION ET DESACTIVATION DE LA REGLE RESEAU DE L'APPLICATION

Pour activer ou désactiver la règle réseau de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez l'application requise dans la liste des applications.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles de l'application**.

   La fenêtre **Règles du contrôle de l'application** s'ouvre.
6. Sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau de l'application la règle réseau de l'application requise.
8. Exécutez une des actions suivantes :
   - Cochez la case à côté du nom de la règle réseau de l'application si vous souhaitez activer la règle.
   - Décochez la case à côté du nom de la règle réseau de l'application si vous souhaitez désactiver la règle.

   Vous ne pouvez pas désactiver la règle réseau de l'application si elle a été créée par le Pare-feu par défaut.
9. Cliquez sur **OK** dans la fenêtre **Règles du contrôle de l'application**.
10. Cliquez sur **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DE L'ACTION DU PARE-FEU POUR LA REGLE RESEAU DE L'APPLICATION

Vous pouvez modifier l'action du Pare-feu pour toutes les règles réseau de l'application qui ont été créées par défaut, ainsi que modifier l'action du Pare-feu pour une règle spécifique de l'application qui a été créée manuellement.

Pour modifier l'action du Pare-feu pour toutes les règles réseau de l'application d'une application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez dans la liste des applications l'application si vous souhaitez modifier l'action du Pare-feu pour toutes les règles réseau de l'application créées par défaut.

   Les règles réseau de l'application définies manuellement, resteront inchangées.

5. Dans la colonne **Réseau**, cliquez avec le bouton gauche de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Hériter**.
   - **Autoriser**.
   - **Interdire**.

6. Cliquez sur **OK** dans la fenêtre **Pare-feu**.

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

Pour modifier l'action du Pare-feu pour une règle réseau de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres des modules Pare-feu et Prévention des intrusions s'afficheront la partie droite de la fenêtre.

3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.

4. Sélectionnez l'application requise dans la liste des applications.

5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles de l'application**.

   La fenêtre **Règles du contrôle de l'application** s'ouvre.

6. Dans la fenêtre **Règles du contrôle de l'application qui s'ouvre**, sélectionnez l'onglet **Règles réseau**.

7. Sélectionnez dans la liste des règles réseau de l'application, sélectionnez la règle réseau de l'application pour lequel vous souhaitez modifier l'action du Pare-feu.

8. Dans la colonne **Autorisation**, cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et sélectionnez l'action que vous voulez définir :

   - **Autoriser**.
   - **Interdire**.
   - **Consigner dans le rapport**.

9. Cliquez sur le bouton **OK**.

10. Dans la fenêtre **Pare-feu**, cliquez sur **OK**.

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

MODIFICATION DE LA PRIORITE DE LA REGLE RESEAU DE L'APPLICATION

La priorité d'exécution de la règle réseau de l'application est définie par l'emplacement de la règle dans la liste des règles réseau. Le Pare-feu applique les règles selon leur ordre d'apparition dans la liste des règles réseau, de haut en bas. Selon chacune des règles réseau traitées appliquées à une connexion réseau spécifique, le Pare-feu autorise ou bloque l'accès réseau à l'adresse et au port indiqués dans les paramètres de cette connexion réseau.

Les règles réseau de l'application que vous avez créées manuellement ont une priorité plus élevée que les règles réseau héritées du groupe parent d'applications.

Vous ne pouvez pas modifier la priorité des règles réseau héritées pour une application. Les règles réseau pour une application (héritées ou créées manuellement) ont priorité sur les règles réseau pour un groupe d'applications. Autrement dit, toutes les applications du groupe héritent automatiquement des règles réseau de ce groupe, mais si une règle pour une application en particulier est modifiée ou créée, elle est appliquée avant toutes les autres règles héritées.

Pour modifier la priorité de la règle réseau de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles réseau des applications**.

   La fenêtre **Pare-feu** sous l'onglet **Règles du contrôle des applications** s'ouvre.
4. Sélectionnez l'application requise dans la liste des applications.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel du fichier, puis sélectionnez l'option **Règles de l'application**.

   La fenêtre **Règles du contrôle de l'application** s'ouvre.
6. Dans la fenêtre **Règles du contrôle de l'application qui s'ouvre**, sélectionnez l'onglet **Règles réseau**.
7. Sélectionnez dans la liste des règles réseau de l'application la règle de l'application dont vous souhaitez modifier la priorité.
8. A l'aide des boutons **Haut** et **Bas**, déplacez la règle réseau de l'application vers la position requise dans la liste des règles réseau de l'application.
9. Cliquez sur **OK** dans la fenêtre **Règles du contrôle de l'application**.
10. Cliquez sur **OK** dans la fenêtre **Pare-feu**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES DU PARE-FEU

Vous pouvez configurer les paramètres de fonctionnement avancés du Pare-feu.

Afin de configurer les paramètres de fonctionnement avancés du Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Pare-feu**.

   Les paramètres du module Pare-feu s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Règles pour les paquets réseau**.

   La fenêtre **Pare-feu** sous l'onglet **Règles pour les paquets réseau** s'ouvre.
4. Cliquez sur le bouton **Avancé**.

   La fenêtre **Avancé** s'ouvre.
5. Dans la fenêtre **Avancé** qui s'ouvre, exécutez une des actions suivantes :
   - Cochez la case située à côté du nom du paramètre avancé pour activer le paramètre.
   - Décochez la case située à côté du nom du paramètre avancé pour désactiver le paramètre.

     Les paramètres avancés du Pare-feu sont :
     - **Autoriser le mode FTP actif**.
     - **Bloquer les connexions s'il est impossible d'afficher une invite pour l'action (interface de l'application non chargée)**.
     - **Ne pas désactiver le Pare-feu avant l'arrêt complet du système**.

     Par défaut, les paramètres avancés du Pare-feu sont activés.
6. Cliquez sur **OK** dans la fenêtre **Avancé**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

PREVENTION DES INTRUSIONS

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

DANS CETTE SECTION

A PROPOS DE LA PROTECTION CONTRE LES ATTAQUES RESEAU

Le module Prévention des intrusions recherche dans le trafic entrant toute trace d'activité réseau caractéristique des attaques réseau. En cas de détection d'une tentative d'attaque réseau contre l'ordinateur de l'utilisateur, Kaspersky Endpoint Security bloque l'activité réseau de l'ordinateur attaquant. Un message vous avertit après qu'une tentative d'attaque réseau a été effectuée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

L'activité réseau de l'ordinateur à l'origine de l'attaque est bloquée pendant une heure. Vous pouvez modifier les paramètres du blocage de l'ordinateur attaquant (cf. section "Modification des paramètres de blocage de l'ordinateur attaquant" à la page 115).

Les descriptions des types d'attaques réseau connues à l'heure actuelle et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Endpoint Security. La liste des attaques réseau que le module Prévention des intrusions détecte est enrichie lors de la mise à jour des bases et des modules de l'application (cf. section "A propos de la mise à jour des bases et des modules de l'application" à la page 171).

ACTIVATION ET DESACTIVATION DE LA PREVENTION DES INTRUSIONS

Par défaut, la Prévention des intrusions est activée et fonctionne en mode optimal. Le cas échéant, vous pouvez désactiver la Prévention des intrusions.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver le module Détection des intrusions sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel des actions du module Détection des intrusions sur la ligne **Détection des intrusions**.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu contextuel l'option **Activer** pour activer le module Protection contre les attaques réseau.

     L'icône de l'état du fonctionnement du module  qui s'affiche à gauche dans la ligne **Détection des intrusions** sera remplacée par l'icône  .
   - Choisissez dans le menu contextuel l'option **Désactiver** pour désactiver le module Détection des intrusions.

     L'icône de l'état du fonctionnement du module  qui s'affiche à gauche dans la ligne **Détection des intrusions** sera remplacée par l'icône  .

Pour activer ou désactiver la Prévention des intrusions depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection antivirus** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Protection contre les attaques réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Prévention des intrusions.
3. Réalisez les opérations suivantes :
   - Cochez la case **Activer la Prévention des intrusions** pour activer la Prévention des intrusions.
   - Décochez la case **Activer la Prévention des intrusions** pour désactiver la Prévention des intrusions.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DES PARAMETRES DE BLOCAGE DE L'ORDINATEUR ATTAQUANT

Pour modifier les paramètres du blocage de l'ordinateur attaquant, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection contre les attaques réseau**.

   La partie droite de la fenêtre affiche les paramètres du module Prévention des intrusions.
3. Dans le groupe **Prévention des intrusions**, cochez la case **Ajouter l'ordinateur attaquant à la liste des ordinateurs bloqués pendant**.

   Si cette case est cochée, en cas de détection d'une tentative d'attaque réseau la Prévention des intrusions bloque l'activité réseau de l'ordinateur attaquant pendant la durée définie pour protéger automatiquement l'ordinateur contre les futures attaques réseau possibles depuis cette adresse.

   Si cette case est décochée, en cas de détection d'une tentative d'attaque réseau, la Prévention des intrusions n'active pas la protection automatique contre les futures attaques réseau possibles depuis cette adresse.
4. Pour modifier la durée du blocage de l'ordinateur attaquant, dans le champ qui se trouve à droite de la case **Ajouter l'ordinateur attaquant à la liste des ordinateurs bloqués pendant**.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONTROLE DU TRAFIC RESEAU

Cette section contient des informations sur le contrôle du trafic réseau et les instructions sur la configuration des paramètres des ports réseau contrôlés.

DANS CETTE SECTION

A PROPOS DU CONTROLE DU TRAFIC RESEAU

Lors du fonctionnement de Kaspersky Endpoint Security, les modules Antivirus courrier (cf. section "Protection du courrier. Antivirus Courrier" à la page 71), Antivirus Internet (cf. section "Protection de l'ordinateur sur l'Internet. Antivirus Internet" à la page 81) et Antivirus IM (cf. section "Protection du trafic des clients de messageries instantanées. Antivirus IM" à la page 88) contrôlent les flux de données transmis via des protocoles déterminés sur les ports TCP et UDP définis et ouverts de l'ordinateur de l'utilisateur. Ainsi par exemple, Antivirus Courrier analyse les informations transmises via le protocole SMTP et Antivirus Internet, les informations transmises via les protocoles HTTP, HTTPS et FTP.

Kaspersky Endpoint Security répartit les ports TCP et UDP du système d'exploitation en plusieurs groupes en fonction de la probabilité d'une attaque réussie contre ceux-ci. Les ports réseaux associés à des services vulnérables doivent être soumis à un contrôle plus strict car ceux-ci courent un risque plus élevé d'être pris pour cible par une attaque réseau. Si vous utilisez des services non standards quelconques affectés à des ports réseau inhabituels, sachez que ces ports peuvent être eux-aussi soumis à une attaque. Vous pouvez créer une liste de ports réseau et une liste d'applications qui sollicitent un accès au réseau et qui doivent faire l'objet d'une attention particulière des modules Antivirus Courrier, Antivirus Internet et Antivirus IM dans le cadre de la surveillance du trafic de réseau.

CONFIGURATION DES PARAMETRES DU CONTROLE DU TRAFIC RESEAU

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres du contrôle du trafic réseau :

- Activer le contrôle de tous les ports réseau.
- Composer la liste des ports réseau contrôlés.
- Composer la liste des applications dont tous les ports réseau sont contrôlés.

DANS CETTE SECTION

ACTIVATION DU CONTROLE DE TOUS LES PORTS RESEAU

Pour activer le contrôle de tous les ports réseau, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler tous les ports réseau**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONSTITUTION DE LA LISTE DES PORTS DE RESEAU CONTROLES

Pour créer la liste des ports réseau contrôlés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**.
4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre. La fenêtre **Ports réseau** contient la liste des ports réseau utilisés habituellement pour le transfert du courrier électronique et du trafic de réseau. Cette liste est livrée avec Kaspersky Endpoint Security.
5. Dans la liste des ports réseau, procédez comme suit :

   - Cochez les cases en regard des ports réseau que vous souhaitez ajouter à la liste des ports réseau contrôlés.

     Par défaut, les cases sont cochées pour tous les ports réseau présentés dans la fenêtre **Ports réseau**.
   - Décochez les cases en regard des ports réseau que vous souhaitez exclure de la liste des ports réseau contrôlés.
6. Si le port réseau contrôlé ne figure pas sur la liste des ports réseau, ajoutez-la de la manière suivante :

   a. Le lien **Ajouter** sous la liste des ports réseau permet d'ouvrir la fenêtre **Port réseau**.

   b. Saisissez le numéro du port réseau dans le champ **Port**.

   c. Dans le champ **Description**, saisissez le nom du port réseau.

   d. Cliquez sur le bouton **OK**.

      La fenêtre **Port réseau** se ferme. Le port réseau que vous ajoutez apparaît en fin de liste.
7. Cliquez sur **OK** dans la fenêtre **Port réseau**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONSTITUTION DE LA LISTE DES APPLICATIONS DONT TOUS LES PORTS RESEAU SONT CONTROLES

Vous pouvez composer une liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security.

Il est conseillé d'ajouter à cette liste des applications dont tous les ports réseau seront contrôlés par Kaspersky Endpoint Security les applications qui reçoivent ou envoient les données via le protocole FTP.

Pour composer la liste des applications dont tous les ports réseau seront contrôlés, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Ports contrôlés**, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**.
4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Ports réseau** s'ouvre.
5. Cochez la case **Contrôler tous les ports pour les applications sélectionnées**.

   La case est cochée par défaut.
6. Dans la liste des applications situé sous la case **Contrôler tous les ports pour les applications indiquées**, procédez comme suit :
   - Cochez les cases en regard des noms des applications dont tous les ports réseau vous souhaitez contrôler.

     Par défaut, les cases sont cochées pour toutes les applications présentées dans la fenêtre **Ports réseau**.
   - Décochez les cases en regard des noms des applications dont tous les ports réseau vous ne souhaitez pas contrôler.
7. Si l'application ne figure pas dans la liste des applications, ajoutez-la d'une des manières suivantes :
   a. A l'aide du lien **Ajouter** situé sous la liste des applications ouvrez le menu contextuel.
   b. Sélectionnez dans le menu contextuel le mode d'ajout d'une application à la liste des applications :
      - Sélectionnez l'option **Applications** pour sélectionner l'application de la liste des applications installées sur l'ordinateur. La fenêtre **Sélection de l'application** s'ouvrira, à l'aide de laquelle vous pourrez indiquer le nom de l'application.
      - Sélectionnez l'option **Parcourir** pour désigner l'emplacement du fichier exécutable de l'application. La fenêtre standard Microsoft Windows **Ouvrir** s'ouvrira, à l'aide de laquelle vous pourrez indiquer le nom du fichier exécutable de l'application.

   c. Après avoir sélectionné l'application, la fenêtre **Application** s'ouvrira.
   d. Saisissez dans le champ **Nom** le nom pour l'application sélectionnée.
   e. Cliquez sur le bouton **OK**.

      La fenêtre **Application** se ferme. L'application que vous avez ajoutée apparaît dans la liste des applications.
8. Cliquez sur **OK** dans la fenêtre **Port réseau**.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

SURVEILLANCE DU RESEAU

Cette section contient des informations sur la surveillance du réseau et explique comment lancer la surveillance de réseau.

DANS CETTE SECTION

A PROPOS DE LA SURVEILLANCE DU RESEAU

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité réseau de l'ordinateur d'utilisateur en temps réel.

LANCEMENT DE LA SURVEILLANCE DU RESEAU

Pour lancer la Surveillance du réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion de la protection**.

   Le groupe **Gestion de la protection** se développe.
4. Ouvrez le menu contextuel en cliquant avec le bouton droit de la souris sur la ligne **Protection de réseau** afin de sélectionner l'action du module Pare-feu.
5. Sélectionnez dans le menu contextuel l'option **Surveillance du réseau**.

   La fenêtre **Surveillance du réseau** s'ouvre. Cette fenêtre affiche les informations sur l'activité réseau de l'ordinateur de l'utilisateur sur quatre onglets :

   - L'onglet **Activité réseau** affiche toutes les connexions réseau avec l'ordinateur de l'utilisateur qui sont actuellement actives. Il affiche non seulement les connexions réseau ouvertes par l'ordinateur de l'utilisateur, mais aussi les connexions réseau entrantes.
   - L'onglet **Ports ouverts** reprend tous les ports réseau ouverts sur l'ordinateur de l'utilisateur.
   - L'onglet **Trafic de réseau** affiche le volume du trafic réseau entrant et sortant entre l'ordinateur de l'utilisateur et les autres ordinateurs du réseau auquel l'utilisateur est connecté au moment présent.
   - L'onglet **Ordinateurs bloqués** affiche la liste des adresses IP dont l'activité réseau a été bloquée par le module Détection des intrusions après une tentative d'attaque réseau effectuée depuis cette adresse IP.

CONTROLE DU LANCEMENT DES APPLICATIONS

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur le Contrôle du lancement des applications et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DU CONTROLE DU LANCEMENT DES APPLICATIONS

Le module Contrôle du lancement des applications surveille les tentatives de lancement d'applications par les utilisateurs et utilise pour ce faire les *règles de contrôle du lancement des applications*.

Le lancement des applications dont aucun paramètre ne respecte les règles de contrôle du lancement des applications est régi par la règle par défaut "Tout autoriser". La règle "Tout autoriser" permet à n'importe quel utilisateur de lancer n'importe quelle application.

Toutes les tentatives de lancement des applications par les utilisateurs sont consignées dans des rapports (cf. section "Utilisation des rapports" à la page 208).

ACTIVATION ET DESACTIVATION DU CONTROLE DU LANCEMENT DES APPLICATIONS

Le Contrôle du lancement des applications est activé par défaut. Le cas échéant, vous pouvez désactiver le Contrôle du lancement des applications.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver Contrôle du lancement des applications sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle du lancement des applications.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle du lancement des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle du lancement des applications**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle du lancement des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle du lancement des applications**, sera modifiée sur l'icône .

Pour activer ou désactiver le Contrôle du lancement des applications depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cochez la case **Activer le Contrôle du lancement des applications** pour activer le Contrôle du lancement des applications.

   - Décochez la case **Activer le Contrôle du lancement des applications** pour désactiver le Contrôle du lancement des applications.

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

A PROPOS DES REGLES DE CONTROLE DU LANCEMENT DES APPLICATIONS

La règle de contrôle du lancement des applications est un ensemble de paramètres qui déterminent les fonctions suivantes du module Contrôle du lancement des applications :

- Classification des applications à l'aide des *conditions de déclenchement de la règle* (ci-après, les "conditions"). La condition de déclenchement de la règle est une équivalence : critères de la condition – valeur de la condition – type de condition (cf. ill. ci-après).

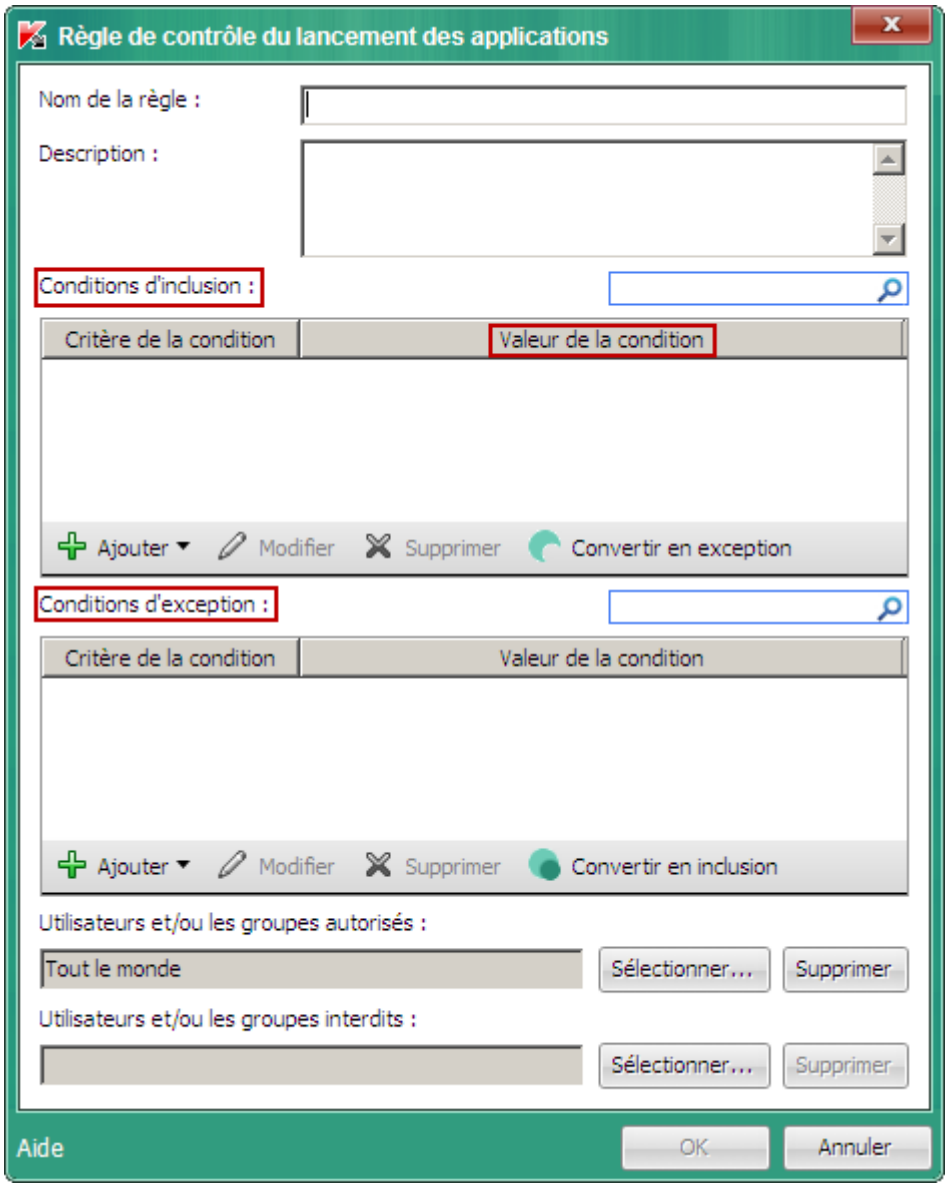


Illustration 4. Règle de contrôle du lancement des applications Paramètres de condition de déclenchement de la règle

Le critère de déclenchement de la règle peut être :

- Le chemin d'accès au dossier contenant le fichier exécutable de l'application ou le chemin d'accès au fichier exécutable de l'application.
- Les métadonnées : nom d'origine du fichier exécutable de l'application, nom du fichier exécutable de l'application sur le disque, version du fichier exécutable de l'application, nom de l'application et éditeur de l'application.

- Le code de hachage (MD5) du fichier exécutable de l'application.
- L'appartenance de l'application à une catégorie KL. La liste Catégorie KL est une liste composée par les experts de Kaspersky Lab. Elle regroupe les applications qui partagent des traits communs.

  Par exemple, la catégorie KL "Applications de bureautique" reprend les applications de la suite Microsoft Office, Adobe® Acrobat® et d'autres.

Le type de condition du déclenchement de la règle détermine le rapport de l'application à la règle :

- *Conditions d'inclusion*. L'application respecte la règle si ces paramètres répondent au moins à une condition d'inclusion de déclenchement de la règle.
- *Conditions d'exception*. L'application ne satisfait pas à la règle si ces paramètres répondent à au moins une condition d'exception de déclenchement de la règle ou ne répondent à aucune des conditions d'inclusion de déclenchement de la règle. La règle ne contrôle pas le lancement de telles applications.

- L'autorisation octroyée aux utilisateurs ou groupes d'utilisateurs sélectionnés pour lancer l'application.

  Vous pouvez sélectionner l'utilisateur et/ou le groupe d'utilisateurs autorisé à lancer l'application qui satisfait à la règle.

  Une règle qui ne désigne aucun utilisateur autorisé à lancer les applications qui satisfont à la règle est une règle *d'interdiction*.

- L'interdiction pour les utilisateurs ou groupes d'utilisateurs sélectionnés de lancer l'application.

  Vous pouvez sélectionner l'utilisateur et/ou le groupe d'utilisateurs qui n'est pas autorisé à lancer l'application qui satisfait aux règles de contrôle du lancement des applications.

  Une règle qui ne désigne aucun utilisateur non autorisé à lancer les applications qui satisfont à la règle est une règle *d'autorisation*.

Une règle d'interdiction a une priorité supérieure à une règle d'autorisation. Par exemple, si une règle d'autorisation du contrôle du lancement des applications a été définie pour un groupe d'utilisateurs et qu'un des membres de ce groupe est soumis à une règle d'interdiction du contrôle du lancement des applications, il ne sera pas autorisé à exécuter l'application.

Statut du fonctionnement de la règle de contrôle du lancement des applications

Les règles de contrôle du lancement des applications peuvent avoir un des trois statuts suivants :

- *Act.* Ce statut indique que la règle est activée.
- *Désact*. Ce statut indique que la règle est désactivée.
- *Test*. Ce statut du fonctionnement de la règle signifie que Kaspersky Endpoint Security ne limite pas l'exécution des applications conformément aux paramètres de la règle mais se contente de consigner dans les rapports (cf. section "Utilisation des rapports" à la page 208) les informations relatives à l'exécution de l'application.

  Le statut de la règle *Test* est utile pour vérifier le fonctionnement d'une nouvelle règle de contrôle du lancement des applications. L'utilisateur n'est pas limité à l'exécution des applications qui sont conformes à la règle dont l'état est *Test*. L'autorisation ou l'interdiction du lancement d'une application sont définis séparément pour les règles de test ou réelles. Par exemple, si une règle de test d'autorisation du contrôle du lancement des applications a été définie pour un utilisateur et que celui-ci est soumis à une règle réelle d'interdiction, alors

Règles de contrôle du lancement des applications par défaut

Les règles suivantes de contrôle du lancement des applications par défaut sont créées :

- **Tout autoriser**. La règle permet à tous les utilisateurs de lancer n'importe quelle application. Cette règle est la base du fonctionnement du Contrôle du lancement des applications en mode "Liste noire" (cf. section "Présentation des modes de fonctionnement du Contrôle du lancement des applications" à la page 130). La règle est activée par défaut.
- **Programmes de mise à jour des applications de confiance**. La règle autorise l'exécution des applications installées ou des mises à jour des applications de la catégorie KM "Programmes de mise à jour des applications de confiance" et pour lesquelles aucune règle d'interdiction n'a été définie. La catégorie KL "Programmes de mise à jour des applications de confiance" reprend les programmes de mise à jour des éditeurs de logiciels les plus connus. La règle est créée par défaut uniquement du côté du Plug-in d'administration de Kaspersky Endpoint Security. La règle est désactivée par défaut.

- **Système d'exploitation et ses modules**. La règle permet à tous les utilisateurs de lancer les applications de la catégorie KL "Catégorie principale". La catégorie KL "Catégorie principale" reprend les applications indispensables au lancement et au fonctionnement du système d'exploitation. L'autorisation de lancement d'une application de cette catégorie KL est requise pour le fonctionnement du Contrôle du lancement des applications en mode "Liste blanche" (cf. section "Présentation des modes de fonctionnement du Contrôle du lancement des applications" à la page 130). La règle est créée par défaut uniquement du côté du Plug-in d'administration de Kaspersky Endpoint Security. La règle est désactivée par défaut.

ACTIONS IMPLIQUANT LES REGLES DU CONTROLE DU LANCEMENT DES APPLICATIONS

Vous pouvez réaliser les opérations suivantes au niveau des règles de contrôle du lancement des applications :

- Ajouter une nouvelle règle.
- Modifier la règle.
- Modifier le statut du fonctionnement de la règle.

  La règle de contrôle du lancement des applications peut être activée (statut de fonctionnement *Act.*), désactivée (statut de fonctionnement *Désact*) ou fonctionner en mode test (statut de fonctionnement *Test*). Par défaut, les règles de contrôle du lancement des applications sont activées après la création (état *Act.)*. Vous pouvez désactiver la règle de contrôle du lancement des applications ou activer son fonctionnement en mode test.
- Supprimer la règle.

DANS CETTE SECTION

AJOUT ET MODIFICATION D'UNE REGLE DE CONTROLE DU LANCEMENT DES APPLICATIONS

Pour ajouter ou modifier une règle de contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Si vous voulez modifier une règle, cliquez sur le bouton **Modifier**.

   La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

4. Définissez ou modifiez les paramètres de la règle. Pour ce faire, procédez comme suit :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom**.

   b. Le tableau **Conditions d'inclusion** permet de composer ou de modifier la liste des conditions d'inclusion pour le déclenchement de la règle de contrôle du lancement des applications (cf. page 126). Utilisez pour ce faire les boutons **Ajouter**, **Modifier**, **Supprimer** et **Convertir en exception**.

   c. Dans le tableau **Conditions d'exception**, composez ou modifiez la liste des conditions d'exception du déclenchement de la règle de contrôle du lancement des applications. Utilisez pour ce faire les boutons **Ajouter**, **Modifier**, **Supprimer** et **Convertir l'act. en condition**.

   d. Vous pouvez modifier le type de condition de déclenchement de la règle. Pour ce faire, procédez comme suit :

      - Pour faire passer une condition du type inclusion en type exception, sélectionnez la condition dans le tableau **Conditions d'inclusion**, puis cliquez sur **Convertir en exception**.

      - Pour faire passer une condition du type exception au type inclusion, sélectionnez la condition dans le tableau **Conditions d'exception**, puis cliquez sur le bouton **Convertir en inclusion**.

   e. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés à exécuter les applications qui répondent aux conditions d'inclusion de déclenchement de la règle. Pour ce faire, dans le champ **Utilisateurs et/ou les groupes autorisés**, saisissez les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**. La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

   f. Rédigez ou modifiez la liste des utilisateurs et/ou des groupes d'utilisateurs qui ne sont pas autorisés à exécuter les applications qui répondent aux conditions d'inclusion de déclenchement de la règle. Pour ce faire, dans le champ **Utilisateurs et/ou les groupes interdits**, saisissez les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**. La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

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

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

AJOUT D'UNE CONDITION DE DECLENCHEMENT DE REGLE DE CONTROLE DU LANCEMENT DES APPLICATIONS

Pour ajouter une condition de déclenchement de la règle de contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** si vous souhaitez ajouter une condition de déclenchement d'une nouvelle règle de contrôle du lancement des applications.

   - Dans la liste **Règles de contrôle du lancement des applications**, sélectionnez la règle requise, puis cliquez sur le bouton **Ajouter** si vous souhaitez ajouter une condition de déclenchement d'une règle de contrôle du lancement des applications qui existe déjà.

La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

4. Cliquez sur le bouton **Ajouter** dans le tableau **Conditions d'inclusion** ou **Conditions d'exception** de déclenchement de la règle de contrôle du lancement des applications.

   Le menu contextuel du bouton **Ajouter** s'ouvre.

5. Réalisez les opérations suivantes :

   - Choisissez l'option **Conditions à partir des propriétés du fichier** afin de créer une condition de déclenchement de la règle de contrôle du lancement des applications sur la base des propriétés du fichier. Pour ce faire, procédez comme suit :

     a. Dans la fenêtre **Ouvrir** standard de Microsoft Windows, choisissez le fichier exécutable de l'application sur la base des propriétés duquel vous souhaitez composer la condition de déclenchement de la règle de contrôle du lancement des applications.

     b. Cliquez sur le bouton **Ouvrir**.

        La fenêtre **Condition à partir des propriétés du fichier** s'ouvre. Les valeurs des paramètres de la fenêtre **Condition à partir des propriétés du fichier** sont extraites des propriétés du fichier exécutable de l'application.

     c. Dans la fenêtre **Condition à partir des propriétés du fichier**, sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du fichier ou du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application. Sélectionnez pour ce faire le paramètre correspondant.

     d. Au besoin, modifiez les valeurs des paramètres du critère de condition sélectionné.

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

   - Choisissez l'option **Condition à partir des propriétés du fichier du dossier indiqué** afin de composer une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications à partir des propriétés des fichiers du dossier indiqué. Pour ce faire, procédez comme suit :

     a. Dans la fenêtre **Sélection d'un dossier**, sélectionnez le dossier contenant les fichiers exécutables des applications sur la base des propriétés desquels vous souhaitez composer une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications.

     b. Cliquez sur le bouton **OK**.

        La fenêtre **Ajout des conditions** s'ouvre.

     c. Dans le champ **Dossier**, modifiez si nécessaire le chemin d'accès au dossier contenant les fichiers exécutables des applications. Pour ce faire, cliquez sur le bouton **Sélectionner**. La fenêtre **Sélection du dossier** s'ouvre. Cette fenêtre permet de sélectionner le dossier souhaité.

     d. Dans la liste déroulante **Ajouter selon le critère**, sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application.

        Si vous choisissez l'élément **Métadonnées** dans la liste **Ajouter selon le critère**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom d'origine du fichier**, **Nom du fichier sur le disque**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Editeur**.

     e. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

f. Cliquez sur **Suivant**.

La liste des conditions de déclenchement de la règle définies s'affiche.

g. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de contrôle du lancement des applications.

h. Cliquez sur le bouton **Terminer**.

- Choisissez l'option **Condition(s) à partir des propriétés des applications lancées** pour définir une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications depuis les propriétés des applications exécutées sur l'ordinateur. Pour ce faire, procédez comme suit :

  a. Dans la liste déroulante **Ajouter selon le critère** de la fenêtre **Ajout des conditions**, sélectionnez le critère sur la base duquel vous souhaitez définir une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application.

  Si vous choisissez l'élément **Métadonnées** dans la liste **Ajouter selon le critère**, cochez les cases en regard des propriétés des fichiers exécutables de l'application que vous voulez utiliser dans la condition de déclenchement de la règle : **Nom d'origine du fichier**, **Nom du fichier sur le disque**, **Version du fichier**, **Nom de l'application**, **Version de l'application**, **Editeur**.

  b. Cochez les cases en regard des noms des fichiers exécutables des applications dont vous souhaitez inclure les propriétés dans la ou les conditions de déclenchement de la règle.

  c. Cliquez sur **Suivant**.

  La liste des conditions de déclenchement de la règle définies s'affiche.

  d. Dans la liste des conditions de déclenchement de la règle définies, cochez les cases en regard des conditions que vous souhaitez ajouter à la règle de contrôle du lancement des applications.

  e. Cliquez sur le bouton **Terminer**.

- Choisissez l'option **Condition(s) "Catégorie KL"** afin de définir une ou plusieurs conditions de déclenchement de la règle de contrôle du lancement des applications selon le critère catégorie KL. Pour ce faire, procédez comme suit :

  a. Dans la fenêtre **Condition(s) Catégorie KL**, cochez les cases en regard des noms des catégories KL qui vont servir de base à la création de la condition de déclenchement de la règle.

  b. Cliquez sur le bouton **OK**.

- Choisissez l'option **Condition manuelle** pour définir manuellement une condition de déclenchement de la règle de contrôle du lancement des applications. Pour ce faire, procédez comme suit :

  a. Saisissez le chemin d'accès au fichier exécutable de l'application dans la fenêtre **Condition personnalisée**. Pour ce faire, cliquez sur le bouton **Sélectionner**. La fenêtre **Ouvrir** Microsoft Windows s'ouvre. Cette fenêtre permet de sélectionner le fichier exécutable de l'application.

  b. Sélectionnez les critères sur la base desquels vous souhaitez créer une ou plusieurs conditions de déclenchement de la règle : **Métadonnées**, **Chemin du fichier ou du dossier**, **Code de hachage du fichier (MD5)** ou **Catégorie KL** à laquelle appartient le fichier exécutable de l'application. Sélectionnez pour ce faire le paramètre correspondant.

  c. Au besoin, modifiez les valeurs des paramètres du critère de condition sélectionné.

  d. Cliquez sur le bouton **OK**.

- Sélectionnez l'option **Condition d'après le support du fichier** pour définir la condition de déclenchement de la règle de contrôle du lancement des applications sur la base des informations relatives au support du fichier exécutable de l'application. Pour ce faire, procédez comme suit :

  a. Dans la liste **Support** de la fenêtre **Condition d'après le support du fichier**, sélectionnez le type de support depuis lequel le lancement de l'application sera soumis à la règle de contrôle du lancement des applications.

  b. Cliquez sur le bouton **OK**.

MODIFICATION DE L'ETAT DE FONCTIONNEMENT DE LA REGLE DE CONTROLE DU LANCEMENT DES APPLICATIONS

Pour modifier l'état du fonctionnement de la règle de contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez la règle dont vous souhaitez modifier l'état.
4. Dans la colonne **Etat**, procédez comme suit :
   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Act*.
   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Désact*.
   - Si vous souhaitez que la règle fonctionne en mode test, sélectionnez la valeur *Test*.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DES MODELES DES MESSAGES DU CONTROLE DU LANCEMENT DES APPLICATIONS

Quand l'utilisateur tente de lancer une application interdite par la règle de contrôle du lancement des applications, Kaspersky Endpoint Security affiche un message sur le blocage du lancement. Si l'utilisateur estime que le blocage du lancement de l'application n'a pas lieu d'être, il peut cliquer sur un lien dans la notification afin d'envoyer une réclamation à l'administrateur du réseau local de l'organisation.

Il existe des modèles pour les notifications relatives au blocage du lancement de l'application et pour les messages de réclamation. Vous pouvez modifier les modèles des messages.

Pour modifier le modèle de message, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle du lancement des applications**.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

   La fenêtre **Modèles** s'ouvre.
4. Exécutez une des actions suivantes :
   - Si vous souhaitez modifier le modèle de la notification relative au blocage du lancement de l'application, choisissez l'onglet **Blocage**.
   - Pour modifier le modèle de message de réclamation à l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Réclamation**.

5. Modifiez le modèle de message de blocage ou de réclamation. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.

6. Cliquez sur le bouton **OK**.

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

PRESENTATION DES MODES DE FONCTIONNEMENT DU CONTROLE DU LANCEMENT DES APPLICATIONS

Le module Contrôle du lancement des applications peut fonctionner selon deux modes :

- **Liste noire**. Mode dans le cadre duquel le Contrôle du lancement des applications autorise tous les utilisateurs à lancer n'importe quelle application, à l'exception de celles qui figurent dans les règles d'interdiction du Contrôle du lancement des applications (cf. section "A propos des règles de contrôle du lancement des applications" à la page 123).

  Il s'agit du mode de fonctionnement du Contrôle du lancement des applications par défaut. L'autorisation du lancement de toutes les applications repose sur la règle du Contrôle du lancement des applications "Tout autoriser" créée par défaut.

- **Liste blanche**. Mode dans le cadre duquel le Contrôle du lancement des applications interdit à tous les utilisateurs de lancer n'importe quelle application, à l'exception de celles qui figurent dans les règles d'autorisation du Contrôle du lancement des applications. Si les règles d'autorisation du Contrôle du lancement des applications sont rédigées complètement, le Contrôle du lancement des applications interdit le lancement de toutes les nouvelles applications qui n'ont pas été vérifiées par l'administrateur du réseau local, mais il garantit le fonctionnement du système d'exploitation et des applications vérifiées nécessaires aux utilisateurs dans l'exécution de leurs tâches.

La configuration du Contrôle du lancement des applications pour le fonctionnement dans ces modes est possible au départ de l'interface locale de Kaspersky Endpoint Security ou dans Kaspersky Security Center.

Ceci étant dit, Kaspersky Security Center propose des outils qui ne sont pas accessibles dans l'interface locale de Kaspersky Endpoint Security et qui sont indispensables pour réaliser les opérations suivantes :

- Création des catégories d'application (cf. section "Etape 2. Création des catégories d'applications" à la page 132). Les règles du Contrôle du lancement des applications du côté de Kaspersky Security Center reposent sur des catégories d'application que vous avez créées et non pas sur des conditions d'inclusion ou d'exception comme dans l'interface locale de Kaspersky Endpoint Security.

- Collecte des informations relatives aux applications installées sur les ordinateurs du réseau local de l'entreprise (cf. section "Etape 1. Collecte des informations relatives aux applications installées sur les ordinateurs des utilisateurs" à la page 131).

- Analyse du fonctionnement du Contrôle du lancement des applications après la modification du mode (cf. section "Etape 4. Test des règles d'autorisation du contrôle du lancement des applications" à la page 133).

C'est pour cette raison qu'il est conseillé de configurer le mode de fonctionnement du Contrôle du lancement des applications du côté de Kaspersky Security Center.

PASSAGE DU MODE "LISTE NOIRE" AU MODE "LISTE BLANCHE"

Cette section reprend les informations relatives au passage du mode de fonctionnement "Liste noire" du Contrôle du lancement des applications au mode "Liste blanche" du côté de Kaspersky Security Center et fournit des recommandations sur l'utilisation optimale de la fonctionnalité Contrôle du lancement des applications.

DANS CETTE SECTION

ETAPE 1. COLLECTE DES INFORMATIONS RELATIVES AUX APPLICATIONS INSTALLEES SUR LES ORDINATEURS DES UTILISATEURS

Pour cette étape, il faut avoir une idée des applications utilisées sur les ordinateurs du réseau local de l'entreprise. Pour ce faire, il est conseillé de récolter les informations relatives aux éléments suivants :

- Versions des systèmes d'exploitation Microsoft Windows.
- Fichiers exécutables lancés au démarrage du système d'exploitation. Définir les fichiers exécutables qui sont des fichiers système et ceux qui ont une implication dans l'activité professionnelle.
- Editeurs dont les applications sont considérées comme des applications de confiance sur le réseau local de l'organisation.
- Logiciels de bureautique et leurs versions.
- Logiciels spécialisés, développés en interne.
- Paquets standard d'applications d'entreprise et leur composition.
- Référentiel des distributions dans le réseau local de l'entreprise.

Pour récolter les informations relatives aux applications utilisées sur les ordinateurs du réseau local de l'entreprise, vous devez utiliser les données présentées dans les dossiers **Registre des applications** et **Fichiers exécutables des applications**. Les dossiers **Registre des applications** et **Fichiers exécutables des applications** font partie du dossier **Applications et vulnérabilités** de l'arborescence de la console Kaspersky Security Center.

Le dossier **Registre des applications** contient la liste des applications détectées sur les postes clients par l'Agent d'administration installés sur ces postes.

Le dossier **Fichiers exécutables** contient la liste des fichiers exécutables lancés à un moment ou l'autre sur les postes client ou découverts pendant le fonctionnement de la tâche d'inventaire de Kaspersky Endpoint Security (cf. section "Présentation des tâches pour Kaspersky Endpoint Security" à la page 248).

Après avoir ouvert la fenêtre des propriétés de l'application sélectionnée dans le dossier **Registre des applications** ou **Fichiers exécutables des applications**, vous pouvez obtenir les informations générales sur l'application et les informations relatives aux fichiers exécutables ainsi que consulter la liste des ordinateurs sur lesquels cette application est installée.

ETAPE 2. CREATION DES CATEGORIES D'APPLICATIONS

Au cours de cette étape, vous devez créer les catégories d'applications sur la base desquelles il est possible de créer les règles de contrôle du lancement des applications.

Il est conseillé de créer une catégorie "Applications pour le travail" qui reprend la sélection standard d'applications utilisées dans l'entreprise. Si différents groupes d'utilisateurs utilisent différentes sélections d'applications, vous pouvez créer une catégorie d'applications distincte pour chaque groupe d'utilisateurs.

Pour créer une catégorie d'applications, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Ouvrez le dossier **Ordinateurs administrés** de l'arborescence de la console.
3. Cliquez-droit pour ouvrir le menu contextuel dans le volet des résultats.
4. Dans le menu contextuel, sélectionnez l'option **Créer** → **Catégorie**.

   L'Assistant de création de catégories d'applications s'ouvre.
5. Suivez les instructions de l'Assistant de création de catégories d'applications.

ETAPE 3. CREATION DES REGLES D'AUTORISATION DU CONTROLE DU LANCEMENT DES APPLICATIONS

Cette étape correspond à la création des règles de contrôle du lancement des applications qui autorisent les utilisateurs du réseau local à lancer les applications appartenant aux catégories créées à l'étape antérieure.

Pour créer une règle d'autorisation du contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs gérés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans le volet des résultats, choisissez l'onglet **Stratégies**.
4. Cliquez-droit pour ouvrir le menu contextuel de la stratégie.
5. Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie s'ouvre.
6. Sélectionnez le groupe **Contrôle du lancement des applications** dans la fenêtre des propriétés de la stratégie.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.

7. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle de contrôle du lancement des applications** s'ouvre.

8. Dans la liste déroulante **Catégorie**, sélectionnez la catégorie d'applications créée à l'étape précédente sur la base de laquelle vous souhaitez créer la règle d'autorisation.

9. Composez la liste des utilisateurs et/ou des groupes d'utilisateurs autorisés à lancer les applications qui appartiennent à la catégorie sélectionnée. Pour ce faire, saisissez dans le champ **Utilisateurs et/ou les groupes qui reçoivent l'autorisation** les noms des utilisateurs et/ou des groupes d'utilisateurs manuellement ou à l'aide du bouton **Sélectionner**. La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**. Cette fenêtre permet de choisir les utilisateurs et/ou les groupes d'utilisateurs.

10. Ne remplissez pas la liste des utilisateurs autorisés à lancer les applications appartenant à la catégorie sélectionnée.

11. Cochez la case **Programmes de mise à jour des applications de confiance** si vous souhaitez que les applications de la catégorie qui figure dans la règle soient considérées comme des applications de mise à jour de confiance par Kaspersky Endpoint Security et qu'il les autorise à lancer d'autres applications pour lesquelles aucune règle de contrôle du lancement n'a été définie.

12. Cliquez sur le bouton **OK**.

13. Cliquez sur le bouton **Appliquer** dans le groupe **Contrôle du lancement des applications** de la fenêtre des propriétés de la stratégie.

ETAPE 4. TEST DES REGLES D'AUTORISATION DU CONTROLE DU LANCEMENT DES APPLICATIONS

Il convient de réaliser les opérations suivantes à cette étape :

1. Modifier le statut du fonctionnement des règles d'autorisation créées pour le contrôle du lancement des applications sur *Test* (cf. section "Modification du statut de la règle du Contrôle du lancement des applications du côté de Kaspersky Security Center" à la page 134).

2. Analyser le fonctionnement des règles d'autorisation de test du contrôle du lancement des applications.

   Pour analyser le fonctionnement des règles de test du contrôle du lancement des applications, il faut étudier les événements du fonctionnement du module Contrôle du lancement des applications survenus sur Kaspersky Security Center. Si l'exécution de toutes les applications que vous aviez en tête au moment de créer les catégories d'applications a été autorisée, alors les règles sont correctes. Dans le cas contraire, il faut ajuster les paramètres des catégories d'application et des règles de contrôle du lancement des applications que vous avez créées.

Pour pouvoir consulter les événements relatifs au fonctionnement du module Contrôle du lancement des applications dans le référentiel des événements de Kaspersky Security Center, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.

2. Ouvrez le dossier **Sélection d'événements\Evénements\Informations/Evénements critiques** de l'arborescence de la console afin de consulter les événements relatifs aux lancements d'application interdits ou autorisés.

   Dans la zone de travail de Kaspersky Security Center, située à droite de l'arborescence de la console, vous pouvez voir la liste de tous les événements correspondant au niveau d'importance sélectionné transmis sur Kaspersky Security Center au cours de la période définie dans les propriétés du Serveur d'administration.

3. Pour consulter les informations relatives aux événements, ouvrez les propriétés de l'événement d'une des méthodes suivantes :

   - Double-cliquez gauche sur l'événement.
   - Cliquez-droit sur le nom du poste client pour ouvrir le menu contextuel de l'événement et choisissez l'option **Propriétés**.
   - Cliquez sur le bouton **Ouvrir les propriétés de l'événement** à droite de la liste des événements.

ETAPE 5. PASSAGE AU MODE "LISTE BLANCHE"

Il convient de réaliser les opérations suivantes à cette étape :

- Activer les règles de contrôle du lancement des applications que vous avez créées. Pour ce faire, il convient de faire passer le statut du fonctionnement de la règle de *Test* à *Actif*.
- Activer les règles créées par défaut "Programmes de mise à jour des applications de confiance" et "Système d'exploitation et ses modules". Pour ce faire, il convient de faire passer le statut du fonctionnement de la règle de *Désact.* à *Actif*.
- Désactiver la règle créée par défaut "Tout autoriser". Pour ce faire, il convient de faire passer le statut du fonctionnement de la règle de *Actif* à *Désact*.

VOIR EGALEMENT

A propos des règles de contrôle du lancement des applications 123

Modification du statut de la règle du Contrôle du lancement des applications du côté de Kaspersky Security Center . 134

MODIFICATION DU STATUT DE LA REGLE DU CONTROLE DU LANCEMENT DES APPLICATIONS DU COTE DE KASPERSKY SECURITY CENTER

Pour modifier l'état du fonctionnement de la règle de contrôle du lancement des applications, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs gérés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration dont font partie les postes clients requis.
3. Dans le volet des résultats, choisissez l'onglet **Stratégies**.
4. Cliquez-droit pour ouvrir le menu contextuel de la stratégie.
5. Dans le menu contextuel de la stratégie, choisissez l'option **Propriétés**.

   La fenêtre des propriétés de la stratégie s'ouvre.
6. Sélectionnez le groupe **Contrôle du lancement des applications** dans la fenêtre des propriétés de la stratégie.

   Les paramètres du module Contrôle du lancement des applications s'afficheront dans la partie droite de la fenêtre.
7. Sélectionnez la règle de contrôle du lancement des applications dont vous souhaitez modifier l'état.
8. Réalisez une des opérations suivantes dans la colonne **Etat** :
   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Act*.
   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Désact*.
   - Si vous souhaitez que la règle fonctionne en mode test, sélectionnez la valeur *Test*.
9. Cliquez sur le bouton **Appliquer**.

CONTROLE DE L'ACTIVITE DES APPLICATIONS

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur le Contrôle de l'activité des applications et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DU CONTROLE DE L'ACTIVITE DES APPLICATIONS

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

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

Le module Pare-feu contrôle l'activité réseau des applications (cf. page 92).

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

Pour contribuer au fonctionnement plus efficace du Contrôle de l'activité des applications, il est conseillé de participer au Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 257). Les données obtenues à l'aide de Kaspersky Security Network permettent de référer plus précisément les applications à un groupe de confiance ou à un autre, et aussi appliquer les règles optimales du contrôle des applications.

Lors du lancement suivant de l'application, le Contrôle de l'activité des applications analyse l'intégrité de l'application. Si l'application n'a pas été modifiée, le module applique les règles de contrôle des applications existantes. En cas de modification de l'application, le Contrôle de l'activité des applications l'analyse comme s'il s'agit de sa première exécution.

ACTIVATION ET DESACTIVATION DU CONTROLE DE L'ACTIVITE DES APPLICATIONS

Par défaut, le Contrôle de l'activité des applications est activé et fonctionne dans le mode recommandé par les experts de Kaspersky Lab. Le cas échéant, vous pouvez désactiver le Contrôle de l'activité des applications.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver Contrôle de l'activité des applications sous l'onglet Statut de la protection de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle de l'activité des applications.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle de l'activité des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle de l'activité des applications**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle de l'activité des applications.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle de l'activité des applications**, sera modifiée sur l'icône .

Pour activer ou désactiver le Contrôle de l'activité des applications depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :
   - Cochez la case **Activer le Contrôle de l'activité des applications** pour activer le Contrôle de l'activité des applications.
   - Décochez la case **Activer le Contrôle de l'activité des applications** pour désactiver le Contrôle de l'activité des applications.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

REPARTITION DES APPLICATIONS SELON LES GROUPES DE CONFIANCE

Au premier lancement de l'application, le module Contrôle de l'activité des applications vérifie le niveau de danger de l'application et la place dans un des groupes de confiance.

Kaspersky Endpoint Security répartit toutes les applications lancées sur l'ordinateur en groupes de confiance. Les applications sont réparties en groupes de confiance selon le niveau de danger que ces applications peuvent représenter pour le système d'exploitation.

Les zones de confiances suivantes sont :

- **De confiance**. Ce groupe reprend les applications qui satisfont à une ou plusieurs des conditions suivantes :
  - Les applications sont dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network contient des enregistrements relatifs à ces applications.
  - L'utilisateur a placé les applications dans le groupe "De confiance".

  Il n'existe aucune opération interdite pour ces applications.
- **Restrictions faibles**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
  - L'indice de danger de ces applications est inférieur à 50.
  - L'utilisateur a placé les applications dans le groupe "Restrictions faibles".

  Il existe des restrictions minimes sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.
- **Restrictions élevées**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.
  - L'indice de danger ces applications est compris entre 51 et 71.
  - L'utilisateur a placé les applications dans le groupe "Restrictions élevées".

  Il existe des restrictions considérables sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.
- **Douteuses**. Ce groupe reprend les applications qui satisfont aux conditions suivantes :
  - Les applications ne sont pas dotées de la signature numérique d'un éditeur de confiance.
  - La base des applications de confiance de Kaspersky Security Network ne contient pas d'enregistrements relatifs à ces applications.

- L'indice de danger ces applications est compris entre 71 et 100.
- L'utilisateur a placé les applications dans le groupe "Douteuses".

Il existe des restrictions considérables sur les actions que ces applications peuvent exercer sur les ressources du système d'exploitation.

A la première étape de l'analyse de l'application, Kaspersky Internet Security cherche l'enregistrement sur l'application dans la base interne des applications connues, et puis envoie une demande à la base Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 257) (dans le cas de la connexion à Internet). Si l'enregistrement a été trouvé dans la base de Kaspersky Security Network, l'application se place dans le groupe de confiance enregistré dans la base de Kaspersky Security Network.

Pour répartir les applications inconnues selon les groupes de confiance, Kaspersky Endpoint Security utilise par défaut l'analyse heuristique. Pendant l'analyse heuristique, Kaspersky Endpoint Security définit le niveau de danger de l'application. En fonction du niveau de danger de l'application, Kaspersky Endpoint Security place l'application dans un groupe de confiance approprié. Au lieu d'utiliser l'analyse heuristique, vous pouvez définir le groupe de confiance où Kaspersky Endpoint Security doit mettre automatiquement les applications inconnues.

Par défaut, Kaspersky Endpoint Security analyse l'application pendant 30 secondes. Si à l'issue de ce temps, le niveau de danger de l'application n'a pas été défini, Kaspersky Endpoint Security place l'application dans le groupe de confiance Restrictions faibles et continue le processus de définition du niveau de danger de l'application en arrière-plan. Ensuite, Kaspersky Endpoint Security place l'application dans un groupe de confiance définitif. Vous pouvez modifier la durée consacrée à l'analyse du niveau de danger des applications exécutées. Si vous êtes convaincu que toutes les applications exécutées sur l'ordinateur de l'utilisateur ne menacent pas la sécurité, vous pouvez réduire la durée d'évaluation du niveau de danger de l'application. Si, au contraire, vous installez sur l'ordinateur de l'utilisateur des applications dont vous ne pouvez pas garantir la fiabilité en matière de sécurité, il est conseillé d'augmenter la durée d'évaluation du niveau de danger des applications.

Si le niveau de danger de l'application est élevé, Kaspersky Endpoint Security en avertit l'utilisateur et invite à sélectionner le groupe de confiance pour y placer cette application. La notification contient les statistiques d'utilisation de cette application par les participants de Kaspersky Security Network. En vous basant sur ces statistiques et l'historique de l'apparition de l'application sur l'ordinateur, l'utilisateur peut prendre une décision plus réfléchie sur le groupe de confiance correspondant à cette application.

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Si vous voulez placer automatiquement les applications avec une signature numérique dans le groupe "De confiance", cochez la case **Faire confiance aux applications dotées d'une signature numérique**.
4. Sélectionner le mode de répartition des applications inconnues selon les groupes de confiance :
   - Si vous souhaitez utiliser l'analyse heuristique pour la répartition des applications inconnues selon les groupes de confiance, sélectionnez l'option **Déterminer le groupe à l'aide de l'analyse heuristique**.
   - Si vous souhaitez placer toutes les applications inconnues dans le groupe de confiance indiqué, sélectionnez l'option **Placer automatiquement dans le groupe** et sélectionnez le groupe de confiance requis dans la liste déroulante.
5. Indiquez la durée consacrée à l'analyse de l'application exécutée dans le champ **Durée maximale pour déterminer le groupe**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DU GROUPE DE CONFIANCE

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

Les experts de Kaspersky Lab déconseillent de déplacer les applications du groupe de confiance défini automatiquement dans un autre groupe de confiance. Au lieu de cela, modifiez si nécessaire les règles pour l'application en question (cf. section "Modification des règles de l'application" à la page 141).

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Règles du contrôle des applications** de la fenêtre **Applications** s'ouvre.
4. Sélectionnez sous l'onglet **Règles du contrôle des applications** l'application requise.
5. Exécutez une des actions suivantes :

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

UTILISATION DES REGLES DE CONTROLE DES APPLICATIONS

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

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

DANS CETTE SECTION

MODIFICATION DES REGLES DE CONTROLE DES GROUPES DE CONFIANCE ET DES REGLES DE CONTROLE DES GROUPES D'APPLICATIONS

Par défaut, les règles optimales de contrôle des applications ont été créées pour différents groupes de confiance. Les paramètres des règles de contrôle de groupes d'applications qui font partie du groupe de confiance héritent les valeurs des paramètres des règles de contrôle de groupes de confiance. Vous pouvez modifier les règles de contrôle de groupes de confiance préinstallées et les règles de contrôle de groupes d'applications.

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

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Règles du contrôle des applications** de la fenêtre **Applications** s'ouvre.
4. Sélectionnez sous l'onglet **Règles du contrôle des applications** le groupe de confiance ou le groupe d'applications requis.
5. Cliquez-droit pour ouvrir le menu contextuel du groupe de confiance ou du groupe d'applications.
6. Dans le menu contextuel du groupe de confiance ou du groupe d'applications, sélectionne l'option **Règles pour le groupe**.

   La fenêtre **Règles du contrôle du groupe d'applications** s'ouvre.

7. Dans la fenêtre **Règles du contrôle du groupe d'applications**, exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et base de registres** pour modifier les règles de contrôle du groupe de confiance et les règles de contrôle du groupe d'applications qui régissent les droits du groupe de confiance ou du groupe d'applications relatives aux opérations avec le registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.

   - Sélectionnez l'onglet **Privilèges** pour modifier les règles de contrôle du groupe de confiance ou les règles de contrôle du groupe d'applications qui régissent les droits du groupe de confiance ou du groupe d'applications relatifs à l'accès aux processus et aux objets du système d'exploitation.

8. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.

9. Sélectionnez l'option souhaitée dans le menu contextuel.

   - **Hériter**.

   - **Autoriser**.

   - **Interdire**.

   - **Consigner dans le rapport**.

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

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

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

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

MODIFICATION DES REGLES DE CONTROLE DE L'APPLICATION

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

Pour modifier une règle du contrôle de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

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

   L'onglet **Règles du contrôle des applications** de la fenêtre **Applications** s'ouvre.

4. Sélectionnez sous l'onglet **Règles du contrôle des applications** l'application requise.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de l'application. Dans le menu contextuel de l'application, sélectionnez l'option **Règles pour l'application.**

   - Cliquez sur le bouton **Avancé** dans le coin inférieur droit de l'onglet **Règles du contrôle des applications**.

La fenêtre **Règles du contrôle de l'application** s'ouvre.

6. Dans la fenêtre **Règles du contrôle de l'application**, exécutez une des actions suivantes :

   - Sélectionnez l'onglet **Fichiers et base de registres** pour modifier les règles du contrôle de l'application qui régissent les droits de l'application relatifs aux opérations avec le registre du système d'exploitation, les fichiers utilisateur et les paramètres d'applications.

   - Sélectionnez l'onglet **Privilèges** pour modifier les règles du contrôle de l'application qui régissent les droits de l'application relatifs à l'accès aux processus et à d'autres objets du système d'exploitation.

7. Pour la ressource requise, cliquez-droit dans la colonne de l'action correspondante pour ouvrir le menu contextuel.

8. Sélectionnez l'option souhaitée dans le menu contextuel.

   - **Hériter**.

   - **Autoriser**.

   - **Interdire**.

   - **Consigner dans le rapport**.

9. Cliquez sur le bouton **OK**.

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

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

TELECHARGEMENT ET MISE A JOUR DES REGLES DE CONTROLE DES APPLICATIONS DEPUIS LA BASE DE KASPERSKY SECURITY NETWORK

Par défaut, les règles du contrôle des applications téléchargées depuis la base de Kaspersky Security Network sont appliquées pour les applications découvertes dans cette base.

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

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

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

3. Décochez la case **Mettre à jour les règles de contrôle des applications depuis la base de KSN**.

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

DESACTIVATION DE L'HERITAGE DES RESTRICTIONS DU PROCESSUS PARENT

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

Lorsque l'application tente d'accéder à la ressource contrôlée, le Contrôle de l'activité des applications analyse les droits de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource. Dans ce cas, c'est la règle de la priorité minimale qui est appliquée : lorsque les droits d'accès de l'application et du processus parent sont comparés, les droits d'accès avec la priorité minimale sont appliqués à l'activité de l'application.

Priorité des droits d'accès :

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

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

Si l'activité de l'application est bloquée à cause du manque des droits chez un des processus parental, vous pouvez changer ces règles (cf. section "Modification des règles pour l'application sélectionnée" à la page 141) ou désactiver l'héritage des restrictions du processus parent.

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Règles du contrôle des applications** de la fenêtre **Applications** s'ouvre.
4. Sélectionnez sous l'onglet **Règles du contrôle des applications** l'application requise.
5. Cliquez-droit pour ouvrir le menu contextuel de l'application.
6. Dans le menu contextuel de l'application, sélectionnez l'option **Règles pour l'application.**

   La fenêtre **Règles du contrôle de l'application** s'ouvre.
7. Dans la fenêtre **Règles du contrôle de l'application** qui s'ouvre, sélectionnez l'onglet **Exclusions**.
8. Cochez la case **Restriction non héritée du processus parent (application)**.
9. Cliquez sur le bouton **OK**.
10. Dans la fenêtre **Applications**, cliquez sur **OK**.
11. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

EXCLUSION DE CERTAINES ACTIONS DES APPLICATIONS DES REGLES DU CONTROLE DES APPLICATIONS

Pour exclure certaines actions des applications des règles du contrôle des applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Applications**.

   L'onglet **Règles du contrôle des applications** de la fenêtre **Applications** s'ouvre.
4. Sélectionnez sous l'onglet **Règles du contrôle des applications** l'application requise.
5. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de l'application, puis sélectionnez l'option **Règles de l'application**.

   La fenêtre **Règles du contrôle de l'application** s'ouvre.
6. Dans la fenêtre **Règles du contrôle de l'application** qui s'ouvre, sélectionnez l'onglet **Exclusions**.
7. Cochez les cases en regard des actions de l'application à ne pas contrôler.
8. Cliquez sur le bouton **OK**.
9. Dans la fenêtre **Applications**, cliquez sur **OK**.
10. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DES PARAMETRES DE STOCKAGE DES REGLES DU CONTROLE DES APPLICATIONS NON UTILISEES

Les règles du contrôle des applications qui n'ont pas été utilisées depuis 60 jours sont supprimées automatiquement par défaut. Vous pouvez modifier la durée de stockage des règles du contrôle des applications non utilisées ou désactiver la suppression automatique.

Pour configurer les paramètres de stockage des règles du contrôle des applications non utilisées, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cochez la case **Supprimer les règles du contrôle des applications qui n'ont plus été lancées depuis** et indiquez le nombre de jours requis si vous voulez que Kaspersky Endpoint Security supprime les règles du contrôle des applications non utilisées.
   - Décochez la case **Supprimer les règles du contrôle des applications qui n'ont plus été lancées depuis** pour désactiver la suppression automatique des règles du contrôle des applications non utilisées.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

PROTECTION DES RESSOURCES DU SYSTEME D'EXPLOITATION ET DES DONNEES PERSONNELLES

Le module Contrôle de l'activité des applications gère les droits des applications relatifs aux opérations sur différentes catégories de ressources du système d'exploitation et de données personnelles.

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

Vous pouvez exécuter les opérations suivantes :

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

DANS CETTE SECTION

AJOUT DE LA CATEGORIE DES RESSOURCES PROTEGEES

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

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Ressources**.

   L'onglet **Ressources protégées** de la fenêtre **Applications** s'ouvre.
4. Sélectionnez dans la partie gauche de l'onglet **Ressources protégées** la section ou la catégorie des ressources protégées dans laquelle vous souhaitez ajouter une nouvelle catégorie des ressources protégées.
5. Cliquez-droit pour ouvrir le menu contextuel du bouton **Ajouter**.
6. Sélectionnez **Catégorie** dans le menu contextuel.

   La fenêtre **Catégorie des ressources protégées** s'ouvre.
7. Saisissez dans la fenêtre **Catégorie des ressources protégées** le nom de la nouvelle catégorie des ressources protégées.
8. Cliquez sur le bouton **OK**.

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

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

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

Après avoir ajouté la catégorie de ressources protégées, vous pouvez la modifier ou la supprimer à l'aide des boutons **Modifier** et **Supprimer** dans la partie supérieure gauche de l'onglet **Ressources protégées**.

AJOUT DE LA RESSOURCE PROTEGEE

Pour ajouter une ressource protégée, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.

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

   L'onglet **Ressources protégées** de la fenêtre **Applications** s'ouvre.

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

5. Cliquez-gauche dans la partie supérieure gauche de l'onglet **Ressources protégées** afin d'ouvrir le menu contextuel du bouton **Ajouter**.

6. Dans le menu contextuel, sélectionnez le type de ressource que vous souhaitez ajouter :

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

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

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

8. Cliquez sur le bouton **Parcourir**.

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

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

    Sous l'onglet **Ressources protégées** un élément nouveau apparaît dans la liste des ressources protégées.

11. Cliquez sur le bouton **OK**.

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

Après avoir ajouté la ressource protégée, vous pouvez la modifier ou la supprimer à l'aide des boutons **Modifier** et **Supprimer** dans la partie supérieure gauche de l'onglet **Ressources protégées**.

DESACTIVATION DE LA PROTECTION DE LA RESSOURCE

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle de l'activité des applications**.

   Les paramètres du module Contrôle de l'activité des applications s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ressources**.

   L'onglet **Ressources protégées** de la fenêtre **Applications** s'ouvre.
4. Exécutez une des actions suivantes :
   - Sélectionnez la ressource dans la liste des ressources protégées de la partie gauche de l'onglet dont vous souhaitez désactiver la protection et décochez la case en regarde de son nom.
   - Cliquez sur le bouton **Exclusions** et procédez comme suit :
     a. Cliquez-gauche dans la fenêtre **Exclusions** afin d'ouvrir le menu contextuel du bouton **Ajouter**.
     b. Dans le menu contextuel, sélectionnez le type de ressource que vous souhaitez ajouter à la liste des exclusions de la protection du module Contrôle de l'activité des applications : **Fichier ou dossier** ou **Clé de registre**.

        La fenêtre **Ressource protégée** s'ouvre.
     c. Saisissez dans la fenêtre **Ressource protégée** dans le champ **Nom** le nom de la ressource protégée.
     d. Cliquez sur le bouton **Parcourir**.
     e. Définissez dans la fenêtre qui s'ouvre les paramètres requis en fonction du type de la ressource protégée que vous souhaitez ajouter à la liste des exclusions de la protection du module Contrôle de l'activité des applications.
     f. Cliquez sur le bouton **OK**.
     g. Dans la fenêtre **Ressource protégée**, cliquez sur **OK**.

        Dans la liste des ressources exclues de la protection du module Contrôle de l'activité des applications, un élément nouveau apparaît.

        Après avoir ajouté la ressource à la liste des exclusions de la protection du module Contrôle de l'activité des applications, vous pouvez la modifier ou la supprimer à l'aide des boutons **Modifier** et **Supprimer** dans la partie supérieure de la fenêtre **Exclusions**.

     h. Dans la fenêtre **Exclusions**, cliquez sur **OK**.
5. Dans la fenêtre **Applications**, cliquez sur **OK**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONTROLE DES PERIPHERIQUES

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur le Contrôle des périphériques et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DU CONTROLE DES PERIPHERIQUES

Contrôle des périphériques garantit la sécurité des informations confidentielles en limitant l'accès utilisateur aux périphériques installés ou connectés à l'ordinateur :

- périphériques de mémoire (disques durs, supports amovibles, lecteurs de bande, CD/DVD) ;
- dispositifs de transmission des informations (modems, carte de réseau externe) ;
- dispositifs de conversion en sortie papier (imprimantes) ;
- bus de connexion (ci-après bus) : interfaces qui permettent de connecter les périphériques à l'ordinateur (USB, FireWire, Infrarouge, etc.).

Le Contrôle des périphériques gère l'accès utilisateur aux périphériques à l'aide des *règles d'accès aux périphériques* (ci-après règles d'accès) et des *règles d'accès aux bus de connexion* (ci-après règles d'accès aux bus).

ACTIVATION ET DESACTIVATION DU CONTROLE DES PERIPHERIQUES

Le Contrôle des périphériques est activé par défaut. Le cas échéant, vous pouvez activer le Contrôle des périphériques.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver le Contrôle des périphériques, sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle des périphériques.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle des périphériques.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle des périphériques**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle des périphériques.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle des périphériques**, sera modifiée sur l'icône .

Pour activer ou désactiver le Contrôle des périphériques depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer le Contrôle des périphériques** pour activer le Contrôle des périphériques.
   - Décochez la case **Activer le Contrôle des périphériques** pour désactiver le Contrôle des périphériques.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A PROPOS DES REGLES D'ACCES AUX PERIPHERIQUES ET AUX BUS DE CONNEXION

La règle d'accès aux périphériques est un ensemble des paramètres qui définit les fonctions suivantes du module Contrôle des périphériques :

- L'autorisation aux utilisateurs et/ou aux groupes d'utilisateurs sélectionnés d'accéder les types des périphériques pour les périodes définies.

  Vous pouvez sélectionner les utilisateurs et/ou les groupes d'utilisateurs et leur créer une programmation de l'accès aux périphériques.

- Définition de droits de lecture du contenu des périphériques de mémoire.

- Définition de droits de modification du contenu des périphériques de mémoire.

Par défaut, pour tous les types de périphériques de la classification du module Contrôle des périphériques sont créées les règles d'accès qui autorisent l'accès libre aux périphériques à tous les utilisateurs à tout moment si l'accès aux bus de connexion pour les types appropriés de périphériques est autorisé.

La règle d'accès au bus de connexion représente une extension ou une interdiction d'accès au bus de connexion.

Par défaut, les règles qui autorisent l'accès à tous les bus ont été créées pour les bus de connexion de la classification du module Contrôle des périphériques.

Vous ne pouvez pas créer et supprimer les règles d'accès aux périphériques et les règles d'accès aux bus de connexion, vous ne pouvez que les modifier.

A PROPOS DES PERIPHERIQUES DE CONFIANCE

Périphériques de confiance sont les périphériques que les utilisateurs définis dans les paramètres du périphérique de confiance peuvent accéder librement à tout moment.

Les actions suivantes peuvent être exécutées sur les périphériques de confiance :

- ajout du périphérique à la liste des périphériques de confiance ;

- modification de l'utilisateur et/ou groupe d'utilisateurs qui ont l'accès au périphérique de confiance ;

- suppression du périphérique de la liste des périphériques de confiance.

Si le périphérique est ajouté à la liste des périphériques de confiance et une règle d'accès qui interdit ou limite l'accès est créée pour ce type de périphérique, lors de la prise de la décision sur l'accès au périphérique la présence du périphérique sur la liste des périphériques de confiance a une priorité plus élevée que la règle d'accès.

DECISIONS TYPES SUR L'ACCES AUX PERIPHERIQUES

Une fois que l'utilisateur a connecté un périphérique à l'ordinateur, Kaspersky Endpoint Security prend la décision sur l'accès à ce périphérique.

Tableau 2. Décisions types sur l'accès aux périphériques

N°	CONDITIONS D'ORIGINE	ETAPES INTERMEDIAIRES AVANT LA PRISE DE DECISION SUR L'ACCES AU PERIPHERIQUE			DECISION SUR L'ACCES AU PERIPHERIQUE
		VERIFICATION DE LA PRESENCE DU PERIPHERIQUE DANS LA LISTE DES PERIPHERIQUES DE CONFIANCE	VERIFICATION DE L'ACCES AU PERIPHERIQUE SUR LA BASE DE LA REGLE D'ACCES	VERIFICATION DE L'ACCES AU BUS SUR LA BASE DE LA REGLE D'ACCES AU BUS	
1	Le périphérique ne figure pas dans le classement du module Contrôle des périphériques.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Ignoré	Accès autorisé
2	Le périphérique est un périphérique de confiance.	Figure sur la liste des périphériques de confiance.	Ignoré	Ignoré	Accès autorisé
3	L'accès au périphérique est autorisé.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé	Ignoré	Accès autorisé
4	Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès autorisé	Accès autorisé
5	Accès au périphérique dépend du bus.	Ne figure pas sur la liste des périphériques de confiance.	Accès dépend du bus.	Accès interdit.	Accès interdit.
6	L'accès au périphérique est autorisé. Règle d'accès au bus inexistante.	Ne figure pas sur la liste des périphériques de confiance.	Accès autorisé	Règle d'accès au bus inexistante.	Accès autorisé
7	Accès au périphérique interdit.	Ne figure pas sur la liste des périphériques de confiance.	Accès interdit.	Ignoré	Accès interdit.
8	Règle d'accès au périphérique et règle d'accès au bus inexistante.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Règle d'accès au bus inexistante.	Accès autorisé
9	Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Accès autorisé	Accès autorisé
10	Règle d'accès au périphérique absente.	Ne figure pas sur la liste des périphériques de confiance.	Règle d'accès inexistante	Accès interdit.	Accès interdit.

Vous pouvez modifier la règle d'accès au périphérique après sa connexion. Si le périphérique a été connecté et la règle d'accès a autorisé l'accès au périphérique, mais vous avez ensuite modifié la règle d'accès pour interdire l'accès au périphérique, toute tentative d'accès au périphérique pour l'opération de fichiers (consultation de l'arborescence des catalogue, lecture, enregistrement) sera d'ores et déjà bloquée par Kaspersky Endpoint Security. Le blocage du périphérique sans système de fichiers aura lieu uniquement lors de la connexion suivante du périphérique.

MODIFICATION D'UNE REGLE D'ACCES AUX PERIPHERIQUES

Pour modifier le droit d'accès aux périphériques, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Types de périphériques**.

   Sous l'onglet **Types de périphériques** se trouvent les règles d'accès pour tous les périphériques qui figurent dans le classement du module Contrôle des périphériques.

4. Sélectionnez la règle d'accès que vous souhaitez modifier.

5. Cliquez sur le bouton **Modifier**. Le bouton est accessible uniquement pour les types de périphériques avec un système de fichiers.

   La fenêtre **Configuration de la règle d'accès aux périphériques** s'ouvre.

   Par défaut, la règle d'accès aux périphériques autorise un accès libre au type de périphériques à tout moment pour tous les utilisateurs. Cette règle d'accès dans la liste **Utilisateurs et/ou groupes d'utilisateurs** contient le groupe **Tous**, et contient dans le tableau **Privilèges du groupe d'utilisateurs sélectionné en fonction des planifications d'accès** la programmation **Tout le temps** avec des droits définis pour toutes les opérations possibles avec les périphériques.

6. Modifiez les paramètres de la règle d'accès aux périphériques :

   a. Pour modifier la liste **Utilisateurs et/ou groupes d'utilisateurs**, utilisez les boutons **Ajouter**, **Modifier**, **Supprimer**.

   b. Pour modifier la liste de programmations d'accès aux périphériques, utilisez les boutons **Créer**, **Modifier**, **Copier**, **Supprimer** dans le tableau **Privilèges du groupe sélectionné d'utilisateurs en fonction des programmations de l'accès**.

   c. Sélectionnez l'utilisateur et/ou le groupe d'utilisateurs dans la liste **Utilisateurs et/ou groupes d'utilisateurs**.

   d. Dans le tableau **Privilèges du groupe sélectionné d'utilisateurs en fonction des programmations de l'accès**, configurez la programmation de l'accès aux périphériques pour l'utilisateur et/ou le groupe sélectionné d'utilisateurs. Pour ce faire, cochez les cases à côté des noms des programmations de l'accès aux périphériques que vous souhaitez utiliser dans la règle modifiable d'accès aux périphériques.

   e. Pour chaque programmation de l'accès aux périphériques utilisée pour l'utilisateur ou le groupe d'utilisateurs sélectionnés, définissez les opérations autorisées lors de l'utilisation des périphériques. Pour ce faire, dans le tableau **Privilèges du groupe sélectionné d'utilisateurs en fonction des programmations de l'accès** cochez les cases dans les colonnes avec les noms des opérations qui vous intéressent.

   f. Répétez les étapes c à e pour les autres éléments de la liste **Utilisateurs et/ou groupes d'utilisateurs**.

   g. Cliquez sur le bouton **OK**.

   Une fois que vous avez modifié les valeurs d'origine des paramètres de la règle d'accès aux périphériques, le paramètre d'accès au type de périphérique prend la valeur *Autorisé avec des restrictions*.

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

MODIFICATION DE LA REGLE D'ACCES AU BUS DE CONNEXION

Pour modifier la règle d'accès au bus de connexion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez l'onglet **Bus de connexion**.

   Sous l'onglet **Bus de connexion** se trouvent les règles d'accès pour tous les bus de connexion qui existent dans la classification du module Contrôle des périphériques.
4. Sélectionnez la règle d'accès au bus que vous souhaitez modifier.
5. Modifiez la valeur du paramètre d'accès :
   - Pour autoriser l'accès au bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Autoriser**.
   - Pour interdire l'accès au bus de connexion, cliquez dans la colonne **Accès** pour ouvrir le menu contextuel et sélectionnez l'option **Interdire**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACTIONS AVEC LES PERIPHERIQUES DE CONFIANCE

Cette section contient des informations sur les actions avec les périphériques de confiance.

DANS CETTE SECTION

AJOUT DU PERIPHERIQUE A LA LISTE DES PERIPHERIQUES DE CONFIANCE

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder.

Pour ajouter un périphérique à la liste des périphériques de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

   Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périphériques de confiance**.
3. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Ajout de périphériques de confiance** s'ouvre.
4. Cochez la case en regard du nom du périphérique que vous souhaitez ajouter à la liste des périphériques de confiance.

   La liste des périphériques dans la colonne **Périphériques** dépend de la valeur sélectionnée dans la liste déroulante **Afficher les périphériques connectés**.
5. Cliquez sur le bouton **Sélectionner**.

   La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** s'ouvre.
6. Définissez dans la fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** les utilisateurs et/ou les groupes d'utilisateurs pour lesquels Kaspersky Endpoint Security reconnaît les périphériques sélectionnés en tant que périphériques de confiance.

   Les noms des utilisateurs et/ou des groupes d'utilisateurs, définis dans la fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes** seront affichés dans le champ **Autoriser les utilisateurs et/ou les groupes d'utilisateurs**.
7. Dans la fenêtre **Ajout de périphériques de confiance**, cliquez **OK**.

   Sous l'onglet **Périphériques de confiance** de la fenêtre de configuration du module **Contrôle des périphériques** du tableau s'affichera la ligne des paramètres du périphérique de confiance ajouté.
8. Répétez les étapes 4 à 8 pour chacun des périphériques que vous souhaitez ajouter à la liste des périphériques de confiance pour des utilisateurs et/ou des groupes d'utilisateurs spécifiques.
9. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DU PARAMETRE UTILISATEURS DU PERIPHERIQUE DE CONFIANCE

Par défaut, si le périphérique est ajouté à la liste des périphériques de confiance, tous les utilisateurs (groupe d'utilisateurs Tous) sont autorisés à y accéder. Vous pouvez modifier le paramètre **Utilisateurs** du périphérique de confiance.

Pour modifier le paramètre Utilisateurs du périphérique de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périphériques de confiance**.
4. Sélectionnez le périphérique dont vous souhaitez modifier les paramètres dans la liste des périphériques de confiance.
5. Cliquez sur le bouton **Modifier**.

   La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.
6. Modifier la liste des utilisateurs et/ou des groupes d'utilisateurs pour lesquels ce périphérique est un périphérique de confiance.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

SUPPRESSION DU PERIPHERIQUE DE LA LISTE DES PERIPHERIQUES DE CONFIANCE

Pour supprimer le périphérique de la liste des périphériques de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez l'onglet **Périphériques de confiance**.
4. Sélectionnez le périphérique que vous souhaitez supprimer de la liste des périphériques de confiance.
5. Cliquez sur le bouton **Supprimer**.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

La décision sur l'accès au périphérique que vous avez supprimé de la liste des périphériques de confiance est prise par Kaspersky Endpoint Security sur la base des règles d'accès aux périphériques et sur la base des règles d'accès aux bus de connexion.

MODIFICATION DES MODELES DES MESSAGES DU CONTROLE DES PERIPHERIQUES

Quand l'utilisateur tente de s'adresser au périphérique bloqué, Kaspersky Endpoint Security affiche le message sur le blocage d'accès au périphérique ou sur l'interdiction de l'opération sur le contenu du périphérique. Si l'utilisateur croit que le blocage d'accès au périphérique ou l'interdiction de l'opération sur le contenu du périphérique sont intervenus par erreur, il peut cliquer sur le lien dans le message de blocage pour envoyer une réclamation à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message de blocage d'accès au périphérique et de message d'interdiction de l'opération avec le contenu du périphérique. Vous pouvez modifier les modèles des messages.

Pour modifier le modèle de message du Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

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

   - Pour modifier le modèle de message de blocage d'accès au périphérique ou d'interdiction de l'opération avec le contenu du périphérique, sélectionnez l'onglet **Blocage**.
   - Pour modifier le modèle de message de réclamation à l'administrateur du réseau local d'entreprise, sélectionnez l'onglet **Réclamation**.
5. Modifiez le modèle de message de blocage ou de réclamation. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACCES AU PERIPHERIQUE BLOQUE

L'utilisateur peut accéder au périphérique bloqué. Pour ce faire, il faut envoyer la demande depuis la fenêtre de configuration du module Contrôle des périphériques ou en passant par le lien dans le message de blocage de périphérique.

Les fonctions de Kaspersky Endpoint Security pour recevoir l'accès temporaire au périphérique sont disponibles uniquement dans le cas où Kaspersky Endpoint Security fonctionne sous une stratégie de Kaspersky Security Center et que cette fonctionnalité a été activée dans les paramètres de la stratégie.

Pour accéder au périphérique bloqué depuis la fenêtre de configuration du module Contrôle des périphériques, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle des périphériques**.

   Les paramètres du module Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Demander l'accès**.

   La fenêtre **Demande d'accès au périphérique** s'ouvre.

4. Sélectionnez dans la liste des périphériques connectés le périphérique que vous souhaitez accéder.

5. Cliquez sur le bouton **Obtenir la clé d'accès**.

   La fenêtre **Obtention de la clé d'accès au périphérique** s'ouvre.

6. Indiquez dans le champ **Durée de l'accès** la durée pendant laquelle vous souhaitez avoir accès au périphérique.

7. Cliquez sur le bouton **Exporter**.

   Une fenêtre standard Microsoft Windows intitulée **Enregistrement de la clé d'accès** s'ouvre.

8. Dans la fenêtre Microsoft Windows **Enregistrement de la clé d'accès**, sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès au périphérique, puis cliquez sur **Enregistrer**.

9. Transmettez le fichier contenant la clé d'accès au périphérique à l'administrateur du réseau local de l'organisation.

10. Il vous remettra le code d'accès au périphérique.

11. Dans la fenêtre **Demande de l'accès au périphérique**, cliquez sur le bouton **Activer le code d'accès**.

    La fenêtre standard Microsoft Windows **Chargement du code d'accès** s'ouvre.

12. Dans la fenêtre Microsoft Windows **Chargement du code d'accès**, sélectionnez le fichier contenant le code d'accès au périphérique remis par l'administrateur du réseau local, puis cliquez sur **Ouvrir**.

    La fenêtre **Activation du code d'accès au périphérique** qui fournit des informations sur l'accès octroyé s'ouvre.

13. Dans la fenêtre **Activation du code d'accès au périphérique**, cliquez sur **OK**.

Pour accéder au périphérique bloqué via le lien dans le message de blocage de l'appareil, procédez comme suit :

1. Depuis la fenêtre de message de blocage du périphérique ou du bus de connexion, cliquez sur le lien **Demander l'accès**.

   La fenêtre **Obtention de la clé d'accès au périphérique** s'ouvre.

2. Indiquez dans le champ **Durée de l'accès** la durée pendant laquelle vous souhaitez avoir accès au périphérique.

3. Cliquez sur le bouton **Exporter**.

   Une fenêtre standard Microsoft Windows intitulée **Enregistrement de la clé d'accès** s'ouvre.

4. Dans la fenêtre Microsoft Windows **Enregistrement de la clé d'accès**, sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant la clé d'accès au périphérique, puis cliquez sur **Enregistrer**.

5. Transmettez le fichier contenant la clé d'accès au périphérique à l'administrateur du réseau local de l'organisation.

6. Il vous remettra le code d'accès au périphérique.

7. Dans la fenêtre **Demande de l'accès au périphérique**, cliquez sur le bouton **Activer le code d'accès**.

   La fenêtre standard Microsoft Windows **Chargement du code d'accès** s'ouvre.

8. Dans la fenêtre Microsoft Windows **Chargement du code d'accès**, sélectionnez le fichier contenant le code d'accès au périphérique remis par l'administrateur du réseau local, puis cliquez sur **Ouvrir**.

   La fenêtre **Activation du code d'accès au périphérique** qui fournit des informations sur l'accès octroyé s'ouvre.

9. Dans la fenêtre **Activation du code d'accès au périphérique**, cliquez sur **OK**.

La durée d'accès au périphérique octroyée peut varier de celle que vous avez demandée. L'accès au périphérique est octroyé pour une durée que l'administrateur du réseau local indique lors de la création du code d'accès au périphérique.

CREATION DU CODE D'ACCES AU PERIPHERIQUE

Pour octroyer à l'utilisateur un accès temporaire au périphérique, il faut un code d'accès au périphérique. Vous pouvez créer le code d'accès au périphérique sur Kaspersky Security Center.

Pour créer le code d'accès au périphérique, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.

2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.

3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.

4. Dans la liste des postes clients, sélectionnez l'ordinateur à l'utilisateur duquel vous souhaitez octroyer un accès temporaire au périphérique.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Dans le menu contextuel du poste client, choisissez l'option **Propriétés**.

   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.

6. Choisissez la section **Tâches**.

   La liste des tâches locales pour l'administration de Kaspersky Endpoint Security apparaît dans la partie droite de la fenêtre.

7. Choisissez la tâche **Contrôle des périphériques** dans la liste des tâches locales.

8. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche. Dans le menu contextuel de la tâche, choisissez l'option **Propriétés**.

   - Cliquez sur le bouton **Propriétés**.

   La fenêtre **Propriétés : Contrôle des périphériques** s'ouvre.

9. Dans la fenêtre **Propriétés: Contrôle des périphériques**, sélectionnez la section **Paramètres**.

   Les paramètres de la tâche locale Contrôle des périphériques s'afficheront dans la partie droite de la fenêtre.

10. Dans la partie droite de la fenêtre, cliquez sur le bouton **Accorder l'accès**.

    La fenêtre **Autorisation d'accès temporaire au périphérique** s'ouvre.

11. Dans la fenêtre **Autorisation d'accès temporaire au périphérique**, cliquez sur le bouton **Parcourir**.

    La fenêtre standard de Microsoft Windows **Sélection de la clé d'accès** s'ouvre.

12. Dans la fenêtre Microsoft Windows **Sélection de la clé d'accès**, sélectionnez le fichier contenant la clé d'accès que vous avez reçu de l'utilisateur, puis cliquez sur **Ouvrir**.

    Les informations relatives au périphérique auquel l'utilisateur a demandé l'accès s'affichent dans la fenêtre **Autorisation d'accès temporaire au périphérique**.

13. Définissez la valeur du paramètre **Durée de l'accès**. Ce paramètre détermine la durée pendant laquelle vous permettez à l'utilisateur d'accéder au périphérique.

    La valeur proposée par défaut est celle indiquée par l'utilisateur lors de la création de la clé d'accès.

14. Définissez la valeur du paramètre **Délai d'activation**. Le paramètre définit la période au cours de laquelle l'utilisateur peut activer l'accès au périphérique à l'aide du code d'activation.

15. Cliquez sur le bouton **Enregistrer le code d'accès**.

    La fenêtre Microsoft Windows standard **Enregistrement du code d'accès** s'ouvre.

16. Sélectionnez le dossier dans lequel vous souhaitez enregistrer le fichier contenant le code d'accès au périphérique.

17. Cliquez sur le bouton **Exporter**.

CONTROLE INTERNET

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Cette section contient des informations sur le Contrôle Internet et les instructions sur la configuration des paramètres du module.

DANS CETTE SECTION

A PROPOS DU CONTROLE INTERNET

Le modèle Contrôle Internet permet de contrôler l'activité utilisateur du réseau local d'entreprise : limiter ou autoriser l'accès aux sites Internet.

Une ressource Internet désigne aussi bien une page Internet individuelle ou plusieurs pages ainsi qu'un site Internet ou plusieurs sites regroupés selon des traits communs.

Le Contrôle Internet offre les possibilités suivantes :

- Economie du trafic.

  Pour contrôler le trafic le module offre la possibilité de limiter ou interdire le téléchargement des fichiers multimédia et de limiter ou interdire l'accès aux sites Internet sans rapport avec l'activité professionnelle.

- Délimitation de l'accès selon les catégories de contenu des sites Internet.

  Pour minimiser le trafic et les pertes éventuelles dues à abus d'accès, vous pouvez limiter ou interdire l'accès aux sites Internet de catégories spécifiques (par exemple, interdire l'accès aux sites Internet appartenant à la catégorie "Réseaux sociaux").

- Une gestion centralisée d'accès aux sites Internet.

  Dans le cadre de l'utilisation de Kaspersky Security Center, il est possible de configurer l'accès aux ressources Internet tant pour des individus que pour des groupes.

Toutes les restrictions et les interdictions d'accès aux sites Internet sont réalisées sous forme de règles d'accès aux sites Internet (cf. section "A propos des règles d'accès aux sites Internet" à la page 162) (ci-après règles).

ACTIVATION ET DESACTIVATION DU CONTROLE INTERNET

Le Filtrage du contenu est activé par défaut. Vous pouvez désactiver le Filtrage du contenu le cas échéant.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver le Contrôle Internet, sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Contrôle Internet.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer le Contrôle Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle Internet**, sera modifiée sur l'icône .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver le Contrôle Internet.

     L'icône de l'état du fonctionnement du module , qui s'affiche à gauche dans la ligne **Contrôle Internet**, sera modifiée sur l'icône .

Pour activer ou désactiver le Contrôle Internet depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer le Contrôle Internet** pour activer le Contrôle Internet.
   - Décochez la case **Activer le Contrôle Internet** pour désactiver le Contrôle Internet.

   Si le Contrôle Internet est désactivé, Kaspersky Endpoint Security ne contrôle pas l'accès aux sites Internet.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

A PROPOS DES REGLES D'ACCES AUX SITES INTERNET

La règle d'accès aux ressources Internet est un ensemble de filtres et d'actions que Kaspersky Endpoint Security exécute lorsque les utilisateurs consultent les ressources Internet définies dans la règle à l'heure planifiée indiquée du fonctionnement de la règle. Les filtres permettent de préciser les sites Internet dont l'accès est contrôlé par le Contrôle Internet.

Les filtres suivants sont accessibles :

- **Filtrage selon le contenu**. Le Contrôle Internet organise les ressources en catégories de contenu et en catégories de type de données. Vous pouvez contrôler l'accès des utilisateurs aux sites Internet des catégories de contenu et/ou des catégories de types de données spécifiques. Lorsque les utilisateurs consultent les sites Internet qui appartiennent à la catégorie de contenu sélectionnée et/ou à la catégorie de type de données sélectionnée, Kaspersky Endpoint Security exécute l'action indiquée dans la règle.

- **Filtrage selon les URL des ressources Internet**. Vous pouvez contrôler l'accès des utilisateurs à toutes les adresses des sites Internet ou à certaines adresses des sites Internet/ou à certains groupes d'adresses des sites Internet.

  Si le filtre de contenu et le filtre par les adresses des sites Internet sont activés et les adresses des sites Internet définies et/ou les groupes d'adresses des sites Internet définis appartiennent aux catégories de contenu ou aux catégories de types de données sélectionnées, Kaspersky Endpoint Security ne contrôle pas l'accès à tous les sites Internet des catégories de contenu sélectionnées et/ou des catégories de types de données sélectionnées, mais uniquement aux adresses des sites Internet définies et/ou aux groupes d'adresses des sites Internet.

- **Filtrer par nom d'utilisateur et de groupe d'utilisateurs**. Vous pouvez définir les utilisateurs et/ou les groupes d'utilisateurs pour lesquels l'accès aux sites Internet est contrôlé conformément à la règle.

- **Planification de l'application de la règle**. Vous pouvez planifier l'application de la règle. La planification de l'application de la règle définit le moment où Kaspersky Endpoint Security contrôle l'accès aux ressources Internet indiquées dans la règle.

Après l'installation de l'application Kaspersky Endpoint Security la liste des règles du module Contrôle Internet n'est pas vide. Deux règles sont préinstallées :

- La règle "Scripts et tables de styles" qui autorise tous les utilisateurs à accéder à tout moment à tous les sites dont l'URL contient des fichiers portant l'extension css, js, vbs. Par exemple, http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- La "Règle par défaut" qui autorise tous les utilisateurs à accéder à tous les sites Internet à tout moment.

ACTIONS AVEC LES REGLES D'ACCES AUX SITES INTERNET

Vous pouvez exécuter avec les règles d'accès aux sites Internet les actions suivantes :

- Ajouter une nouvelle règle.

- Modifier la règle.

- Définir la priorité de la règle.

  La priorité d'une règle dépend de la position de la ligne avec une brève description de la règle dans le tableau **Règles d'accès par ordre de priorité** de la fenêtre de configuration du module Contrôle Internet. En d'autres termes, la règle qui se trouve au-dessus des autres règles dans le tableau **Règles d'accès par ordre de priorité** a une priorité supérieure.

Si le site Internet que l'utilisateur essaie d'accéder correspond aux paramètres de plusieurs règles, l'action de Kaspersky Endpoint Security sera définie par la règle avec une priorité plus élevée.

- Vérifier le fonctionnement de la règle.

  Vous pouvez vérifier la cohérence de l'application des règles à l'aide du service "Diagnostic des règles".

- Activer et désactiver la règle.

  La règle d'accès aux sites Internet peut être activée (état *Act*) ou désactivée (état *Désact*). Par défaut, toute règle nouvellement créée est activée (état *Act*). Vous pouvez désactiver la règle.

- Supprimer la règle.

DANS CETTE SECTION

AJOUT ET MODIFICATION DE LA REGLE D'ACCES AUX SITES INTERNET

Pour ajouter ou modifier la règle d'accès aux sites Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Si vous voulez ajouter une règle, cliquez sur le bouton **Ajouter**.
   - Si vous souhaitez modifier une règle, sélectionnez-la dans le tableau **Les règles d'accès par ordre de priorité**, puis cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
4. Définissez ou modifiez les paramètres de la règle. Pour ce faire, procédez comme suit :

   a. Définissez ou modifiez le nom de la règle dans le champ **Nom**.

   b. Sélectionnez l'option requise dans la liste déroulante **Filtrer le contenu** :

      - **Tout contenu**.
      - **Par catégorie**.
      - **Par types de données**.
      - **Par catégories et types de données**.

      Si un élément autre que **Tout contenu** est sélectionné, s'ouvre le groupe de sélection des catégories de contenu et/ou des catégories de type de données. Cochez les cases en regard des noms des catégories de contenu et/ou des catégories de type de données que vous souhaitez.

Si la case en regard du nom de la catégorie de contenu et/ou de la catégorie de type de données, Kaspersky Endpoint Security conformément à la règle contrôle l'accès aux sites Internet qui appartiennent aux catégories de contenu et/ou aux catégories de type de données sélectionnées.

c. Choisissez l'option requise dans la liste déroulante **Appliquer aux adresses** :

- **A toutes les adresses**.
- **Aux adresses spécifiques**.

Si l'élément **Aux adresses spécifiques** est sélectionné, le groupe pour créer la liste des adresses des sites Internet s'ouvre. Vous pouvez créer ou modifier la liste des adresses des sites Internet à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**.

d. Cochez la case **Indiquez les utilisateurs et/ou les groupes** et cliquez sur le bouton **Sélectionner**.

La fenêtre de Microsoft Windows **Sélectionnez Utilisateurs ou Groupes s'ouvre**.

e. Définissez ou modifier la liste des utilisateurs et/ou des groupes d'utilisateurs qui interdit ou limite leur accès aux sites Internet prévus dans la règle.

f. Choisissez l'option requise dans la liste déroulante **Action** :

- **Autoriser**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security autorise l'accès aux sites Internet conformes aux paramètres de la règle.
- **Interdire**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security interdit l'accès aux sites Internet conformes aux paramètres de la règle.
- **Avertir**. Si cette valeur est sélectionnée, Kaspersky Endpoint Security affiche un message d'avertissement sur le caractère éventuellement indésirable du site Internet lorsque l'utilisateur essaie d'accéder aux sites Internet conformes aux paramètres de la règle. Les liens du message d'avertissement permettent à l'utilisateur d'accéder au site Internet demandé.

g. Dans la liste déroulante **Planification de l'application de la règle**, sélectionnez le nom de la planification requise ou créez une autre planification sur la base de votre sélection. Pour ce faire, procédez comme suit :

1. Cliquez sur le bouton **Configuration** en regard de la liste déroulante **Planification de l'application de la règle**.

   La fenêtre **Planification de l'application de la règle** s'ouvre.

2. Pour ajouter à la planification de l'application de la règle un intervalle au cours duquel la règle n'est pas appliquée, cliquez-gauche sur les cellules correspondant aux heures et aux jours voulus de la semaine dans le tableau représentant la planification de l'application de la règle.

   La couleur des cellules deviendra grise.

3. Pour modifier, dans la planification de l'application de la règle, l'intervalle au cours duquel la règle est appliquée en intervalle au cours duquel la règle n'est pas appliquée, cliquez-gauche sur les cellules grises du tableau correspondant aux heures et aux jours voulus de la semaine.

   La couleur des cellules deviendra verte.

4. Cliquez sur le bouton **OK** ou sur **Enregistrer sous** si vous planifiez l'application de la règle sur la base de la règle "Toujours", composée par défaut. Cliquez sur le bouton **Enregistrer sous** si vous planifiez l'application de la règle sur la base d'une planification autre qu'une planification par défaut.

   La fenêtre **Nom de la planification de l'application de la règle** s'ouvre.

5. Saisissez le nom de la planification de l'application de la règle ou gardez le nom proposé par défaut.

6. Cliquez sur le bouton **OK**.

5. Dans la fenêtre **Règle d'accès aux sites Internet**, cliquez **OK**.

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

DEFINITION DE LA PRIORITE DES REGLES D'ACCES AUX SITES INTERNET

Vous pouvez définir la priorité de chaque règle dans la liste des règles en les structurant dans l'ordre spécifique.

Pour définir la priorité des règles d'accès aux sites Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez la règle dont vous souhaitez modifier la priorité.
4. Déplacez la règle en position souhaitée dans la liste des règles à l'aide des boutons **Haut** et **Bas**.
5. Répétez les paragraphes 3 et 4 de l'instruction pour les règles dont la priorité vous souhaitez modifier.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

VERIFICATION DU FONCTIONNEMENT DES REGLES D'ACCES AUX SITES INTERNET

Pour évaluer la coordination des règles du Contrôle Internet, vous pouvez vérifier leur fonctionnement. Pour ce faire, le module Contrôle Internet prévoit le service Diagnostic des règles.

Pour vérifier le fonctionnement des règles d'accès aux sites Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Diagnostic**.

   La fenêtre **Diagnostic des règles** s'ouvre.
4. Remplissez les champs dans le groupe **Conditions** :

   a. Cochez la case **Indiquez l'adresse** pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à un site Internet spécifique. Saisissez l'adresse du site Internet dans le champ ci-dessous.

   b. Définissez la liste des utilisateurs et/ou des groupes d'utilisateurs si vous voulez vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet pour des utilisateurs et/ou des groupes d'utilisateurs spécifiques.

   c. Sélectionnez dans la liste déroulante **Filtrer le contenu** l'élément requis (**Selon les catégories de contenu**, **Selon les types de données** ou **Selon les catégories de contenu et des types de données**) pour vérifier le fonctionnement des règles que Kaspersky Endpoint Security utilise pour contrôler l'accès à des sites Internet avec des catégories de contenu et/ou des catégories de type de données.

   d. Cochez la case **Tenir compte de l'heure de la tentative d'accès** si vous voulez vérifier le fonctionnement des règles en tenant compte du jour de la semaine et de l'heure des tentatives d'accès aux sites Internet indiqués dans les conditions du diagnostic des règles. Indiquez ensuite le jour de la semaine et l'heure.
5. Cliquez sur le bouton **Analyser**.

A l'issue de l'analyse, un message sur l'action de Kaspersky Endpoint Security conformément à la première règle appliquée au moment de l'accès au site Internet défini (autorisation, interdiction, avertissement) sera affiché. La première règle appliquée est celle qui se trouve dans la liste des règles de Contrôle Internet au-dessus des autres règles conformes aux conditions du diagnostic. Le message est affiché à droite du bouton **Analyser**. Le tableau en dessous affiche la liste des autres règles qui se sont déclenchées et le nom de l'action exécutée par Kaspersky Endpoint Security. Les règles sont classées par ordre de priorité décroissante.

ACTIVATION ET DESACTIVATION DE LA REGLE D'ACCES AUX SITES INTERNET

Pour activer ou désactiver la règle d'accès aux sites Internet, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, sélectionnez la règle que vous souhaitez activer ou désactiver.
4. Dans la colonne **Etat**, procédez comme suit :
   - Pour activer l'utilisation de la règle, sélectionnez la valeur *Act*.
   - Pour désactiver l'utilisation de la règle, sélectionnez la valeur *Désact*.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

EXPORTATION ET IMPORTATION DE LA LISTE DES ADRESSES DES SITES INTERNET

Si vous avez créé dans la règle d'accès aux sites Internet une liste des adresses des sites Internet, vous pouvez l'exporter dans un fichier au format TXT. Vous pouvez ensuite importer la liste depuis ce fichier pour ne pas créer manuellement la liste des adresses des sites Internet lors de la configuration de la règle. La fonction de l'exportation et de l'importation de la liste des adresses des sites Internet peut vous être utile si vous créez par exemple les règles aux paramètres similaires.

Pour exporter la liste des adresses des sites Internet dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Sélectionnez la règle dont la liste des adresses des sites Internet vous souhaitez exporter dans un fichier.
4. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
5. Pour exporter uniquement une partie de la liste des adresses des sites Internet, sélectionnez les adresses requises des sites Internet.
6. Cliquez sur le bouton  à droite du champ avec la liste des adresses des sites Internet.

   La fenêtre de confirmation de l'action s'ouvre.

7. Exécutez une des actions suivantes :

   - Pour exporter uniquement les éléments sélectionnés dans liste des adresses des sites Internet, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Oui**.
   - Pour exporter tous les éléments sélectionnés dans liste des adresses des sites Internet, cliquez dans la fenêtre de confirmation de l'action sur le bouton **Non**.

     La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvrira.

8. Dans la fenêtre de Microsoft Windows **Enregistrer sous**, sélectionnez le fichier où vous souhaitez exporter la liste des adresses des sites Internet, puis cliquez sur le bouton **Enregistrer**.

Pour importer dans la règle la liste des adresses des sites Internet depuis un fichier, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :

   - Cliquez sur le bouton **Ajouter** pour créer une nouvelle règle d'accès aux sites Internet.
   - Sélectionnez la règle d'accès aux sites Internet que vous souhaitez modifier. Cliquez sur le bouton **Modifier**.

   La fenêtre **Règle d'accès aux sites Internet** s'ouvre.
4. Exécutez une des actions suivantes :

   - Pour créer une nouvelle règle d'accès aux sites Internet, sélectionnez dans la liste déroulante **Appliquer aux adresses** l'élément **Aux adresses spécifiques**.
   - Si vous modifiez la règle d'accès aux sites Internet, passez au paragraphe 5 de l'instruction.
5. Cliquez sur le bouton  à droite du champ avec la liste des adresses des sites Internet.

   Si vous créez une nouvelle règle la fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.

   Si vous modifiez la règle, la fenêtre de confirmation de l'action s'ouvre.
6. Exécutez une des actions suivantes :

   - Si vous créez une nouvelle règle d'accès aux sites Internet, passez au paragraphe 7 de l'instruction.
   - Si vous modifiez la règle d'accès aux sites Internet, dans la fenêtre de confirmation de l'action exécutez une des actions suivantes :

     - Pour ajouter aux éléments existants les éléments importés de la liste des adresses des sites Internet, cliquez sur le bouton **Oui**.
     - Pour supprimer les éléments existants de la liste des adresses des sites Internet et ajouter les éléments importés, cliquez sur le bouton **Non**.

   La fenêtre standard de Microsoft Windows **Ouvrir le fichier** s'ouvre.
7. Sélectionnez dans la fenêtre de Microsoft Windows **Ouvrir le fichier** le fichier avec la liste des adresses des sites Internet à importer.
8. Cliquez sur le bouton **Ouvrir**.
9. Dans la fenêtre **Règle d'accès aux sites Internet**, cliquez **OK**.

REGLES DE CREATION DE MASQUES D'ADRESSES DES SITES INTERNET

Le *masque d'adresse du site Internet* (ci-après également "masque d'adresse") peut vous être utile lorsque vous devez saisir une multitude d'adresses de sites Internet similaires lorsque vous créez une règle d'accès aux sites Internet. Un seul masque correct peut se substituer à une multitude d'adresses des sites Internet.

Pour créer un masque d'adresse, il faut prendre en considération les règles suivantes :

1. Le caractère `*` remplace n'importe quelle séquence de caractères dont le nombre de caractères est zéro ou plus.

   Par exemple, lors de la saisie du masque d'adresse *abc* la règle d'accès aux sites Internet s'applique à toutes les adresses qui contiennent la séquence abc. Exemple : http://www.example.com/page_0-9abcdef.html.

   Le caractère `?` est l'équivalent au point d'interrogation et pas à n'importe quel caractère ce qui est typique pour les règles de création des masques d'adresses dans le module Antivirus Internet.

   Pour ajouter le caractère `*` au masque d'adresse, vous devez saisir deux caractères `*`, et non pas la séquence `\*` ce que prévoient les règles de création des masques d'adresses dans le module Antivirus Internet.

2. La séquence de caractères `www.` dans le début du masque d'adresse est équivalente à la séquence `*.`.

   Exemple : le masque d'adresse www.example.com est équivalent à *.example.com.

3. Si le masque d'adresse commence par un caractère autre que `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `*.`.

4. La séquence des caractères `*.` dans le début du masque est équivalente à la séquence `*.` ou à une ligne vide.

   Exemple : le masque d'adresse http://www.*.example.com couvre l'adresse http://www2.example.com.

5. Si le masque d'adresses se termine par le caractère différent de `/` ou `*`, le contenu du masque d'adresse est équivalent au même contenu avec le préfixe `/*`.

   Exemple : le masque d'adresse http://www.example.com couvre les adresses du type http://www.example.com/abc, où a, b, c sont n'importe quels caractères.

6. Si le masque d'adresse se termine par le caractère `/`, le contenu du masque d'adresse est équivalent au même contenu avec le suffixe `*.`

7. La séquence des caractères `/*` à la fin du masque d'adresse est traitée comme `/*` ou comme la ligne vide.

8. La vérification des adresses des sites Internet par masque d'adresse est effectuée compte tenu du schéma (http ou https) :

   - S'il n'y a pas de protocole réseau dans le masque d'adresse, ce masque d'adresse couvre l'adresse avec n'importe quel protocole réseau.

     Exemple : le masque d'adresse example.com couvre les adresses http://example.com et https://example.com.

   - S'il y a un protocole réseau dans le masque d'adresse, ce masque d'adresse couvre uniquement les adresses avec le protocole réseau identique à celui du masque d'adresse.

     Exemple : le masque d'adresse http://*.example.com couvre l'adresse http://www.example.com et ne couvre pas l'adresse https://www.example.com.

9. Le masque d'adresse dans les guillemets doubles est interprété sans aucune permutation supplémentaire, sauf le caractère * s'il faisait partie du masque d'adresse d'origine. Cela veut dire que pour ces masques d'adresses les règles 5 et 7 ne sont pas appliquées.

10. Lors de la comparaison au masque d'adresse du site Internet ne sont pas pris en compte le nom d'utilisateur et le mot de passe, le port de connexion et le registre de caractères.

Tableau 3. Exemples d'application des règles de création de masques d'adresses

N°	MASQUE D'ADRESSE	ADRESSE DU SITE INTERNET ANALYSEE	EST-CE QUE L'ADRESSE ANALYSEE SATISFAIT AU MASQUE D'ADRESSE	COMMENTAIRES
1	*.example.com	http://www.123example.com	Non	Cf. règle 1.
2	*.example.com	http://www.123.example.com	Oui	Cf. règle 1.
3	*example.com	http://www.123example.com	Oui	Cf. règle 1.
4	*example.com	http://www.123.example.com	Oui	Cf. règle 1.
5	http://www.*.example.com	http://www.123example.com	Non	Cf. règle 1.
6	www.example.com	http://www.example.com	Oui	Cf. règles 2, 1.
7	www.example.com	https://www.example.com	Oui	Cf. règles 2, 1.
8	http://www.*.example.com	http://123.example.com	Oui	Cf. règles 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Oui	Cf. règles 2, 5, 1.
10	example.com	http://www.example.com	Oui	Cf. règles 3, 1.
11	http://example.com	http://example.com/abc	Oui	Cf. règles 6.
12	http://example.com/*	http://example.com	Oui	Cf. règles 7.
13	http://example.com	https://example.com	Non	Cf. règle 8.
14	"example.com"	http://www.example.com	Non	Cf. règle 9.
15	"http://www.example.com"	http://www.example.com/abc	Non	Cf. règle 9.
16	"*.example.com"	http://www.example.com	Oui	Cf. règles 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Oui	Cf. règles 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Oui	Cf. règles 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Non	Le masque d'adresse contient plus d'informations que l'adresse du site Internet

MODIFICATION DES MODELES DES MESSAGES DU CONTROLE INTERNET

En fonction de l'action définie dans les propriétés des règles du Contrôle Internet, lorsque les utilisateurs essaient d'accéder aux sites Internet Kaspersky Endpoint Security affiche un message (en remplaçant la réponse du serveur HTTP par une page HTML avec le message) d'un des types suivants :

- **Message d'avertissement**. Ce message avertit sur le danger éventuel du site Internet et/ou sur la non-conformité à la stratégie d'entreprise. Kaspersky Endpoint Security affiche le message d'avertissement si dans les propriétés de la règle qui décrit ce site Internet dans la liste déroulante **Action** l'élément **Avertir** est sélectionné.

  Si vous croyez recevoir ce message d'avertissement par erreur, en cliquant sur le lien dans le corps du message d'avertissement vous pouvez ouvrir un message de réclamation destiné à l'administrateur du réseau local d'entreprise.

- **Message de blocage du site Internet**. Kaspersky Endpoint Security affiche le message de blocage du site Internet, si dans les propriétés de la règle qui décrit ce site Internet dans la liste déroulante **Action** l'élément **Interdire** est sélectionné.

  Si vous croyez que l'accès au site Internet a été bloqué par erreur, cliquez sur le lien dans le corps du message de blocage du site Internet pour ouvrir un message de réclamation destiné à l'administrateur du réseau local d'entreprise.

Il existe des modèles spécifiques de message d'avertissement et de message de réclamation destinés à l'administrateur du réseau local d'entreprise. Vous pouvez modifier leur contenu.

Pour modifier le modèle de message de Filtrage du contenu, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Contrôle Internet**.

   Les paramètres du module Contrôle Internet s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Modèles**.

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

   - Si vous souhaitez modifier le modèle du message d'avertissement sur le danger éventuel du site Internet, sélectionnez l'onglet **Avertissement**.
   - Si vous souhaitez modifier le modèle du message de blocage d'accès au site Internet, sélectionnez l'onglet **Blocage**.
   - Si vous souhaitez modifier le modèle du message de réclamation, sélectionnez l'onglet **Réclamation**.
5. Modifier le modèle de message. Pour ce faire, utilisez les boutons **Par défaut** et **Variables**.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MISE A JOUR DES SIGNATURES DES MENACES ET DES MODULES DU PROGRAMME

Cette section contient des informations sur la mise à jour des bases et des modules de l'application (ci-après mises à jour) et les instructions sur la configuration des paramètres de la mise à jour.

DANS CETTE SECTION

A PROPOS DE LA MISE A JOUR DES BASES ET DES MODULES DE L'APPLICATION

La mise à jour des bases et des modules de l'application Kaspersky Endpoint Security préserve l'actualité de la protection de l'ordinateur. Chaque jour, de nouveaux virus, et autres applications présentant une menace apparaissent dans le monde. Les bases de Kaspersky Endpoint Security contiennent les données relatives aux menaces et les méthodes de neutralisation. Pour détecter de nouvelles menaces dans les plus brefs délais, il vous faut régulièrement mettre à jour les bases et les modules de l'application.

La mise à jour régulière requiert une licence d'utilisation de l'application valide. En l'absence d'une telle licence, vous ne pourrez réaliser la mise à jour qu'une seule fois.

Les serveurs de mise à jour de Kaspersky Lab sont la principale source de mise à jour pour Kaspersky Endpoint Security.

Pour réussir le téléchargement du paquet de mise à jour depuis les serveurs de mise à jour de Kaspersky Lab, l'ordinateur doit être connecté à l'Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si vous utilisez un serveur proxy, il faudra configurer les paramètres du serveur proxy.

Lors de la mise à jour, les objets suivants sont téléchargés et installés sur votre ordinateur :

- **Les bases de Kaspersky Endpoint Security**. La protection de l'ordinateur est garantie par l'utilisation de bases de données qui contiennent les signatures des menaces et 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 nouvelles menaces et les moyens de lutter contre celles-ci. Pour cette raison, il est recommandé d'actualiser régulièrement les bases.

  En plus des bases de Kaspersky Endpoint Security, la mise à jour concerne également les pilotes de réseau qui assurent l'interception du trafic de réseau par les modules de la protection.

- **Les modules de l'application**. Outre les bases de Kaspersky Internet Security, il est possible d'actualiser les modules de l'application. Les mises à jour des modules de l'application permettent de supprimer les vulnérabilités de Kaspersky Internet 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 relatives à l'état actuel des bases de Kaspersky Endpoint Security apparaissent dans la section **Mise à jour** du groupe **Gestion des tâches** sous l'onglet **Centre de gestion** de la fenêtre principale de l'application.

Les informations relatives aux résultats de la mise à jour et à tous les événements survenus pendant l'exécution des tâches sont consignées dans le rapport de Kaspersky Endpoint Security (cf. section "Utilisation des rapports" à la page 208).

A PROPOS DES SOURCES DE MISES A JOUR

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules de l'application de Kaspersky Endpoint Security.

La source de mises à jour peut être un serveur FTP, HTTP (par exemple, Kaspersky Security Center, les serveurs des mises à jour de Kaspersky Lab), un dossier local ou de réseau.

Si vous ne pouvez pas accéder aux serveurs de mises à jour de Kaspersky Lab (par exemple, votre accès à Internet est limité), vous pouvez contacter le siège social de Kaspersky Lab afin d'obtenir les adresses des partenaires de Kaspersky Lab (http://www.kaspersky.com/fr/). Les partenaires de Kaspersky Lab vous transmettront les mises à jour sur disque amovible.

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir les mises à jour des modules de l'application.

VOIR EGALEMENT

CONFIGURATION DE LA MISE A JOUR

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres de la mise à jour :

- Ajouter de nouvelles sources des mises à jour.

  La liste des sources des mises à jour contient par défaut le serveur Kaspersky Security Center et les serveurs des mises à jour de Kaspersky Lab. Vous pouvez ajouter d'autres sources des mises à jour à la liste. Vous pouvez indiquer en tant que sources des mises à jour les serveurs HTTP ou FTP, ainsi que les dossiers partagés.

  Si plusieurs ressources ont été sélectionnées en tant que sources des mises à jour, Kaspersky Endpoint Security les consultera pendant la mise à jour dans l'ordre de la liste et exécute la tâche de mise à jour en utilisant le paquet de mise à jour de la première source de mise à jour disponible.

  Si vous avez sélectionné en tant que source des mises à jour une ressource située hors de l'intranet, vous devrez être connecté à Internet pour effectuer la mise à jour.

- Sélectionnez la région du serveur de mises à jour de Kaspersky Lab.

  Si vous utilisez les serveurs de Kaspersky Lab en tant que source des mises à jour, vous pouvez sélectionner le serveur de mises à jour de Kaspersky Lab pour télécharger le paquet de mise à jour en fonction de sa situation géographique. Serveurs de mise à jour de Kaspersky Lab sont répartis dans plusieurs pays. En utilisant le serveur de mises à jour de Kaspersky Lab le plus proche, vous pouvez réduire la durée nécessaire à la récupération des mises à jour.

  Par défaut, les paramètres de la mise à jour utilisent les informations géographiques reprises dans le registre du système d'exploitation.

- Configurer la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé.

  Afin d'économiser le trafic Internet, vous pouvez configurer la mise à jour de Kaspersky Endpoint Security sur les ordinateurs du réseau local d'entreprise depuis un répertoire partagé. Pour ce faire, un des ordinateurs du réseau local d'entreprise récupère le dernier paquet de mise à jour depuis le serveur de Kaspersky Security Center ou les serveurs des mises à jour de Kaspersky Lab et copie le paquet de mise à jour dans le dossier partagé. Après, tous les autres ordinateurs du réseau local d'entreprise pourront télécharger le paquet de mise à jour depuis le dossier partagé.

- Sélectionner le mode de lancement de la tâche de mise à jour.

  Si l'exécution de la tâche est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche ignorée dès que cela est possible.

  Vous pouvez reporter le lancement de la tâche de mise à jour par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche de mise à jour **Selon la programmation** et l'heure de lancement de Kaspersky Endpoint Security est le même que l'heure programmée pour le lancement de la tâche de mise à jour. La tâche de mise à jour ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

- Configurer le lancement de la tâche de mise à jour avec les droits d'un autre utilisateur.

DANS CETTE SECTION

AJOUT D'UNE SOURCE DE MISES A JOUR

Pour ajouter une source de mises à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Mode d'exécution et Source de mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Source**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la source de mises à jour** s'ouvre.
5. Dans la fenêtre **Sélection de la source de mises à jour**, sélectionnez le dossier avec le paquet des mises à jour ou saisissez le chemin complet du dossier dans le champ **Source**.
6. Cliquez sur le bouton **OK**.
7. Dans la fenêtre **Mise à jour**, cliquez sur **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

VOIR EGALEMENT

SELECTION DE LA REGION DU SERVEUR DE MISES A JOUR

Pour choisir la région du serveur de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Mode d'exécution et Source de mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Source** dans le groupe **Serveur proxy**, sélectionnez **Choisir dans la liste**.
5. Sélectionnez dans la liste déroulante le pays le plus proche de vous.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

VOIR EGALEMENT

A propos des sources de mises à jour 172

Ajout d'une source de mises à jour 174

Configuration de la mise à jour depuis un dossier partagé..... 176

CONFIGURATION DE LA MISE A JOUR DEPUIS UN DOSSIER PARTAGE

La configuration de la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé comprend les étapes suivantes :

1. Activation du mode de copie du paquet des mises à jour vers un dossier partagé sur un des ordinateurs du réseau local d'entreprise.

2. Configuration de la mise à jour de Kaspersky Endpoint Security de puis le dossier partagé indiqué sur les autres ordinateurs du réseau local d'entreprise.

Pour activer le mode de copie du paquet des mises à jour vers un dossier partagé, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Avancé**, cochez la case **Copier la mise à jour des bases dans le dossier**.

4. Saisissez le chemin d'accès au dossier partagé où sera stocké le paquet des mises à jour récupéré. Vous pouvez le faire d'une des manières suivantes :

   - Saisissez le chemin d'accès au dossier partagé dans le champ au-dessous de la case **Copier la mise à jour des bases dans le dossier**.

   - Cliquez sur le bouton **Parcourir**. Ensuite sélectionnez le dossier requis dans la fenêtre **Sélectionner un dossier** qui s'ouvre et cliquez sur **OK**.

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

Pour configurer la mise à jour de Kaspersky Endpoint Security depuis un dossier partagé, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Mode d'exécution et Source de mises à jour**, cliquez sur le bouton **Source des mises à jour**.

   L'onglet **Source** de la fenêtre **Mise à jour** s'ouvre.

4. Sous l'onglet **Source**, cliquez sur le bouton **Ajouter**.

   La fenêtre **Sélection de la source de mises à jour** s'ouvre.

5. Sélectionnez dans la fenêtre **Sélection de la source de mises à jour** le dossier partagé avec le paquet des mises à jour ou saisissez le chemin d'accès complet au dossier partagé dans le champ **Source**.

6. Cliquez sur le bouton **OK**.

7. Sous l'onglet **Source**, décochez les cases en regard des noms des sources de mises à jour qui ne sont pas le dossier partagé que vous avez indiqué.

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

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

VOIR EGALEMENT

SELECTION DU MODE DE LANCEMENT DE LA TACHE DE MISE A JOUR

Pour programmer l'exécution de la tâche de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Mise à jour** s'ouvre.
4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche de mise à jour :

   - Sélectionnez l'option **Automatique**, si vous souhaitez que Kaspersky Endpoint Security lance la tâche de mise à jour en fonction de la présence du paquet des mises à jour dans la source de mise à jour. L'intervalle de vérification de la présence du paquet des mises à jour par Kaspersky Endpoint Security est augmenté en cas d'épidémie et réduit en situation normale.
   - Sélectionnez l'option **Manuel** pour lancer la tâche de mise à jour manuellement.
   - Sélectionnez l'option **Selon la programmation** pour programmer l'exécution de la tâche de mise à jour.
5. Exécutez une des actions suivantes :

   - Si vous avez sélectionné l'option **Automatique** ou **Manuel**, passez au paragraphe 6 de l'instruction.
   - Si vous avez sélectionné l'option **Selon la programmation**, définissez les paramètres de programmation du lancement de la tâche de mise à jour. Pour ce faire, procédez comme suit :

     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche de mise à jour. Sélectionnez une des options suivantes : **Minutes**, **Heures**, **Jours**, **Chaque semaine**, **Au moment défini**, **Tous les mois**, **Après le lancement de l'application**.

     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche de mise à jour.

     c. Indiquez dans le champ **Intervalle entre le lancement et le démarrage de l'application** le temps qui doit s'écouler avant l'exécution de la tâche de mise à jour après le lancement de Kaspersky Endpoint Security.

     Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application**, le champ **Intervalle entre le lancement et le démarrage de l'application** est inaccessible.

     d. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches de mise à jour non exécutées en temps opportun.

     Si vous avez sélectionné dans la liste déroulante **Fréquence** l'élément **Heures**, **Minutes** ou **Après le lancement de l'application**, la case **Lancer les tâches non exécutées** est inaccessible.

6. Cliquez sur le bouton **OK**.

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

VOIR EGALEMENT

Lancement et arrêt des tâches 178

LANCEMENT DE LA TACHE DE MISE A JOUR AVEC LES DROITS D'UN AUTRE UTILISATEUR

Par défaut, la tâche de mise à jour de Kaspersky Endpoint Security est lancée au nom de l'utilisateur que vous avez utilisé pour ouvrir votre session dans le système d'exploitation. Cependant, la mise à jour de Kaspersky Endpoint Security peut se dérouler depuis une source à laquelle vous n'avez pas accès (par exemple, depuis un dossier partagé contenant le paquet des mises à jour) ou pour laquelle vous ne bénéficiez pas des droits d'utilisateur autorisé du serveur proxy. Vous pouvez indiquer l'utilisateur bénéficiant de ces droits, dans les paramètres de Kaspersky Endpoint Security et lancer la tâche de mise à jour de Kaspersky Endpoint Security au nom de cet utilisateur.

Pour lancer une tâche de mise à jour sous les droits d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.

3. Dans le groupe **Mode d'exécution et Source de mises à jour**, cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Mise à jour** s'ouvre.

4. Sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les droits de l'utilisateur**.

5. Saisissez dans le champ **Nom** le compte utilisateur sous les droits duquel il faut accéder à la source des mises à jour.

6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur sous les droits duquel il faut accéder à la source des mises à jour.

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

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

LANCEMENT ET ARRET DES TACHES

Quel que soit le mode de lancement de la tâche de mise à jour sélectionné, vous pouvez lancer ou arrêter la tâche de mise à jour de Kaspersky Endpoint Security à tout moment.

Le téléchargement du paquet des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab requiert une connexion Internet.

Pour lancer ou arrêter la tâche de recherche de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion des tâches**.

   Le groupe **Gestion des tâches** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec le nom de la tâche de mise à jour.

   Le menu de sélection des actions avec la tâche de mise à jour.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Lancer la mise à jour** pour lancer la tâche de mise à jour.

     L'état de l'exécution de la tâche de mise à jour affiché à droite du bouton **Mise à jour** passera à *En exécution*.
   - Sélectionnez dans le menu l'option **Arrêter la mise à jour** pour arrêter la tâche de mise à jour.

     L'état de l'exécution de la tâche de mise à jour affiché à droite du bouton **Mise à jour** passera à *Arrêté*.

ANNULATION DE LA DERNIERE MISE A JOUR

Après la première mise à jour des bases et des modules de l'application, vous aurez la possibilité de revenir à l'état antérieur à la mise à jour des bases et des modules de l'application.

Chaque fois que l'utilisateur lance la mise à jour, Kaspersky Internet Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Ceci permet de revenir, le cas échéant, à l'utilisation des bases et des modules de l'application antérieurs. La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte qui fait que Kaspersky Endpoint Security bloque une application sans danger.

Pour restaurer la dernière mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion des tâches**.

   Le groupe **Gestion des tâches** se développe.
4. Ouvrez avec le bouton droit de la souris le menu contextuel de la tâche **Mise à jour**.
5. Sélectionnez l'option **Restaurer la mise à jour**.

CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

Pour configurer les paramètres du serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** de la partie gauche de la fenêtre, sélectionnez la section **Mise à jour**.

   Dans la partie droite de la fenêtre seront affichés les paramètres de mise à jour des bases et des modules de l'application.
3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Configuration**.

   L'onglet **Serveur proxy** de la fenêtre **Mise à jour** s'ouvre.
4. Sous l'onglet **Serveur proxy**, cochez la case **Utiliser le serveur proxy**.
5. Définissez les paramètres du serveur proxy.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

Vous pouvez aussi configurer les paramètres du serveur proxy dans le groupe **Paramètres complémentaires** sous l'onglet **Configuration** de la fenêtre principale de l'application.

ACTIVATION ET DESACTIVATION DE L'ANALYSE DES FICHIERS EN QUARANTAINE APRES LA MISE A JOUR

Si l'analyse du fichier de Kaspersky Endpoint Security découvert des indices de l'infection, mais ne peut pas définir exactement la nature des programmes malveillants qui l'ont infecté, Kaspersky Endpoint Security place ce fichier en quarantaine. Il se peut que la prochaine mise à jour des bases et des modules de l'application permette à Kaspersky Endpoint Security de détecter catégoriquement la menace et de la supprimer. Vous pouvez activer l'analyse automatique des fichiers en quarantaine après chaque mise à jour des bases et des modules d'application.

Il est recommandé d'analyser périodiquement les fichiers en quarantaine. Leur statut peut changer après l'analyse. Certains fichiers peuvent ainsi être réparés et restaurés dans leur emplacement d'origine et vous pouvez continuer à les utiliser.

Pour activer ou désactiver l'analyse des objets en quarantaine après la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

   Les paramètres de gestion des rapports et des stockages seront affichés dans la partie droite de la fenêtre.
3. Dans le groupe **Paramètres de la quarantaine locale et de la sauvegarde**, exécutez une des actions suivantes :

   - Cochez la case **Analyser les fichiers en quarantaine après une mise à jour** pour activer l'analyse des fichiers en quarantaine après chaque mise à jour de Kaspersky Endpoint Security.
   - Décochez la case **Analyser les fichiers en quarantaine après une mise à jour** pour désactiver l'analyse des fichiers en quarantaine après chaque mise à jour de Kaspersky Endpoint Security.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ANALYSE DE L'ORDINATEUR

La recherche de virus et d'autres applications présentant une menace est un facteur décisif pour assurer la protection de l'ordinateur. Il est indispensable d'effectuer la recherche de virus et d'autres applications présentant une menace pour votre ordinateur à intervalle régulier afin d'éviter la propagation d'applications malveillantes qui n'auraient pas été découvertes par les modules de la protection, par exemple en raison d'un niveau de protection trop faible ou pour toute autre raison.

Cette section présente les particularités et la configuration des tâches d'analyse, des niveaux de protection et des technologies d'analyse. Elle explique également comment manipuler les fichiers non traités par Kaspersky Endpoint Security lors de la recherche d'éventuels virus et autres programmes présentant un danger potentiel sur l'ordinateur.

DANS CETTE SECTION

A PROPOS DES TACHES D'ANALYSE

Kaspersky Endpoint Security propose les tâches suivantes pour la recherche de virus et d'autres applications présentant une menace :

- **Analyse complète**. Analyse minutieuse de tout le système. Kaspersky Internet Endpoint analyse par défaut les objets suivants :
  - mémoire vive ;
  - objets chargés au démarrage du système d'exploitation ;
  - sauvegarde du système d'exploitation ;
  - tous les disques durs et amovibles.
- **Analyse rapide**. Kaspersky Endpoint Security analyse par défaut les objets chargés au démarrage du système d'exploitation.
- **Analyse personnalisée**. Kaspersky Endpoint Security analyse les objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet de la liste suivante :
  - mémoire vive ;
  - objets chargés au démarrage du système d'exploitation ;
  - sauvegarde du système d'exploitation ;
  - bases de messagerie ;
  - tous les disques durs, disques de réseau et disques amovibles ;
  - n'importe quel fichier sélectionné.

La tâche d'analyse complète et la tâche d'analyse rapide sont des tâches spécifiques. Pour ces tâches, il est déconseillé de modifier la liste des objets à analyser.

Après le lancement des tâches d'analyse, la progression de l'analyse est affichée dans le champ en regard du nom de la tâche d'analyse exécutée dans le groupe **Gestion des tâches** sous l'onglet **Centre de gestion** de la fenêtre principale de Kaspersky Endpoint Security.

Les informations relatives aux résultats de l'analyse et à tous les événements survenus pendant l'exécution des tâches d'analyse sont consignées dans le rapport de Kaspersky Endpoint Security.

LANCEMENT ET ARRET DE LA TACHE D'ANALYSE

Quel que soit le mode de lancement de la tâche d'analyse sélectionné, vous pouvez lancer ou arrêter cette tâche à tout moment.

Pour lancer ou arrêter la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion des tâches**.

   Le groupe **Gestion des tâches** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec le nom de la tâche d'analyse.

   Le menu de sélection des actions pour la tâche d'analyse s'ouvre.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Lancer l'analyse** pour lancer la tâche d'analyse.

     L'état de l'exécution de la tâche d'analyse affiché à droite du bouton avec le nom de la tâche d'analyse passera à *En exécution*.

   - Sélectionnez dans le menu l'option **Arrêter l'analyse** pour arrêter la tâche d'analyse.

     L'état de l'exécution de la tâche d'analyse affiché à droite du bouton avec le nom de la tâche d'analyse passera à *Arrêté*.

CONFIGURATION DES PARAMETRES DES TACHES D'ANALYSE

Pour configurer les paramètres des tâches d'analyse, vous pouvez exécuter les opérations suivantes :

- Modifier le niveau de protection des fichiers.

  Vous pouvez sélectionner un des niveaux de protection prédéfinis pour les fichiers ou personnaliser les paramètres du niveau de protection des fichiers. Après avoir modifié les paramètres du niveau de protection des fichiers, vous pouvez à tout moment revenir aux paramètres recommandés du niveau de protection des fichiers.

- Modifier l'action que Kaspersky Endpoint Security exécute en cas de découverte d'un fichier infecté.

- Créer la zone d'analyse.

  Vous pouvez élargir ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets d'analyse ou en modifiant le type de fichiers à analyser.

- Optimiser l'analyse.

  Vous pouvez optimiser l'analyse des fichiers : réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Endpoint Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés. Vous pouvez également réduire la période d'analyse d'un fichier. A l'issue du temps défini, Kaspersky Endpoint Security exclut le fichier de l'analyse en cours (sauf les archives et les objets qui incluent plusieurs fichiers).

- Configurer l'analyse des fichiers composés.

- Configurer l'utilisation des méthodes d'analyse.

  Kaspersky Endpoint Security utilise l'analyse sur la base de signatures. Pendant l'analyse sur la base de signatures, Kaspersky Endpoint Security compare l'objet trouvé aux signatures des bases de l'application. Conformément aux recommandations des spécialistes de Kaspersky Lab, l'analyse sur la base de signatures est toujours activée.

  Vous pouvez utiliser l'analyse heuristique afin d'augmenter l'efficacité de la protection. Pendant l'analyse heuristique, Kaspersky Endpoint Security analyse l'activité des objets dans le système d'exploitation. L'analyse heuristique permet d'identifier de nouveaux objets malveillants dont les définitions n'ont pas encore été ajoutées aux bases Kaspersky Endpoint Security.

- Configurer l'utilisation des technologies d'analyse.

  Vous pouvez activer les technologies iChecker et iSwift. Les technologies iChecker et iSwift permettent d'optimiser la vitesse de la recherche de virus en excluant les fichiers qui n'ont pas été modifiés depuis la dernière analyse.

- Sélectionner le mode d'exécution des tâches d'analyse.

  Si l'exécution de la tâche d'analyse est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique de la tâche d'analyse ignorée dès que cela est possible.

  Vous pouvez reporter le lancement de la tâche d'analyse par rapport au démarrage de l'application si vous avez sélectionné le mode d'exécution de la tâche d'analyse **Selon la programmation** et l'heure de lancement de Kaspersky Endpoint Security est le même que l'heure programmée pour le lancement de la tâche d'analyse. La tâche d'analyse ne sera lancée qu'à l'issue de la période écoulée après le démarrage de Kaspersky Endpoint Security.

- Configurer le lancement de la tâche d'analyse avec les droits d'un autre utilisateur.

- Configurer les paramètres d'analyse des disques amovibles à la connexion.

DANS CETTE SECTION

MODIFICATION DU NIVEAU DE PROTECTION DES FICHIERS

Kaspersky Endpoint Security utilise de différents ensembles de paramètres pour exécuter les tâches d'analyse. Ces ensembles de paramètres sont appelés *niveaux de protection des fichiers*. Il existe trois niveaux prédéfinis de protection des fichiers : **Elevé**, **Recommandé**, **Faible**. Les paramètres du niveau de protection des fichiers **Recommandé** sont considérés comme optimum, ils sont recommandés par les experts de Kaspersky Lab.

Afin de modifier le niveau de protection des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, exécutez une des actions suivantes :
   - Pour définir un des niveaux prédéfinis de protection des fichiers (**Elevé**, **Recommandé**, **Faible**), sélectionnez-le à l'aide du curseur.
   - Pour personnaliser le niveau de protection des fichiers, cliquez sur le bouton **Configuration** et définissez les paramètres dans la fenêtre avec le nom de la tâche d'analyse qui s'ouvre.

     Une fois que vous avez personnalisé le niveau de protection des fichiers, le nom du niveau de protection des fichiers dans le groupe **Niveau de protection** devient **Autre**.
   - Pour sélectionner le niveau de protection des fichiers **Recommandé**, cliquez sur le bouton **Par défaut**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MODIFICATION DE L'ACTION SUR LES FICHIERS INFECTES

Pour modifier l'action à exécuter sur les fichiers infectés, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Action en cas de découverte d'une menace** sélectionnez l'option requise :
   - **Sélectionner l'action automatiquement**.
   - **Exécuter l'action : Réparer. Supprimer si la réparation est impossible**.
   - **Exécuter l'action : Réparer**.
   - **Exécuter l'action : Supprimer**.
   - **Exécuter l'action : Informer**.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse fait référence à l'emplacement et au type de fichiers (par exemple, tous les disques durs, objets de démarrage, bases de messagerie), analysés par Kaspersky Endpoint Security pendant l'exécution de la tâche d'analyse.

Pour former la zone d'analyse, procédez comme suit :

- Composer la liste des objets à analyser.
- Sélectionnez le type de fichiers à analyser.

Pour composer la liste des objets à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse rapide**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Objet d'analyse**.

   La fenêtre **Objets à analyser** s'ouvre.
4. Dans **Objets à analyser**, exécutez une des actions suivantes :
   - Cliquez sur le bouton **Ajouter**, si vous voulez ajouter un nouvel objet à la liste des objets à analyser.
   - Pour modifier l'emplacement de l'objet, sélectionnez-le dans la liste des objets analysés et cliquez sur le bouton **Modifier**.

   La fenêtre **Sélection de l'objet à analyser** s'ouvre.
   - Pour supprimer un objet de la liste des objets à analyser, sélectionnez l'objet dans la liste des objets à analyser, puis cliquez sur **Supprimer**.

La fenêtre de confirmation de suppression s'ouvrira.

Vous ne pouvez pas supprimer ou modifier les objets ajoutés à la liste des objets à analyser par défaut.

5. Exécutez une des actions suivantes :

   - Pour ajouter un nouvel objet ou modifier l'emplacement de l'objet de la liste des objets à analyser, sélectionnez l'objet dans la fenêtre **Sélection de l'objet à analyser** et cliquez sur le bouton **Ajouter**.

     Tous les objets sélectionnés dans la fenêtre **Sélection de l'objet à analyser** seront affichés dans la liste **Zone de protection** dans la fenêtre **Antivirus Fichiers**.

     Cliquez sur le bouton **OK**.

   - Pour supprimer l'objet, cliquez sur le bouton **Oui** dans la fenêtre de confirmation de suppression.

6. Le cas échéant, répétez les étapes 4 et 5 pour ajouter, modifier l'emplacement ou supprimer les objets de la liste des objets à analyser.

7. Pour exclure l'objet de la liste des objets à analyser, décochez la case en regard de l'objet dans la liste **Zone de protection**. Cet objet ne sera pas analysé pendant l'exécution de la tâche d'analyse tout en restant dans la liste des objets à analyser.

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

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

Pour sélectionner le type de fichiers à analyser, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées**, qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche d'analyse requise : **Analyse complète**, **Analyse rapide**.

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre avec le nom de la tâche d'analyse sélectionnée, sélectionnez l'onglet **Zone d'action**.

5. Sélectionnez dans le groupe **Types de fichiers** le type de fichiers que vous souhaitez analyser pendant l'exécution de la tâche d'analyse :

   - Sélectionnez **Tous les fichiers** pour analyser tous les fichiers.

   - Sélectionnez **Fichiers analysés selon le format** pour analyser les fichiers dont les formats sont plus exposés à l'infection.

   - Sélectionnez **Fichiers analysés selon l'extension** pour analyser les fichiers dont les extensions sont plus exposées à l'infection.

   Au moment de choisir le type d'objet à analyser, il convient de ne pas oublier les éléments suivants :

   - La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple TXT) et son activation ultérieure est relativement faible. Mais il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, les formats EXE, DLL, DOC). Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est assez élevé.

   - Le malfaiteur peut envoyer un virus ou une autre application présentant une menace sur votre ordinateur dans le fichier exécutable en tant que fichier avec un autre nom avec l'extension txt. Si vous avez sélectionné l'analyse des fichiers selon l'extension, ce fichier sera ignoré lors de l'analyse. Si vous avez choisi l'analyse des fichiers selon le format, alors l'Antivirus Fichiers analysera l'en-tête du fichier, quelle que soit l'extension, et identifiera le fichier comme étant au format EXE. Un tel fichier est scrupuleusement analysé sur les virus et sur d'autres applications présentant une menace.

6. Dans la fenêtre avec le nom de la tâche d'analyse, cliquez sur **OK**.

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

OPTIMISATION DE L'ANALYSE DES FICHIERS

Pour optimiser l'analyse des fichiers, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Zone d'action**.

5. Dans le groupe **Optimisation de l'analyse**, procédez comme suit :

   - Cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

   - Cochez la case **Ignorer les objets si l'analyse dure plus de** et définissez la durée d'analyse d'un fichier (en secondes).

6. Cliquez sur le bouton **OK**.

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

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés tels que des archives ou les bases de données est une pratique très répandue. Pour détecter les virus dissimulés et les autres applications présentant une menace de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement de l'analyse. Vous pouvez limites le cercle des fichiers composés analysés pour accélérer l'analyse.

Pour configurer l'analyse des fichiers composés, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Zone d'action**.

5. Sélectionnez dans le groupe **Analyse des fichiers composés** les fichiers composés à analyser : archives, paquets d'installation ou objets OLE incorporés, fichiers au format de messagerie ou fichiers protégés par un mot de passe.

6. Si dans le groupe **Optimisation de l'analyse** la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est décochée, vous pouvez indiquer pour chaque type de fichier composé s'il faut analyser tous les fichiers de ce type ou uniquement les nouveaux fichiers. Pour réaliser la sélection, cliquez sur le lien tous/nouveaux, situé à côté du nom de type du fichier composé. Le lien change de valeur lorsque vous appuyez sur le bouton gauche de la souris.

Si la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés** est cochée, l'application analyse uniquement les nouveaux fichiers.

7. Cliquez sur le bouton **Avancé**.

   La fenêtre **Fichiers composés** s'ouvre.

8. Dans le groupe **Limite selon la taille**, exécutez une des actions suivantes :

   - Si vous ne souhaitez pas décompacter les fichiers composés de grande taille, cochez la case **Ne pas décompacter les fichiers composés de grande taille** et indiquez la valeur requise dans le champ **Taille maximale du fichier**.

   - Si vous souhaitez décompacter les fichiers composés de grande taille, décochez la case **Ne pas décompacter les fichiers composés de grande taille**.

     Un fichier de grande taille est celui dont la taille dépasse la valeur indiquée dans le champ **Taille maximale du fichier**.

   Kaspersky Endpoint Security analyse les fichiers de grande taille extraits des archives que la case **Ne pas décompacter les fichiers composés de grande taille** soit cochée ou non.

9. Cliquez sur le bouton **OK**.

10. Dans la fenêtre avec le nom de la tâche d'analyse, cliquez sur **OK**.

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

SELECTION DES METHODES D'ANALYSE

Pour utiliser les méthodes d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

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

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.

5. Dans le groupe **Méthodes d'analyse**, cochez la case **Analyse heuristique**, si vous souhaitez que l'application utilise l'analyse heuristique pendant l'exécution de la tâche d'analyse. Ensuite, définissez le niveau de spécification de l'analyse heuristique à l'aide du curseur : **superficielle**, **moyenne** ou **minutieuse**.

6. Cliquez sur le bouton **OK**.

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

UTILISATION DES TECHNOLOGIES D'ANALYSE

Pour utiliser des technologies d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.

   La fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
5. Dans le groupe **Technologies d'analyse**, cochez les cases à côté des noms des technologies que vous souhaitez utiliser pendant l'analyse.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

SELECTION DU MODE DE LANCEMENT DE LA TACHE D'ANALYSE

Pour sélectionner le mode d'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre avec le nom de la tâche sélectionnée s'ouvre.
4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche d'analyse :

   - Sélectionnez l'option **Manuel** pour lancer la tâche d'analyse manuellement.
   - Sélectionnez l'option **Selon la programmation**, pour programmer l'exécution de la tâche d'analyse.
5. Exécutez une des actions suivantes :

   - Si vous avez sélectionné l'option **Manuel**, passez au paragraphe 6 de l'instruction.
   - Si vous avez sélectionné l'option **Selon la programmation**, définissez les paramètres de programmation du lancement de la tâche d'analyse. Pour ce faire, procédez comme suit :

     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche d'analyse. Sélectionnez une des options suivantes : **Jours**, **Chaque semaine**, **Au moment défini**, **Tous les mois**, **Après le lancement de l'application**, **Après chaque mise à jour**.

     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche d'analyse.

c. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion les tâches d'analyse non exécutées en temps opportun.

Si dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application** ou **Après chaque mise à jour** est sélectionné, la case **Lancer les tâches non exécutées** est inaccessible.

d. Cochez la case **Suspendre l'analyse si l'écran de veille est inactif et si l'ordinateur est bloqué** si vous souhaitez que Kaspersky Endpoint Security suspende l'analyse lorsque les ressources de l'ordinateur sont occupées. Cette option de programmation de la tâche d'analyse permet d'économiser les ressources pendant l'utilisation de l'ordinateur.

6. Cliquez sur le bouton **OK**.

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

CONFIGURATION DU LANCEMENT DE LA TACHE DE RECHERCHE DE VULNERABILITES AVEC LES DROITS D'UN AUTRE UTILISATEUR

Par défaut, la tâche d'analyse est lancée sous le compte que l'utilisateur a utilisé pour ouvrir la session dans le système d'exploitation. Toutefois, il peut s'avérer parfois nécessaire d'exécuter une tâche d'analyse sous les droits d'un autre utilisateur. Vous pouvez indiquer l'utilisateur bénéficiant de ces droits, dans les paramètres de la tâche d'analyse et lancer la tâche d'analyse au nom de cet utilisateur.

Pour configurer le lancement de la tâche d'analyse avec les droits d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section avec le nom de la tâche requise (**Analyse complète**, **Analyse rapide**, **Analyse personnalisée**).

   Les paramètres de la tâche d'analyse sélectionnée s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre avec le nom de la tâche d'analyse sélectionnée s'ouvre.

4. Sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les droits de l'utilisateur**.

5. Saisissez dans le champ **Nom** le compte utilisateur sous les droits duquel il faut lancer la tâche d'analyse.

6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur sous les droits duquel il faut lancer la tâche d'analyse.

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

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

ANALYSE DES DISQUES AMOVIBLES LORS DE LEUR CONNEXION A L'ORDINATEUR

Ces derniers temps, les programmes malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles sont fort répandus. Kaspersky Endpoint Security prend en charge la recherche de virus et d'autres applications présentant une menace sur les disques amovibles lors de leur connexion à l'ordinateur.

Pour configurer l'analyse des disques amovibles lors de leur connexion à l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Sélectionnez le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre.

   La partie droite de la fenêtre affichera les paramètres généraux des tâches planifiées.
3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez dans la liste déroulante **Actions à la connexion du disque** l'action requise :
   - **Ne pas analyser**.
   - **Analyse complète**.
   - **Analyse rapide**.
4. Cochez la case **Taille maximale** de disque et indiquez dans le champ à côté la valeur en mégaoctets si vous souhaitez que Kaspersky Endpoint Security analyse les disques amovibles dont la taille est inférieure ou égale à la valeur définie.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MANIPULATION DES FICHIERS NON TRAITES

Cette section explique comment manipuler les fichiers infectés que Kaspersky Endpoint Security n'a pas traité lors de la recherche de la présence éventuelle de virus et autres programmes dangereux sur l'ordinateur.

DANS CETTE SECTION

PRESENTATION DES FICHIERS NON TRAITES

Kaspersky Endpoint Security consigne les informations relatives aux fichiers dans lesquels il a découvert une menace active pendant son fonctionnement, mais qu'il n'a pas traités. Ces informations se présentent sous la forme d'événements dans la liste des fichiers non traités.

Un fichier infecté est considéré comme *traité* si Kaspersky Endpoint Security, lors de la recherche de la présence éventuelle de virus et autres programmes dangereux, a réalisé une des opérations suivantes sur le fichier infecté conformément aux paramètres définis de l'application :

- Réparer.
- Supprimer.
- Supprimer si la réparation est impossible.

Un fichier infecté est considéré comme *non traité* si Kaspersky Endpoint Security, lors de la recherche de la présence éventuelle de virus et autres programmes dangereux, n'a réalisé, pour une raison quelconque, aucune action sur le fichier infecté conformément aux paramètres définis de l'application.

Une telle situation peut se présenter dans les cas suivants :

- Le fichier à analyser n'est pas accessible (par exemple, il se trouve sur un disque réseau ou sur un support externe sans droit en écriture).
- Dans le groupe **Action en cas de détection d'une menace** des paramètres de l'application pour les tâches, l'action **Informer** a été sélectionnée et lorsque le message relatif au message infecté s'est affiché, l'utilisateur a choisi l'option **Ignorer**.

Vous pouvez lancer manuellement la tâche d'analyse personnalisée de fichiers depuis la liste des fichiers non traités après la mise à jour des bases et des modules de l'application. Le statut des fichiers peut changer après l'analyse. En fonction du statut, vous pouvez réaliser vous-même les actions requises sur les fichiers.

Par exemple, vous pouvez exécuter les opérations suivantes :

- supprimer les fichiers dont le statut est *Infecté* (cf. section "*Suppression de fichiers dans la liste des fichiers non traités*" à la page 195) ;
- restaurer les fichiers infectés qui contiennent des informations importantes et restaurer des fichiers dont l'état est *Réparé* et *Sain* (cf. section "*Restauration de fichiers au départ de la liste des fichiers non traités*" à la page 194) ;
- placer en quarantaine les fichiers dont l'état est *Potentiellement infecté* (cf. section "*Mise en quarantaine du fichier*" à la page 221).

MANIPULATION DE LA LISTE DES FICHIERS NON TRAITES

La liste des fichiers non traités se présente sous la forme d'un tableau. Chaque ligne du tableau désigne un événement impliquant un fichier non traité (par la suite, désigné également par l'expression "événement relatif à un fichier non traité") et indique le type de menace découverte dans le fichier.

Vous pouvez réaliser les opérations suivantes sur les fichiers non traités au départ de la liste des fichiers non traités :

- consulter la liste des fichiers non traités ;
- analyser les fichiers non traités à l'aide de la version actuelle des bases et des modules de Kaspersky Endpoint Security ;
- restaurer des fichiers de la liste des fichiers non traités vers leurs dossiers d'origine ou vers n'importe quel autre dossier (si le dossier d'origine du fichier n'est pas accessible en écriture) ;
- supprimer des fichiers de la liste des fichiers non traités ;
- ouvrir le dossier d'origine du fichier non traité.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer les événements relatifs aux fichiers non traités selon les valeurs des colonnes ou à l'aide de filtres complexes ;
- utiliser la fonction de recherche d'événements relatifs aux fichiers non traités ;
- trier les événements relatifs aux fichiers non traités ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des fichiers non traités ;
- regrouper les événements relatifs aux fichiers non traités.

Le cas échéant, vous pouvez copier les événements sélectionnés relatifs aux fichiers non traités dans le Presse-papiers.

DANS CETTE SECTION

LANCEMENT DE LA TACHE D'ANALYSE PERSONNALISEE POUR LES FICHIERS NON TRAITES

Vous pouvez lancer manuellement la tâche d'analyse personnalisée de fichiers non traités, par exemple si l'analyse avait été interrompue pour une raison quelconque ou si vous souhaitez que Kaspersky Endpoint Security analyse les fichiers après une nouvelle mise à jour des bases et des modules de l'application.

Pour lancer la tâche d'analyse personnalisée pour les fichiers non traités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockages**, choisissez l'onglet **Objets non traités**.

4. Dans le tableau sous l'onglet **Objets non traités**, sélectionnez un ou plusieurs événements relatifs aux fichiers que vous souhaitez analyser. Pour sélectionner plusieurs événements, utilisez la touche **CTRL**.

5. Lancez la tâche d'analyse personnalisée des fichiers d'une des manières suivantes :

   - Cliquez sur le bouton **Nouvelle analyse**.

   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Nouvelle analyse**.

A l'issue de l'analyse, un message indique le nombre de fichiers analysés et le nombre de menaces détectées.

RESTAURATION DE FICHIERS AU DEPART DE LA LISTE DES FICHIERS NON TRAITES

Le cas échéant, vous pouvez restaurer des fichiers au départ de la liste des fichiers non traités.

Les experts de Kaspersky Lab conseillent de restaurer les fichiers au départ de la liste des fichiers non traités uniquement s'ils possèdent le statut *Sain*.

Pour restaurer des fichiers depuis la liste des fichiers non traités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

3. Dans la fenêtre **Rapports et stockages**, choisissez l'onglet **Objets non traités**.

4. Si vous souhaitez restaurer tous les fichiers, procédez comme suit :

   a. Cliquez-droit n'importe où dans le tableau de l'onglet **Objets non traités** et ouvrez le menu contextuel.

   b. Choisissez l'option **Restaurer tout**.

      Kaspersky Endpoint Security déplace tous les fichiers de la liste des fichiers non traités vers leurs dossiers d'origine, si ces dossiers sont accessibles en écriture.

   c. Si un des dossiers d'origine des fichiers de la liste n'est pas accessible en écriture, une fenêtre standard **Enregistrer sous** de Microsoft Windows s'ouvre. Cette fenêtre permet de désigner le dossier dans lequel il convient d'enregistrer le fichier.

5. Si vous souhaitez restaurer un ou plusieurs fichiers, procédez comme suit :

   a. Dans le tableau de l'onglet **Objets non traités**, sélectionnez un ou plusieurs événements relatifs aux fichiers non traités que vous souhaitez restaurer au départ de la liste. Pour sélectionner plusieurs événements relatifs aux fichiers non traités, mettez-les en évidence en maintenant la touche **CTRL** enfoncée.

   b. Choisissez une des méthodes suivantes pour restaurer les fichiers :

      - Cliquez sur le bouton **Restaurer**.

      - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Restaurer**.

      Kaspersky Endpoint Security déplace les fichiers sélectionnés vers leurs dossiers d'origine, pour autant que ces dossiers soient accessibles en écriture.

   c. Si un des dossiers d'origine des fichiers de la liste n'est pas accessible en écriture, une fenêtre standard **Enregistrer sous** de Microsoft Windows s'ouvre. Cette fenêtre permet de désigner le dossier dans lequel il convient d'enregistrer le fichier.

SUPPRESSION DE FICHIERS DANS LA LISTE DES FICHIERS NON TRAITES

Vous pouvez supprimer un fichier infecté de la liste des fichiers non traités. Avant de supprimer le fichier, Kaspersky Endpoint Security crée une copie de sauvegarde de celui-ci et la place dans le dossier de sauvegarde au cas où il faudrait restaurer le fichier plus tard (cf. section "Restauration de fichiers au départ de la liste des fichiers non traités" à la page 194).

Pour supprimer des fichiers de la liste des fichiers non traités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockages**, choisissez l'onglet **Objets non traités**.
4. Dans le tableau sous l'onglet **Objets non traités**, sélectionnez un ou plusieurs événements relatifs aux fichiers que vous souhaitez supprimer. Pour sélectionner plusieurs événements, utilisez la touche **CTRL**.
5. Choisissez une des méthodes suivantes pour supprimer les fichiers :

   - Cliquez sur le bouton **Supprimer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Supprimer**.

   Kaspersky Endpoint Security crée une copie de sauvegarde de chaque fichier et la place dans le dossier de sauvegarde (cf. section "Présentation de la quarantaine et du dossier de sauvegarde" à la page 218). Ensuite, Kaspersky Endpoint Security supprime les fichiers sélectionnés de la liste des fichiers non traités.

RECHERCHE DE VULNERABILITES

Cette section fournit des informations sur le module Surveillance des vulnérabilités et sur les particularités et la configuration de la tâche de recherche de vulnérabilités. Elle explique également comment utiliser la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la tâche.

DANS CETTE SECTION

A PROPOS DE LA SURVEILLANCE DES VULNERABILITES

Ce module est disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ce module n'est pas disponible si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Le module Surveillance des vulnérabilités recherche en temps réel la présence éventuelle de vulnérabilités dans les applications exécutées sur l'ordinateur ainsi que dans les applications au moment de leur lancement. Si vous utilisez le module Surveillance des vulnérabilités, il n'est pas nécessaire de lancer la tâche de recherche de vulnérabilités. Une telle analyse est particulièrement indiquée si la tâche de recherches de vulnérabilités dans les applications installées sur l'ordinateur de l'utilisateur n'a jamais été réalisée ou n'a pas été réalisée depuis longtemps (cf. section "A propos de la tâche de recherche de vulnérabilités" à la page 198).

ACTIVATION ET DESACTIVATION DE LA SURVEILLANCE DES VULNERABILITES

Le module Surveillance des vulnérabilités est activé par défaut. Le cas échéant, vous pouvez désactiver la Surveillance des vulnérabilités.

Deux méthodes s'offrent à vous pour activer ou désactiver le module :

- sous l'onglet **Centre de gestion** de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 49) ;
- au départ de la fenêtre de configuration de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 51).

Pour activer ou désactiver la Surveillance des vulnérabilités, sous l'onglet Centre de gestion de la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec les informations sur le module Surveillance des vulnérabilités.

   Le menu de sélection des actions avec le module.
5. Exécutez une des actions suivantes :
   - Sélectionnez dans le menu l'option **Activer** si vous voulez activer la Surveillance des vulnérabilités.

     L'icône du statut du fonctionnement du module  , qui s'affiche à gauche dans la ligne **Surveillance des vulnérabilités**, sera modifiée sur l'icône  .
   - Sélectionnez dans le menu l'option **Désactiver** si vous voulez désactiver la Surveillance des vulnérabilités.

     L'icône du statut du fonctionnement du module  , qui s'affiche à gauche dans la ligne **Surveillance des vulnérabilités**, sera modifiée sur l'icône  .

Pour activer ou désactiver la Surveillance des vulnérabilités depuis la fenêtre de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Protection Endpoint** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Surveillance des vulnérabilités**.

   Les paramètres du module Surveillance des vulnérabilités s'afficheront dans la partie droite de la fenêtre.

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

   - Cochez la case **Activer la Surveillance des vulnérabilités** si vous souhaitez que Kaspersky Endpoint Security recherche la présence éventuelle de vulnérabilités dans les applications exécutées sur l'ordinateur ainsi que dans les applications au lancement.

   - Décochez la case **Activer la Surveillance des vulnérabilités** si vous ne souhaitez pas que Kaspersky Endpoint Security recherche la présence éventuelle de vulnérabilités dans les applications exécutées sur l'ordinateur ainsi que dans les applications au lancement.

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

CONSULTATION DES INFORMATIONS RELATIVES AUX VULNERABILITES DANS LES APPLICATIONS EXECUTEES

Le module Surveillance des vulnérabilités propose des informations sur les vulnérabilités des applications exécutées. Ces informations sont disponibles, si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les postes de travail. Ces informations ne sont pas disponibles si Kaspersky Endpoint Security a été installé sur l'ordinateur sous l'administration du système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Pour consulter les informations relatives aux vulnérabilités des applications exécutées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Contrôle du lieu de travail**.

   Le groupe **Contrôle du lieu de travail** se développe.

4. Cliquez sur le bouton **Observateur de l'activité des programmes**.

L'onglet **Observateur de l'activité des programmes** de la fenêtre **Applications** s'ouvre. Le tableau **Observateur de l'activité des programmes** reprend des informations de synthèse sur l'activité des applications exécutées dans le système d'exploitation. Le statut des vulnérabilités des applications lancées défini par le module Surveillance des vulnérabilités apparaît dans la colonne **État de la vulnérabilité**.

A PROPOS DE LA TACHE DE RECHERCHE DE VULNERABILITES

Les vulnérabilités dans le système d'exploitation peuvent être le résultat, par exemple, d'erreurs de programmation ou de planification, de mots de passe faibles, de l'action de programmes malveillants, etc. La recherche de vulnérabilités consiste à étudier le système d'exploitation, à rechercher des anomalies et des corruptions dans les paramètres des applications de la société Microsoft et d'autres éditeurs.

La recherche de vulnérabilités consiste à fonder un diagnostic sur la sécurité du système d'exploitation et à identifier dans les applications les particularités qui pourraient être exploitées par des individus malintentionnés désireux de diffuser des objets malveillants ou d'accéder aux données personnelles.

Une fois que la tâche de recherche de vulnérabilités a été lancée (cf. section "Lancement et arrêt de la tâche de recherche de vulnérabilités" à la page 199), vous pouvez suivre sa progression dans le champ en regard du nom de la tâche **Recherche de vulnérabilités** du groupe **Gestion des tâches** sous l'onglet **Centre de gestion** de la fenêtre principale de Kaspersky Endpoint Security.

Les informations relatives à l'exécution de la tâche de recherche de vulnérabilités sont consignées dans les rapports (cf. section "Utilisation des rapports" à la page 208).

LANCEMENT ET ARRET DE LA TACHE DE RECHERCHE DE VULNERABILITES

Quel que soit le mode d'exécution de la tâche de recherche de vulnérabilités, vous pouvez à tout moment lancer ou arrêter la tâche de recherche de vulnérabilités.

Pour lancer ou arrêter la tâche de recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Choisissez l'onglet **Centre de gestion**.
3. Cliquez avec la souris sur le groupe **Gestion des tâches**.

   Le groupe **Gestion des tâches** se développe.
4. Cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de la ligne avec le nom de la tâche de recherche de vulnérabilités.

   Le menu de sélection des actions pour la tâche de recherche de vulnérabilités s'ouvre.
5. Exécutez une des actions suivantes :

   - Sélectionnez dans le menu l'option **Lancer l'analyse** pour lancer la tâche de recherche de vulnérabilités.

     L'état de l'exécution de la tâche affiché à droite du bouton avec le nom de la tâche de recherche de vulnérabilités passera à *En exécution*.
   - Sélectionnez dans le menu l'option **Arrêter l'analyse** pour arrêter la tâche de recherche de vulnérabilités.

     L'état de l'exécution de la tâche affiché à droite du bouton avec le nom de la tâche de recherche de vulnérabilités passera à *Arrêté*.

CONSTITUTION DE LA ZONE DE RECHERCHE DE VULNERABILITES

La zone de recherche de vulnérabilités désigne l'éditeur du logiciel ou l'emplacement du dossier d'installation du logiciel (par exemple, toutes les applications de la société Microsoft installées dans le dossier Program Files).

Pour constituer la zone de recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Recherche de vulnérabilités**.

   Les paramètres de la tâche de recherche des vulnérabilités s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Objets à analyser**, procédez comme suit :

   a. Cochez la case **Microsoft** si vous souhaitez que Kaspersky Endpoint Security recherche les vulnérabilités dans les applications de la société Microsoft installées sur l'ordinateur de l'utilisateur.

   b. Cochez la case **Autres éditeurs** si vous souhaitez que Kaspersky Endpoint Security recherche les vulnérabilités dans les applications des sociétés autres que Microsoft installées sur l'ordinateur de l'utilisateur.

   c. Cliquez sur le bouton **Zone complémentaire de recherche de vulnérabilités**.

      La fenêtre **Zone de recherche de vulnérabilités** s'ouvre.

d. Composez la zone complémentaire de recherche de vulnérabilités. Pour ce faire, utilisez les boutons **Ajouter** et **Supprimer**.

e. Dans la fenêtre **Zone de recherche de vulnérabilités**, cliquez sur **OK**.

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

SELECTION DU MODE D'EXECUTION DE LA TACHE DE RECHERCHE DE VULNERABILITES

Pour programmer l'exécution de la tâche de recherche des vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Recherche de vulnérabilités**.

   Les paramètres de la tâche de recherche des vulnérabilités s'afficheront dans la partie droite de la fenêtre.

3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Recherche de vulnérabilités** s'ouvre.

4. Dans le groupe **Mode d'exécution**, sélectionnez une des options suivantes du mode d'exécution de la tâche de recherche des vulnérabilités :

   - Sélectionnez l'option **Manuel** pour lancer la tâche de recherche des vulnérabilités manuellement.

   - Sélectionnez l'option **Selon la programmation**, pour programmer l'exécution de la tâche de recherche des vulnérabilités.

5. Exécutez une des actions suivantes :

   - Si vous avez sélectionné l'option **Manuel**, passez au paragraphe 6 de l'instruction.

   - Si vous avez sélectionné l'option **Selon la programmation**, définissez les paramètres de programmation du lancement de la tâche de recherche des vulnérabilités. Pour ce faire, procédez comme suit :

     a. Définissez dans la liste déroulante **Fréquence** l'heure de lancement de la tâche de recherche des vulnérabilités. Sélectionnez une des options suivantes : **Jours**, **Chaque semaine**, **Au moment défini**, **Tous les mois**, **Après le lancement de l'application**, **Après chaque mise à jour**.

     b. En fonction de l'élément sélectionné dans la liste déroulante **Fréquence**, définissez la valeur des paramètres précisant l'heure de lancement de la tâche de recherche des vulnérabilités.

     c. Cochez la case **Lancer les tâches non exécutées**, si vous souhaitez que Kaspersky Endpoint Security lance à la première occasion la tâche de recherche des vulnérabilités non exécutée en temps opportun.

     Si dans la liste déroulante **Fréquence** l'élément **Après le lancement de l'application** ou **Après chaque mise à jour** est sélectionné, la case **Lancer les tâches non exécutées** est inaccessible.

6. Cliquez sur le bouton **OK**.

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

CONFIGURATION DU LANCEMENT DE LA TACHE DE RECHERCHE DE VULNERABILITES AVEC LES DROITS D'UN AUTRE UTILISATEUR

Par défaut, la tâche de recherche de vulnérabilités est lancée sous le compte que l'utilisateur a utilisé pour ouvrir la session dans le système d'exploitation. Toutefois, il peut s'avérer parfois nécessaire d'exécuter la tâche de recherche de vulnérabilités sous les droits d'un autre utilisateur. Vous pouvez indiquer l'utilisateur bénéficiant de ces droits, dans les paramètres de la tâche de recherche de vulnérabilités lancer la tâche de recherche de vulnérabilités au nom de cet utilisateur.

Pour configurer le lancement de la tâche de recherche de vulnérabilités avec les droits d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Tâches planifiées** qui se trouve dans la partie gauche de la fenêtre, sélectionnez la section **Recherche de vulnérabilités**.

   Les paramètres de la tâche de recherche des vulnérabilités s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Mode d'exécution**.

   L'onglet **Mode d'exécution** de la fenêtre **Recherche de vulnérabilités** s'ouvre.
4. Sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les droits de l'utilisateur**.
5. Saisissez dans le champ **Nom** le compte utilisateur sous les droits duquel il faut lancer la recherche de vulnérabilités.
6. Saisissez dans le champ **Mot de passe** le mot de passe de l'utilisateur sous les droits duquel il faut lancer la recherche de vulnérabilités.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

MANIPULATION SUR LES VULNERABILITES DECOUVERTES

Cette section explique comme utiliser la liste des vulnérabilités découvertes par Kaspersky Endpoint Security suite à l'exécution de la tâche de recherche de vulnérabilités.

DANS CETTE SECTION

A PROPOS DES VULNERABILITES

Kaspersky Endpoint Security consigne les informations obtenues dans le cadre de la tâche de recherche des vulnérabilités (cf. section "A propos de la tâche de recherche de vulnérabilités" à la page 198) dans la liste des vulnérabilités. Ces informations contiennent des données relatives à la source de la vulnérabilité, à son niveau d'importance et aux recommandations sur sa correction.

Si l'utilisateur a consulté les vulnérabilités sélectionnées et a exécuté les actions recommandées pour les supprimer, alors Kaspersky Endpoint Security leur attribue statut *Corrigées*.

Si l'utilisateur ne veut pas que la liste des vulnérabilités affiche les enregistrements relatifs à des vulnérabilités quelconques, il peut les masquer. Kaspersky Endpoint Security attribue le statut *Masquées* à ces vulnérabilités.

La liste des vulnérabilités se présente sous la forme d'un tableau. Chaque ligne du tableau contient les informations suivantes :

- Icône indiquant le niveau d'importance de la vulnérabilité. Les niveaux d'importance suivants sont attribués aux vulnérabilités détectées :
  - Icône . **Critique**. Ce niveau désigne les vulnérabilités très dangereuses qui doivent être corrigées sur le champ. Les individus malintentionnés utilisent activement les vulnérabilités de ce groupe pour infecter le système d'exploitation de l'ordinateur ou pour nuire aux données personnelles de l'utilisateur. Les experts de Kaspersky Lab recommandent d'exécuter en temps utiles toutes les actions de ce groupe pour supprimer la menace.
  - Icône . **Important**. Ce niveau désigne les vulnérabilités importantes qui doivent être corrigées à court terme. Aucune utilisation active de ces vulnérabilités n'a encore été enregistrée. Les individus malintentionnés peuvent commencer à utiliser les vulnérabilités de ce groupe pour infecter le système d'exploitation de l'ordinateur ou pour nuire aux données personnelles de l'utilisateur. Les experts de Kaspersky Lab recommandent d'exécuter les actions de ce groupe pour garantir la protection optimale de l'ordinateur et des données personnelles de l'utilisateur.
  - Icône . **Avertissement**. Ce niveau désigne les vulnérabilités dont la correction peut attendre. Les individus malintentionnés ne vont pas exploiter activement les vulnérabilités de cette application pour l'instant, mais il est possible que de telles vulnérabilités mettent la sécurité de l'ordinateur en jeu à l'avenir.
- Le nom de l'application contenant la vulnérabilité.
- Le dossier qui contient le fichier vulnérable.
- Les informations relatives à l'éditeur de l'application, tirées de la signature numérique.
- La solution de Kaspersky Endpoint Security pour corriger la vulnérabilité.

UTILISATION DE LA LISTE DES VULNERABILITES

Vous pouvez réaliser les opérations suivantes au départ de la liste des vulnérabilités :

- consulter la liste des vulnérabilités ;
- lancer une nouvelle recherche de vulnérabilités après la mise à jour des bases et des modules de l'application ;
- consulter les informations détaillées sur les vulnérabilités et les recommandations pour la supprimer dans un groupe distinct ;
- corriger la vulnérabilité ;
- masquer les vulnérabilités sélectionnées dans la liste des vulnérabilités ;
- filtrer la liste des vulnérabilités selon le degré d'importance de celles-ci ;
- filtrer la liste des vulnérabilités selon les statuts de vulnérabilités *Corrigées* et *Masquées*.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer la liste des vulnérabilités selon les valeurs d'une colonne ou selon un filtre complexe ;
- utiliser la fonction de recherche de vulnérabilités ;
- trier les enregistrements dans la liste des vulnérabilités ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des vulnérabilités ;
- regrouper les enregistrements dans la liste des vulnérabilités.

DANS CETTE SECTION

NOUVEAU LANCEMENT DE LA TACHE DE RECHERCHE DE VULNERABILITES

Pour lancer une analyse des vulnérabilités découvertes antérieurement, vous pouvez relancer la tâche de recherche de vulnérabilités. Ceci peut être nécessaire, par exemple si la tâche de recherche de vulnérabilités a été interrompue pour une raison quelconque ou si vous souhaitez que Kaspersky Endpoint Security analyse à nouveau les fichiers après la mise à jour des bases et des modules de l'application (cf. section "A propos de la mise à jour des bases et des modules de l'application" à la page 171).

Pour lancer à nouveau la tâche de recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

3. Dans la fenêtre **Rapports et stockage**s, choisissez l'onglet **Vulnérabilités**.

   L'onglet **Vulnérabilités** contient la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la recherche de vulnérabilités.

4. Cliquez sur le bouton **Nouvelle analyse**.

   Kaspersky Endpoint Security analyse à nouveau toutes les vulnérabilités de la liste.

L'état d'une vulnérabilité supprimée suite à l'installation du correctif proposé ne change pas après la nouvelle recherche de vulnérabilités.

CORRIGER LES VULNERABILITES:

Vous pouvez corriger une vulnérabilité en installant une mise à jour pour le système d'exploitation, en modifiant la configuration de l'application ou en installant le correctif requis pour une application.

Il se peut que les vulnérabilités détectées ne concernent pas les applications installées, mais leurs copies. Le correctif supprime la vulnérabilité uniquement si l'application a été installée.

Pour corriger une vulnérabilité, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

3. Dans la fenêtre **Rapports et stockage**s, choisissez l'onglet **Vulnérabilités**.

   L'onglet **Vulnérabilités** contient la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la recherche de vulnérabilités.

4. Dans la liste des vulnérabilités, sélectionnez l'entrée de la vulnérabilité qui vous intéresse.

   Le groupe **Corriger les vulnérabilités** apparaît dans la partie inférieure de la liste des vulnérabilités. Le groupe reprend les informations relatives à cette vulnérabilité ainsi que les recommandations relatives à sa suppression.

   Pour chacune des vulnérabilités, les informations suivantes sont accessibles :

   - Le nom de l'application contenant la vulnérabilité.
   - La version de l'application contenant la vulnérabilité.
   - La sévérité de la vulnérabilité.
   - L'identificateur de la vulnérabilité.
   - La date et l'heure de la dernière détection de la vulnérabilité.
   - Les recommandations sur la correction de la vulnérabilité (par exemple, un lien vers les mises à jour du système d'exploitation ou vers un correctif pour une application).
   - Un lien vers une page Internet décrivant la vulnérabilité.

5. Si vous souhaitez obtenir une description détaillée de cette vulnérabilité, cliquez sur le lien **Informations complémentaires** afin d'ouvrir une page Internet décrivant la menace liée à la vulnérabilité sélectionnée. Le site www.secunia.com http://www.secunia.com permet de télécharger la mise à jour requise pour la version actuelle de l'application.

6. Sélectionnez un des modes suivants de correction de la vulnérabilité :

   - S'il existe un ou plusieurs correctifs pour l'application, suivez les instructions fournies à côté du nom du correctif pour installer celui-ci.

   - S'il existe une mise à jour pour le système d'exploitation, suivez les instructions indiquées à côté du nom de la mise à jour requise pour l'installer.

     La vulnérabilité est supprimée après l'installation du correctif ou de la mise à jour. Kaspersky Endpoint Security attribue à la vulnérabilité un statut qui signifie que la vulnérabilité a été corrigée. L'icône ✓ apparaît sur la ligne à côté du nom de l'application. L'entrée relative à la vulnérabilité corrigée apparaît en gris dans la liste des vulnérabilités.

7. Si le groupe **Corriger les vulnérabilités** ne propose aucune information sur la correction de la vulnérabilité, vous pouvez lancer à nouveau la recherche de vulnérabilités après la mise à jour des bases et des modules de Kaspersky Endpoint Security. Dans la mesure où Kaspersky Endpoint Security recherche la présence éventuelle de vulnérabilités à l'aide d'une base de données de vulnérabilités, il se peut que des informations relatives à la suppression d'une vulnérabilité particulière soient disponibles après la mise à jour de l'application.

DISSIMULATION DES ENTREES DANS LA LISTE DES VULNERABILITES

Vous pouvez masquer une entrée sélectionnée relative à une vulnérabilité. Kaspersky Endpoint Security attribue l'état *Masquées* aux entrées que vous avez sélectionnées dans la liste des vulnérabilités et marquées comme masquées. Ensuite, vous pouvez filtrer la liste des vulnérabilités selon l'état *Masquées* (cf. section "*Filtrage de la liste des vulnérabilités en fonction du statut Corrigées et Masquées*" à la page 206).

Pour masquer une entrée dans la liste des vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

3. Dans la fenêtre **Rapports et stockage**s, choisissez l'onglet **Vulnérabilités**.

   L'onglet **Vulnérabilités** contient la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la recherche de vulnérabilités.

4. Dans la liste des vulnérabilités, sélectionnez l'entrée de la vulnérabilité qui vous intéresse.

   Le groupe **Corriger les vulnérabilités** apparaît dans la partie inférieure de la liste des vulnérabilités. Le groupe reprend les informations relatives à cette vulnérabilité ainsi que les recommandations relatives à sa suppression.

5. Cliquez sur le bouton **Masquer**.

   Kaspersky Endpoint Security attribue le statut *Masquée* à la vulnérabilité sélectionnée.

   Si la case **Masquées** est sélectionnée, l'entrée sélectionnée relative à la vulnérabilité est déplacée vers la fin de la liste des vulnérabilités et est mise en évidence en gris.

   Si la case **Masquées** est décochée, l'entrée sélectionnée n'apparaît pas dans la liste des vulnérabilités.

FILTRAGE DE LA LISTE DES VULNERABILITES EN FONCTION DU NIVEAU D'IMPORTANCE DE LA VULNERABILITE

Pour filtrer la liste des vulnérabilités en fonction du niveau d'importance des vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockage**s, choisissez l'onglet **Vulnérabilités**.

   L'onglet **Vulnérabilités** contient la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la recherche de vulnérabilités.
4. Des icônes représentant le niveau d'importance d'une vulnérabilité apparaissent à côté du paramètre **Afficher l'importance**. Filtrez la liste des vulnérabilités en fonction du niveau d'importance de celles-ci à l'aide d'une des méthodes suivantes :

   - Mettez l'icône en évidence si vous souhaitez que tous les enregistrements du même niveau d'importance apparaissent dans la liste des vulnérabilités.
   - Annulez la mise en évidence des icônes si vous souhaitez que les enregistrements de ce niveau d'importance n'apparaissent pas dans la liste des vulnérabilités.

Les enregistrements relatifs aux vulnérabilités du niveau d'importance indiqué apparaissent dans la liste des vulnérabilités. Les conditions du filtrage des enregistrements que vous avez définies dans la liste des vulnérabilités ne sont pas enregistrées après que vous avez fermé la fenêtre **Rapports et stockages**.

FILTRAGE DE LA LISTE DES VULNERABILITES EN FONCTION DU STATUT CORRIGEES ET MASQUEES

Pour filtrer le contenu de la liste des vulnérabilités en fonction du statut Corrigées ou Masquées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockage**s, choisissez l'onglet **Vulnérabilités**.

   L'onglet **Vulnérabilités** contient la liste des vulnérabilités détectées par Kaspersky Endpoint Security suite à l'exécution de la recherche de vulnérabilités.
4. Les icônes indiquant le statut des vulnérabilités sont affichées à côté du paramètre **Afficher les vulnérabilités**. Pour filtrer la liste des vulnérabilités selon le statut *Corrigées*, réalisez une des opérations suivantes :

   - Cochez la case **Corrigées** si vous souhaitez que la liste des vulnérabilités affiche les enregistrements relatifs aux vulnérabilités corrigées. Pour les enregistrements relatifs aux vulnérabilités corrigées, l'icône ✓ apparaît à côté du nom de l'application au lieu de l'icône du niveau d'importance. Les enregistrements relatifs aux vulnérabilités corrigées sont affichés dans la liste des vulnérabilités en gris.
   - Décochez la case **Corrigées** si vous ne souhaitez pas que la liste des vulnérabilités affiche les enregistrements relatifs aux vulnérabilités corrigées.

5. Pour filtrer la liste des vulnérabilités selon le statut *Masquées*, réalisez une des opérations suivantes :

   - Cochez la case **Masquées** si vous ne souhaitez pas que la liste des vulnérabilités affiche les enregistrements relatifs aux vulnérabilités masquées. Les enregistrements relatifs aux vulnérabilités masquées sont affichés dans la liste des vulnérabilités en gris.

   - Décochez la case **Masquées** si vous ne souhaitez pas que la liste des vulnérabilités affiche les enregistrements relatifs aux vulnérabilités masquées.

Les conditions du filtrage des événements que vous avez définies dans la liste des vulnérabilités ne sont pas enregistrées après que vous avez fermé la fenêtre **Rapports et stockages**.

UTILISATION DES RAPPORTS

Cette section explique comment utiliser les rapports et en configurer les paramètres.

DANS CETTE SECTION

PRINCIPES D'UTILISATION DES RAPPORTS

Les informations relatives au fonctionnement de chaque module de Kaspersky Endpoint Security, à l'exécution de chaque tâche d'analyse, de mise à jour, de recherche des vulnérabilités et au fonctionnement de l'application dans son ensemble sont consignées dans un rapport.

Les données du rapport se présentent sous la forme d'un tableau qui reprend la liste des événements. Chaque ligne du tableau contient des informations sur un événement en particulier. Les attributs de l'événement sont repris dans les colonnes du tableau. Certaines colonnes sont complexes et contiennent des sous-colonnes avec des attributs complémentaires. Les attributs varient en fonction des événements enregistrés lors du fonctionnement de divers modules ou tâches.

Il est possible de composer les types de rapports suivants :

- Rapport "Audit système". Ce rapport contient les informations relatives aux événements survenus pendant l'interaction de l'utilisateur avec l'application, ainsi que pendant le fonctionnement de l'application dans son ensemble sans rapport avec un module ou une tâche particuliers de Kaspersky Endpoint Security.
- Rapport "Tous les modules de la protection". Ce rapport contient des informations sur les événements survenus pendant le fonctionnement des modules suivants de Kaspersky Endpoint Security :
  - Antivirus Fichiers.
  - Antivirus Courrier.
  - Antivirus Internet.
  - Antivirus IM ("Chat").
  - Surveillance du système.
  - Pare-feu.
  - Protection contre les attaques réseau.

- Rapport sur le fonctionnement d'un module ou d'une tâche de Kaspersky Endpoint Security. Ce rapport contient des informations sur les événements survenus pendant le fonctionnement du module ou de la tâche sélectionné de Kaspersky Endpoint Security.

Les niveaux d'importance suivants sont utilisés pour les événements :

- Icône . **Informations**. Evénement à caractère informatif qui en général ne contient aucune information importante.
- Icône . **Evénements importants**. Événements qui doivent être examinés, car ils reflètent des situations importantes dans le fonctionnement du programme.
- Icône . **Evénements critiques**. Evénements critiques et dysfonctionnements de l'application entraînant des problèmes dans le fonctionnement de Kaspersky Endpoint Security ou des vulnérabilités dans la protection de l'ordinateur.

Pour faciliter l'utilisation des rapports, vous pouvez modifier la représentation des données à l'écran d'une des manières suivantes :

- filtrer la liste des événements selon divers critères ;
- utiliser la fonction de recherche d'un événement en particulier ;
- consulter l'événement sélectionné dans un groupe distinct ;
- trier la liste des événements selon chaque colonne ;
- afficher ou masquer les données groupées ;
- modifier l'ordre et la sélection des colonnes affichées dans le rapport.

Le cas échéant vous pouvez exporter le rapport obtenu dans un fichier texte.

Vous pouvez également supprimer des informations des rapports selon les modules ou les tâches de Kaspersky Endpoint Security regroupés dans le rapport. Kaspersky Endpoint Security supprime toutes les entrées des rapports sélectionnés depuis la plus ancienne jusqu'au début de la suppression.

CONFIGURATION DES PARAMETRES DES RAPPORTS

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres des rapports :

- Configurer la durée maximum de conservation des rapports.

  Par défaut, la durée maximum de conservation des rapports sur les événements détectés par Kaspersky Endpoint Security est de 30 jours. A l'issue de cette période, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens du fichier de rapport. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

- Configurer la taille maximum du fichier de rapport.

  Vous pouvez définir la taille maximum du fichier contenant le rapport. Par défaut, la taille maximum du fichier du rapport est limitée à 1024 Mo. Une fois que le fichier de rapport a atteint sa taille maximum, Kaspersky Endpoint Security supprime automatiquement les enregistrements les plus anciens dans le fichier de rapport jusqu'à ce que sa taille repasse en-dessous de la taille maximum autorisée. Vous pouvez lever la restriction sur la taille du fichier du rapport ou définir une autre valeur.

DANS CETTE SECTION

CONFIGURATION DE LA DUREE MAXIMALE DE CONSERVATION DES RAPPORTS

Pour configurer la durée maximale de conservation des rapports, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre dans le groupe **Paramètres des rapports** exécutez une des actions suivantes :
   - Cochez la case **Conserver les rapports au maximum** si vous souhaitez limiter la durée de conservation des rapports. Dans le champ à droite de la case **Supprimer les rapports après**, indiquez la durée maximale d'enregistrement des rapports. La durée maximum de conservation par défaut des rapports est de 30 jours.
   - Décochez la case **Conserver les rapports au maximum** si vous voulez annuler les restrictions sur la durée de conservation des rapports.

   Par défaut, la restriction de la durée d'enregistrement des rapports est activée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE LA TAILLE MAXIMALE DU FICHIER DE RAPPORT

Pour configurer la taille maximale du fichier de rapport, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.
3. Dans la partie droite de la fenêtre dans le groupe **Paramètres des rapports** exécutez une des actions suivantes :
   - Cochez la case **Taille maximale du fichier** si vous souhaitez établir une limite sur la taille du fichier du rapport. Dans le champ situé à droite de la case **Taille maximale du fichier**, saisissez la taille maximale du fichier du rapport. Par défaut, la limite sur la taille du fichier du rapport est de 1 024 Mo.
   - Décochez la case **Taille maximum du fichier** si vous souhaitez lever la restriction sur la taille du fichier du rapport.

   Par défaut, la limite sur la taille du fichier du rapport est activée.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

COMPOSITION DES RAPPORTS

Pour composer des rapports, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport "Audit système" s'affiche par défaut sous l'onglet **Rapports**.

3. Si vous souhaitez composer le rapport "Tous les modules de la protection", choisissez l'option **Tous les modules de la protection** dans la liste des modules et des tâches située dans la partie gauche de la fenêtre **Rapports et stockages**.

   La partie droite de la fenêtre affichera le rapport "Tous les modules de la protection" qui contient la liste des événements sur le fonctionnement de tous les modules de la protection de Kaspersky Endpoint Security.

4. Si vous souhaitez composer un rapport sur le fonctionnement d'un module ou d'une tâche, sélectionnez celui-ci dans la liste des modules et des tâches située dans la partie gauche de la fenêtre **Rapports et stockage**.

   La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche de Kaspersky Endpoint Security.

Par défaut, les événements dans le rapport sont classés selon l'ordre croissant des valeurs de la colonne **Date événement**.

CONSULTATION DES INFORMATIONS SUR LES EVENEMENTS DU RAPPORT DANS UN GROUPE PARTICULIER

Vous pouvez consulter des informations détaillées sur l'événement du rapport présenté dans le groupe distinct.

Pour consulter les informations relatives à un événement du rapport dans un groupe distinct, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport "Audit système" s'affiche par défaut sous l'onglet **Rapports**. Ce rapport reprend les informations sur les événements enregistrés qui surviennent durant le fonctionnement de l'application dans l'ensemble, ainsi que pendant le processus d'interaction de l'utilisateur avec l'application.

3. Exécutez une des actions suivantes :

   - Si vous voulez composer le rapport "Tous les modules de la protection", sélectionnez l'option **Tous les modules de la protection** dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport "Tous les modules de la protection" qui contient la liste des événements sur le fonctionnement de tous les modules de la protection.

- Si vous voulez composer le rapport sur le fonctionnement du module particulier ou de la tâche, sélectionnez ce module ou cette tâche dans la liste des modules et des tâches.

  La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche.

4. Le cas échéant, utilisez les filtres, la recherche et le tri pour trouver l'événement requis dans le rapport.

5. Sélectionnez l'événement trouvé dans le rapport.

   Un groupe contenant les attributs de cet événement et les informations relatives à son niveau d'importance apparaît dans la partie inférieure de la fenêtre.

ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Le rapport composé peut être enregistré dans le fichier texte au format TXT ou CSV.

Kaspersky Endpoint Security enregistre l'événement dans un rapport de la même manière qu'il est présenté à l'écran, c'est-à-dire avec la même composition et avec la même séquence d'attributs de l'événement.

Pour enregistrer le rapport dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   L'onglet **Rapports** de la fenêtre **Rapports et stockages** apparaît.

   Le rapport "Audit système" s'affiche par défaut sous l'onglet **Rapports**. Ce rapport reprend les informations sur les événements enregistrés qui surviennent durant le fonctionnement de l'application dans l'ensemble, ainsi que pendant le processus d'interaction de l'utilisateur avec l'application.

3. Exécutez une des actions suivantes :

   - Si vous voulez composer le rapport "Tous les modules de la protection", sélectionnez l'option **Tous les modules de la protection** dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport "Tous les modules de la protection" qui contient la liste des événements sur le fonctionnement de tous les modules de la protection.

   - Si vous voulez composer le rapport sur le fonctionnement du module particulier ou de la tâche, sélectionnez ce module ou cette tâche dans la liste des modules et des tâches.

     La partie droite de la fenêtre affichera le rapport qui contient la liste des événements sur le fonctionnement du module sélectionné ou de la tâche.

4. S'il faut, modifiez la présentation des données dans le rapport à l'aide des moyens suivants :

   - filtrage des événements ;
   - recherche d'événements ;
   - modification de l'emplacement des colonnes ;
   - classement des événements.

5. Cliquez sur le bouton **Enregistrer le rapport** situé dans la partie supérieure droite de la fenêtre.

   Un menu contextuel s'ouvre.

6. Dans le menu contextuel, sélectionnez l'encodage requis pour l'enregistrement du fichier : **Enregistrer dans ANSI** ou **Enregistrer dans Unicode**.

   La fenêtre standard de Microsoft Windows **Enregistrer sous** s'ouvrira.

7. Dans la fenêtre ouverte **Enregistrer sous**, saisissez le champ dans lequel vous voulez enregistrer le fichier de rapport.

8. Saisissez le nom du fichier du rapport dans le champ **Nom du fichier**.

9. Dans le champ **Type de fichier**, sélectionnez le format requis du fichier de rapport : TXT ou CSV.

10. Cliquez sur le bouton **Exporter**.

SUPPRESSION DES INFORMATIONS DES RAPPORTS

Pour supprimer les informations des rapports, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).

2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Dans la partie droite de la fenêtre, dans le groupe **Paramètres des rapports**, cliquez sur le bouton **Supprimer les rapports**.

   La fenêtre **Suppression des informations des rapports** s'ouvrira.

4. Cochez les cases pour les rapports depuis lesquels vous voulez supprimer les informations :

   - **Tous les rapports**.
   - **Rapport de protection général**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Endpoint Security :
     - Antivirus Fichiers.
     - Antivirus Courrier.
     - Antivirus Internet.
     - Antivirus IM ("Chat").
     - Pare-feu.
     - Protection contre les attaques réseau.
   - **Rapport des tâches d'analyse**. Contient les informations sur les tâches exécutées de l'analyse:
     - Analyse complète.
     - Analyse rapide.
     - Analyse personnalisée.

- **Rapport des tâches de mise à jour**. Contient les informations sur les tâches de mise à jour exécutées.
- **Rapport de traitement des règles du Pare-feu**. Contient les informations sur le fonctionnement du Pare-feu.
- **Rapport des modules de contrôle**. Contient les informations sur le fonctionnement des modules suivants de Kaspersky Endpoint Security :
  - Contrôle du lancement des applications.
  - Contrôle de l'activité des applications.
  - Surveillance des vulnérabilités.
  - Contrôle des périphériques.
  - Contrôle Internet.
- **Données de la surveillance du système**. Contient les informations sur le fonctionnement de la Surveillance du système.

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

SERVICE DES NOTIFICATIONS

Cette section reprend les informations sur le service des notifications qui signalent à l'utilisateur les événements dans le fonctionnement de Kaspersky Endpoint Security, ainsi que les instructions sur la configuration des notifications.

DANS CETTE SECTION

A PROPOS DES NOTIFICATIONS DE KASPERSKY ENDPOINT SECURITY

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Endpoint Security. Il peut s'agir d'événements simplement informatifs ou d'événements importants. Par exemple, la notification peut signaler la réussite de la mise à jour des bases et des modules de l'application ou signaler une erreur dans le fonctionnement d'un module qu'il faudra rectifier au plus vite.

Kaspersky Endpoint Security permet de consigner les informations relatives aux événements survenus dans le fonctionnement de l'application dans le journal des événements Microsoft Windows et/ou dans le journal des événements de Kaspersky Endpoint Security.

Kaspersky Endpoint Security peut remettre les notifications d'une des manières suivantes :

- Afficher les notifications à l'aide de messages contextuels dans la zone de notification de la barre des tâches de Microsoft Windows.
- Envoyer les notifications par courrier électronique.

Vous pouvez configurer les modes de remise des notifications. Le mode de remise des notifications est défini pour chaque type d'événement.

CONFIGURATION DU SERVICE DE NOTIFICATIONS

Vous pouvez exécuter les opérations suivantes pour configurer le service de notification :

- Configurer les paramètres des journaux des événements dans lesquels Kaspersky Endpoint Security enregistre les événements.
- Configurer l'affichage des notifications à l'écran.
- Configurer la remise des notifications par courrier électronique.

Grâce au tableau des événements pour la configuration du service de notification, vous pouvez réaliser les opérations suivantes :

- filtrer les événements du service de notification en fonction de la valeur des colonnes ou selon un filtre complexe ;
- utiliser la fonction de recherche des événements du service de notification ;
- trier les événements du service de notification ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des événements du service de notification.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES DES JOURNAUX DES EVENEMENTS

Pour configurer les paramètres des journaux des événements, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** de la partie gauche de la fenêtre, sélectionnez la section **Apparence**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Notifications**.
4. La fenêtre **Notifications** s'ouvrira.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.
5. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer les paramètres des journaux des événements.
6. Cochez les cases en regard des événements requis dans les colonnes **Enregistrer dans le journal local** et **Enregistrer dans le journal d'événements Windows**.

   Les événements de la colonne **Enregistrer dans le journal local** sont repris dans le journal des événements de Kaspersky Endpoint Security. Les événements de la colonne **Enregistrer dans le journal Windows** sont repris dans le journal des événements de Microsoft Windows.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONFIGURATION DE LA REMISE DES NOTIFICATIONS VIA L'ECRAN OU COURRIER ELECTRONIQUE

Pour configurer la remise des notifications via l'écran ou le courrier électronique, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** de la partie gauche de la fenêtre, sélectionnez la section **Apparence**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Notifications**.
4. La fenêtre **Notifications** s'ouvrira.

   La partie gauche de la fenêtre reprend les modules et les tâches de Kaspersky Endpoint Security. La partie droite de la fenêtre affiche la liste des événements générée par le module ou la tâche sélectionné.
5. Dans la partie gauche de la fenêtre, sélectionnez le module ou la tâche pour lequel vous voulez configurer la remise des notifications.
6. Dans la colonne **Notifier sur écran**, cochez les cases en regard des événements requis.

   Les informations relatives aux événements sélectionnés sont affichées dans des messages contextuels dans la zone de notification de la barre des tâches de Microsoft Windows.
7. Dans la colonne **Notifier par courrier électronique**, cochez les cases en regard des événements requis.

   Les informations relatives aux événements sélectionnés sont envoyées par courrier électronique.
8. Cliquez sur le bouton **Configuration des notifications par courrier**.

   La fenêtre **Configuration des notifications par courrier** s'ouvre.
9. Cochez la case **Activer les notifications par courrier** afin d'activer la remise des informations relatives aux événements survenus pendant le fonctionnement de Kaspersky Endpoint Security marqués dans la colonne **Notifier par courrier électronique**.
10. Définissez les paramètres de remise des notifications par courrier.
11. Cliquez sur le bouton **OK**.
12. Dans la fenêtre **Configuration des notifications par courrier**, cliquez sur le bouton **OK**.
13. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

CONSULTATION DU JOURNAL DES EVENEMENTS DE MICROSOFT WINDOWS

Pour consulter le journal des événements de Microsoft Windows,

sélectionner **Démarrer → Configuration → Panneau de configuration → Administration → Observateur d'événements**.

UTILISATION DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Cette section explique comment configurer les paramètres de la quarantaine et du dossier de sauvegarde et comment les utiliser.

DANS CETTE SECTION

A PROPOS DE LA QUARANTAINE ET DE LA SAUVEGARDE

La *quarantaine* est la liste des fichiers potentiellement infectés par des virus ou d'autres programmes dangereux. Les *fichiers potentiellement infectés* sont des fichiers soupçonnés d'être infectés par des virus ou d'autres programmes dangereux ou des modifications de ceux-ci.

Quand Kaspersky Endpoint Security place un fichier potentiellement infecté en quarantaine, il ne le copie pas, mais il le déplace. L'application supprime le fichier du disque dur ou du message et l'enregistre dans un référentiel de données spécial. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Kaspersky Endpoint Security peut détecter des fichiers potentiellement infectés et les placer en quarantaine pendant la recherche d'éventuels virus ou programmes dangereux (cf. section "Analyse de l'ordinateur" à la page 181), ainsi que pendant le fonctionnement des modules de la protection Antivirus Fichiers (cf. section "A propos de l'Antivirus Fichiers" à la page 56), Antivirus Courrier (cf. section "A propos de l'Antivirus Courrier" à la page 71) et Surveillance du système (cf. page 67).

Kaspersky Endpoint Security place les fichiers en quarantaine dans les cas suivants :

- Le code du fichier est semblable à celui d'une menace connue mais il a été partiellement modifié ou sa structure évoque celle d'un programme malveillant, mais ne figure pas dans les bases de Kaspersky Endpoint Security. Dans ce cas, le fichier est placé en quarantaine suite à l'analyse heuristique de l'Antivirus Fichiers et de l'Antivirus Courrier, ou suite à la recherche d'éventuels virus et autres programmes dangereux. L'analyse heuristique donne rarement de faux positifs.

- La séquence des actions réalisées par le fichier est suspecte. Dans ce cas, le fichier est placé en quarantaine suite à l'analyse de son comportement par le module Surveillance du système.

L'utilisateur peut mettre lui-même un fichier en quarantaine s'il le soupçonne d'être infecté par un virus ou d'autres programmes dangereux.

La *Sauvegarde* est une liste des copies de sauvegarde des fichiers supprimés ou modifiés pendant la réparation. La *copie de sauvegarde* est une copie du fichier créée lors de la première réparation ou de la suppression du fichier et qui est conservée dans le même stockage que les fichiers potentiellement infectés. Les copies de sauvegarde des fichiers sont converties dans un format spécial et ne représentent aucun danger.

Il n'est pas toujours possible de préserver l'intégrité des fichiers lors de la réparation. Si le fichier réparé contenait des informations critiques partiellement ou complètement perdues suite à la réparation, l'utilisateur peut tenter de restaurer le fichier depuis sa copie réparée dans son dossier d'origine.

Après la mise à jour des bases et des modules de l'application, il se peut que Kaspersky Endpoint Security puisse identifier à 100 % la menace et la neutraliser. C'est la raison pour laquelle il est conseillé d'analyser les fichiers en quarantaine après chaque mise à jour des bases et des modules de l'application.

Il se peut que le statut du fichier change après l'analyse des fichiers en quarantaine à l'aide des définitions mises à jour :

- Si le fichier n'a pas été réparé lors de l'analyse, le fichier garde le statut *Infecté*.
- Si le fichier a été réparé lors de l'analyse, il reçoit le statut *Sain.* Un fichier de ce type peut être restauré dans son dossier d'origine.

CONFIGURATION DE LA QUARANTAINE ET DE LA SAUVEGARDE

La quarantaine et le dossier de sauvegarde constituent le stockage des données. Vous pouvez réaliser les opérations suivantes au niveau de la configuration de la quarantaine et du dossier de sauvegarde :

- Configurer la durée maximale de conservation des fichiers en quarantaine et des copies de fichiers dans le dossier de sauvegarde.

  Par défaut, la durée de conservation des fichiers placés en quarantaine ou des copies de fichiers placées dans le dossier de sauvegarde est de 30 jours. Une fois ce délai maximal écoulé, Kaspersky Endpoint Security supprime les fichiers les plus anciens du stockage. Vous pouvez annuler la restriction sur la durée de conservation ou la modifier.

- Configurer la taille maximale de la quarantaine et de la sauvegarde.

  Par défaut, la taille maximale de la quarantaine et de la sauvegarde est de 100 Mo. Une fois que la taille maximale a été atteinte, Kaspersky Endpoint Security supprime automatiquement les fichiers les plus anciens de la quarantaine et de la sauvegarde afin de ne plus dépasser la limite. Vous pouvez modifier la taille maximale de la quarantaine ou de la sauvegarde ou supprimer la restriction.

DANS CETTE SECTION

CONFIGURATION DE LA DUREE DE CONSERVATION MAXIMALE DES FICHIERS EN QUARANTAINE ET DANS LE DOSSIER DE SAUVEGARDE

Pour configurer la durée de conservation maximale des fichiers en quarantaine et dans le dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Exécutez une des actions suivantes :

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la quarantaine locale et de la sauvegarde**, cochez la case **Supprimer les objets après** si vous souhaitez limiter la durée de conservation des fichiers en quarantaine et des copies dans la sauvegarde. Dans le champ situé à droite de **Supprimer les objets après**, saisissez la durée de conservation maximale des fichiers en quarantaine et des copies de fichiers dans le dossier de sauvegarde. Par défaut, la durée maximale de conservation des fichiers en quarantaine et des copies dans le dossier de sauvegarde est de 30 jours.

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la quarantaine locale et de la sauvegarde**, décochez la case **Supprimer les objets après** si vous souhaitez lever la restriction sur la durée de conservation des fichiers en quarantaine et des copies dans la sauvegarde.

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

CONFIGURATION DE LA TAILLE MAXIMALE DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Pour configurer la taille maximale de la quarantaine et du dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans le groupe **Paramètres avancés** dans la partie gauche de la fenêtre, sélectionnez la section **Rapports et stockages**.

3. Exécutez une des actions suivantes :

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la quarantaine locale et de la sauvegarde**, cochez la case **Taille maximale** si vous souhaitez définir une taille limite pour la quarantaine et le dossier de sauvegarde. Dans le champ à droite de **Taille maximale**, indiquez la taille maximale de la quarantaine et du dossier de sauvegarde. Par défaut, la taille maximale est limitée à 100 Mo.

   - Dans la partie droite de la fenêtre, dans le groupe **Paramètres de la quarantaine locale et de la sauvegarde**, décochez la case **Taille maximale** si vous ne souhaitez pas définir une taille limite pour la quarantaine et le dossier de sauvegarde.

   Par défaut, il n'y a pas de limite sur la taille de la quarantaine et du dossier de sauvegarde.

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

UTILISATION DE LA QUARANTAINE

Dans la quarantaine, vous pouvez réaliser les opérations suivantes sur les fichiers :

- Consulter la liste des fichiers placés en quarantaine pendant le fonctionnement de Kaspersky Endpoint Security.
- Placer en quarantaine les fichiers soupçonnés de présenter une menace.
- Analyser les fichiers potentiellement infectés à l'aide de la version actuelle des bases et des modules de Kaspersky Endpoint Security.
- Restaurer les fichiers depuis la quarantaine vers leur dossier d'origine.
- Supprimer des fichiers de la quarantaine.
- Ouvrir le dossier d'origine du fichier.
- Envoyer les fichiers potentiellement infectés à Kaspersky Lab pour examen.

La liste des fichiers placés en quarantaine se présente sous la forme d'un tableau. Chaque ligne du tableau contient un événement relatif au fichier potentiellement infecté (par la suite, l'événement de la quarantaine) ou relative au type de menace découverte.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- Filtrer les événements de la quarantaine selon les valeurs d'une colonne ou selon un filtre complexe.
- Utiliser la fonction de recherche d'événements de la quarantaine.
- Trier les événements de la quarantaine.
- Modifier l'ordre et la sélection des colonnes affichées dans la liste des événements de la quarantaine.
- Regrouper les événements de la quarantaine.

Le cas échéant, vous pouvez copier les événements sélectionnés dans le Presse-papiers.

DANS CETTE SECTION

MISE EN QUARANTAINE DU FICHIER

Kaspersky Endpoint Security place automatiquement en quarantaine les fichiers potentiellement infectés détectés lors du fonctionnement des modules de la protection ou lors de la recherche d'éventuels virus ou autres programmes dangereux sur l'ordinateur.

Vous pouvez placer vous-même des fichiers en quarantaine si vous les soupçonnez de contenir des virus ou d'autres programmes dangereux.

Deux méthodes s'offrent à vous pour placer un fichier en quarantaine :

- via le bouton **Placer en quarantaine** sous l'onglet **Quarantaine** de la fenêtre **Rapports et stockages** ;
- via l'option du menu contextuel que vous ouvrez dans la fenêtre standard **Mes documents** de Microsoft Windows.

Pour placer un fichier en quarantaine depuis l'onglet Quarantaine de la fenêtre Rapports et stockages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Quarantaine** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   La fenêtre **Rapports et stockages** s'ouvre à l'onglet **Quarantaine**.

   L'onglet **Quarantaine** contient la liste des fichiers potentiellement infectés que Kaspersky Endpoint Security a découverts suite à l'analyse.

3. Cliquez sur le bouton **Placer en quarantaine**.

4. La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

5. Sélectionnez le fichier que vous souhaitez placer en quarantaine.

6. Cliquez sur le bouton **Ouvrir**.

   Le fichier sélectionné apparaît dans le tableau de l'onglet **Quarantaine**. L'accès à ce fichier est bloqué. Le fichier est déplacé depuis son dossier d'origine vers le dossier de quarantaine. Le fichier est codé dans la quarantaine, ce qui supprime le risque d'infection du système d'exploitation.

Pour placer un fichier en quarantaine au départ de la fenêtre Mes documents de Microsoft Windows, procédez comme suit :

1. Double-cliquez sur le raccourci **Mes documents** qui se trouve sur le Bureau du système d'exploitation de votre ordinateur.

   La fenêtre standard de Microsoft Windows **Mes documents** s'ouvre.

2. Accédez au dossier contenant le fichier que vous voulez placer en quarantaine.

3. Sélectionnez le fichier que vous souhaitez placer en quarantaine.

4. Cliquez-droit pour ouvrir le menu contextuel du fichier.

5. Choisissez l'option **Placer en quarantaine** dans le menu contextuel.

L'accès au fichier est bloqué. Le fichier est déplacé depuis son dossier d'origine vers le dossier de quarantaine. Le fichier est codé dans la quarantaine, ce qui supprime le risque d'infection du système d'exploitation.

LANCEMENT DE LA TACHE D'ANALYSE PERSONNALISEE DES FICHIERS EN QUARANTAINE

Après la mise à jour des bases et des modules de l'application, il se peut que Kaspersky Endpoint Security puisse identifier à 100 % la menace dans les fichiers en quarantaine et la neutraliser. Si l'analyse automatique des fichiers en quarantaine après chaque mise à jour des bases et des modules de l'application n'est pas configurée, vous pouvez lancer manuellement l'analyse personnalisée des fichiers en quarantaine.

Pour lancer la tâche d'analyse personnalisée pour les fichiers en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Le lien **Quarantaine** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   La fenêtre **Rapports et stockages** s'ouvre à l'onglet **Quarantaine**.

3. Sous l'onglet **Quarantaine**, sélectionnez un ou plusieurs événements de quarantaine relatifs aux fichiers potentiellement infectés que vous souhaitez analyser. Pour sélectionner plusieurs événements de la quarantaine, utilisez la touche **CTRL**.

4. Lancez la tâche d'analyse personnalisée des fichiers d'une des manières suivantes :

   - Cliquez sur le bouton **Nouvelle analyse**.

   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Nouvelle analyse**.

A l'issue de l'analyse, un message indique le nombre de fichiers analysés et le nombre de menaces détectées.

RESTAURATION DES FICHIERS DE LA QUARANTAINE

Pour restaurer des fichiers depuis la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Quarantaine** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   La fenêtre **Rapports et stockages** s'ouvre à l'onglet **Quarantaine**.
3. Si vous souhaitez restaurer tous les fichiers placés en quarantaine, procédez comme suit :

   a. Cliquez avec le bouton droit de la souris n'importe où dans le tableau de l'onglet **Quarantaine** et ouvrez le menu contextuel.

   b. Choisissez l'option **Restaurer tout**.

   Kaspersky Endpoint Security déplace tous les fichiers depuis la quarantaine vers leurs dossiers d'origine.
4. Si vous souhaitez restaurer un ou plusieurs fichiers depuis la quarantaine, procédez comme suit :

   a. Sous l'onglet **Quarantaine**, sélectionnez un ou plusieurs événements de quarantaine relatifs aux fichiers que vous souhaitez restaurer. Pour sélectionner plusieurs événements de la quarantaine, utilisez la touche **CTRL**.

   b. Choisissez une des méthodes suivantes pour restaurer les fichiers :

   - Cliquez sur le bouton **Restaurer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Restaurer**.

Kaspersky Endpoint Security déplace les fichiers sélectionnés vers leurs dossiers d'origine.

SUPPRESSION DES FICHIERS DE LA QUARANTAINE

Vous pouvez supprimer un fichier placé en quarantaine. Avant de supprimer le fichier de la quarantaine, Kaspersky Endpoint Security crée une copie de sauvegarde de celui-ci et la place dans le dossier de sauvegarde au cas où il faudrait restaurer le fichier plus tard (cf. section "Restauration des fichiers depuis le dossier de sauvegarde" à la page 225).

Pour supprimer des fichiers depuis la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Quarantaine** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   La fenêtre **Rapports et stockages** s'ouvre à l'onglet **Quarantaine**.
3. Sous l'onglet **Quarantaine**, sélectionnez un ou plusieurs événements de quarantaine relatifs aux fichiers potentiellement infectés que vous souhaitez supprimer de la quarantaine. Pour sélectionner plusieurs événements de la quarantaine, utilisez la touche **CTRL**.
4. Choisissez une des méthodes suivantes pour supprimer les fichiers :

   - Cliquez sur le bouton **Supprimer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Choisissez l'option **Supprimer**.

Kaspersky Endpoint Security supprime tous les fichiers sélectionnés de la quarantaine. Kaspersky Endpoint Security crée une copie de sauvegarde de chaque fichier et la place dans le dossier de sauvegarde.

ENVOI DES FICHIERS POTENTIELLEMENT INFECTES A KASPERSKY LAB POUR EXAMEN

Pour pouvoir envoyer des fichiers potentiellement infectés à Kaspersky Lab, votre ordinateur doit être équipé d'un client de messagerie électronique et il doit être connecté à Internet.

Pour envoyer des fichiers potentiellement infectés pour examen à Kaspersky Lab, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Quarantaine** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.

   La fenêtre **Rapports et stockages** s'ouvre à l'onglet **Quarantaine**.
3. Sous l'onglet **Quarantaine**, sélectionnez un ou plusieurs événements de la quarantaine relatifs aux fichiers potentiellement infectés que vous souhaitez envoyer à Kaspersky Lab pour examen. Pour sélectionner plusieurs événements de la quarantaine, utilisez la touche **CTRL**.
4. Cliquez-droit pour ouvrir le menu contextuel.
5. Choisissez l'option **Envoyer à Kaspersky Lab**.

Une fenêtre de composition de message du client de messagerie installé sur l'ordinateur s'ouvre. Le message contient une archive avec les fichiers à envoyer, l'adresse du destinataire, à savoir newvirus@kaspersky.com et l'objet du message "Objet en quarantaine".

UTILISATION DE LA SAUVEGARDE

Si Kaspersky Endpoint Security détecte un code malveillant dans un fichier, il bloque celui-ci, le supprime de son dossier d'origine et place une copie dans le dossier de sauvegarde avant de tenter de le réparer. Si le fichier est réparé, l'état de la copie de sauvegarde devient *Réparé*. Ensuite, vous pouvez restaurer le fichier au départ de sa copie de réserve réparée dans son dossier d'origine.

Kaspersky Endpoint Security supprime les copies de sauvegarde des fichiers de n'importe quel statut automatiquement à l'issue de la période définie dans les paramètres de l'application.

Vous pouvez supprimer vous-même une copie de sauvegarde d'un fichier restauré ou non.

La liste des copies de sauvegarde des fichiers se présente sous la forme d'un tableau. Chaque ligne du tableau contient l'événement impliquant le fichier infecté (désigné par la suite par l'expression "événement du dossier de sauvegarde" et des informations sur le type de menace détectée dans le fichier.

Vous pouvez réaliser les opérations suivantes sur les copies de sauvegarde des fichiers du dossier de sauvegarde :

- consulter la liste des copies de sauvegarde des fichiers ;
- restaurer les fichiers au départ des copies de sauvegarde dans leurs dossiers d'origine ;
- supprimer des copies de sauvegarde de fichiers du dossier de sauvegarde.

De plus, vous pouvez réaliser les opérations suivantes sur les données du tableau :

- filtrer les événements du dossier de sauvegarde en fonction de la valeur des colonnes ou selon un filtre complexe ;
- utiliser la fonction de recherche d'événements du dossier de sauvegarde ;

- trier les événements du dossier de sauvegarde ;
- grouper les événements du dossier de sauvegarde ;
- modifier l'ordre et la sélection des colonnes affichées dans la liste des événements du dossier de sauvegarde.

Le cas échéant, vous pouvez copier les événements sélectionnés dans le Presse-papiers.

DANS CETTE SECTION

RESTAURATION DES FICHIERS DEPUIS LA SAUVEGARDE

Il est conseillé de restaurer les fichiers au départ des copies de sauvegarde uniquement si ceux-ci ont le statut *Réparé*.

Pour restaurer des fichiers depuis le dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockages**, choisissez l'onglet **Dossier de sauvegarde**.
4. Si vous souhaitez restaurer tous les fichiers du dossier de sauvegarde, procédez comme suit :
   a. Cliquez-droit n'importe où dans le tableau de l'onglet **Dossier de sauvegarde** et ouvrez le menu contextuel.
   b. Choisissez l'option **Restaurer tout**.

   Kaspersky Endpoint Security restaure tous les fichiers depuis le dossier de sauvegarde vers leurs dossiers d'origine.
5. Si vous souhaitez restaurer un ou plusieurs fichiers depuis le dossier de sauvegarde, procédez comme suit :
   a. Dans le tableau de l'onglet **Dossier de sauvegarde**, sélectionnez un ou plusieurs événements du dossier de sauvegarde. Pour sélectionner plusieurs événements, utilisez la touche **CTRL**.
   b. Cliquez sur le bouton **Restaurer**.

Kaspersky Endpoint Security restaure tous les fichiers sélectionnés depuis le dossier de sauvegarde vers leurs dossiers d'origine.

SUPPRESSION DES COPIES DE SAUVEGARDE DES FICHIERS DEPUIS LE DOSSIER DE SAUVEGARDE

Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Le lien **Rapports** dans la partie supérieure de la fenêtre principale de l'application permet d'ouvrir la fenêtre **Rapports et stockages**.
3. Dans la fenêtre **Rapports et stockages**, choisissez l'onglet **Dossier de sauvegarde**.
4. Dans l'onglet **Dossier de sauvegarde**, sélectionnez un ou plusieurs événements du dossier de sauvegarde. Pour sélectionner plusieurs événements du dossier de sauvegarde, utilisez la touche **CTRL**.
5. Cliquez sur le bouton **Supprimer**.

CONFIGURATION COMPLEMENTAIRE DE L'APPLICATION

Cette section contient les informations sur la configuration des paramètres complémentaires de Kaspersky Endpoint Security.

DANS CETTE SECTION

ZONE DE CONFIANCE

Cette section présente des informations sur la zone de confiance et explique comment configurer les règles d'exclusion et composer une liste d'applications de confiance.

DANS CETTE SECTION

A PROPOS DE LA ZONE DE CONFIANCE

La *zone de confiance* est une liste d'objets et d'applications composée par l'administrateur que Kaspersky Endpoint Security ne contrôle pas. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection de Kaspersky Endpoint Security.

L'administrateur du système forme indépendamment la zone de confiance selon les particularités des objets avec lesquels il faut travailler, ainsi que selon les applications installées sur l'ordinateur. Il faudra peut-être inclure des objets et des applications dans la zone de confiance si Kaspersky Endpoint Security bloque l'accès à un objet ou à une application quelconque alors que vous êtes certain que cet objet ou cette application ne pose absolument aucun danger.

Vous pouvez exclure de l'analyse les objets des types suivants :

- fichiers d'un format déterminé ;
- fichiers selon un masque ;
- certaines zones (par exemple, un dossier ou une application) ;
- processus des applications ;
- objets selon le classement de l'Encyclopédie des virus de Kaspersky Lab (à savoir, en fonction de l'état que Kaspersky Endpoint Security a attribué à l'objet à l'issue de l'analyse).

Règle d'exclusion

La *règle d'exclusion* est un ensemble de conditions sous lesquelles Kaspersky Endpoint Security n'analyse pas l'objet à la recherche de virus et autres programmes dangereux.

Le *type de menace* est un état qui correspond à l'état assigné par Kaspersky Endpoint Security à un objet au cours de la recherche d'éventuels virus et autres programmes dangereux. Cet état est attribué en fonction du classement des applications malveillantes et d'autres applications présentes dans l'encyclopédie des virus de Kaspersky Lab. Le lien http://www.viruslist.com/fr/ vous vous permet d'accéder au site Internet de l'Encyclopédie des virus de Kaspersky Lab et d'obtenir des informations détaillées sur la menace relative à l'objet.

A leur tour, les règles d'exclusion permettent d'utiliser des applications légitimes qui pourraient être employées par des individus malintentionnés pour nuire à l'ordinateur et aux données de l'utilisateur. Ces applications en elles-mêmes n'ont pas de fonctions malveillantes, mais ces applications pourraient être utilisées en guise d'auxiliaire pour un programme malveillant. Cette catégorie reprend les applications d'administration à distance, les clients IRC, les serveurs FTP, divers utilitaires de suspension ou d'arrêt de processus, les enregistreurs de frappe, les applications d'identification de mots de passe, les numéroteurs automatiques vers des sites Internet payants. Ce logiciel n'est pas classé en tant que virus (not-a-virus), mais il peut être classé parmi d'autres types d'applications, notamment Adware, Riskware. Vous pouvez obtenir des informations détaillées sur les logiciels publicitaires et les applications légitimes qui pourraient être exploitées par des individus mal intentionnés pour nuire à l'ordinateur et aux données de l'utilisateur sur le site de l'Encyclopédie de virus de Kaspersky Lab en cliquant sur le lien http://www.viruslist.com/fr/.

Kaspersky Endpoint Security peut bloquer de telles applications. Pour éviter le blocage, il est possible de créer des règles d'exclusion de l'analyse de Kaspersky Endpoint Security pour les applications utilisées. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque de la menace selon le classement de l'Encyclopédie des virus de Kaspersky Lab. Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'un système d'accès à distance qui permet de travailler sur un ordinateur distant. Kaspersky Endpoint Security classe cette activité parmi les activités qui présentent un risque potentiel et peut la bloquer. Afin d'éviter le blocage de l'application, il faut composer une règle d'exclusion pour laquelle le type de menace sera Remote Administrator.

Les règles d'exclusions peuvent être utilisées pendant le fonctionnement des modules et des tâches suivants de l'application définis par l'administrateur du système :

- Antivirus Fichiers.
- Antivirus Courrier.
- Antivirus Internet.
- Contrôle de l'activité des applications.
- Tâches d'analyse.
- Surveillance du système.

Liste des applications de confiance

Liste des applications de confiance est une liste des applications pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et de réseau (y compris l'activité suspecte), ni les requêtes adressées à la base de registres système. Par défaut Kaspersky Endpoint Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère. Kaspersky Endpoint Security exclut de l'analyse toute application ajoutée à la liste des applications de confiance (cf. section "Composition de la liste des applications de confiance" à la page 232).

Par exemple, si vous estimez que les objets utilisés par l'application Microsoft Windows Bloc-notes ne posent aucun danger et ne doivent pas être analysés (vous faites confiance à cette application), il faut ajouter l'application Microsoft Windows Bloc-notes à la liste des applications de confiance pour ne pas analyser les objets utilisés par cette application.

De plus, certaines actions que Kaspersky Endpoint Security juge comme dangereuses peuvent être sans danger dans le cadre du fonctionnement de toute une série de programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale pour les logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (par exemple, Punto Switcher). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion des applications de confiance de l'analyse permet d'éviter les problèmes de compatibilité entre Kaspersky Endpoint Security et d'autres applications (par exemple, les problèmes liés à la double analyse du trafic de réseau d'un ordinateur par Kaspersky Endpoint Security et un autre logiciel antivirus) et d'améliorer les performances de l'ordinateur, ce qui est particulièrement important dans le cadre de l'utilisation d'applications serveur.

Le fichier exécutable et le processus d'une application de confiance restent toujours soumis à la recherche d'éventuels virus et autre programmes présentant une menace. Pour exclure entièrement l'application de l'analyse de Kaspersky Endpoint Security, il faut utiliser les règles d'exclusions.

CONFIGURATION DE LA ZONE DE CONFIANCE

Vous pouvez exécuter les opérations suivantes pour configurer les paramètres de la zone de confiance :

- Créer une règle d'exclusion.

  Vous pouvez créer une règle d'exclusion qui, lorsqu'elle est exécutée, indique à Kaspersky Endpoint Security de ne pas analyser l'objet indiqué ni le type de menace.

- Suspendre l'application de la règle d'exclusion.

  Vous pouvez suspendre temporairement l'utilisation d'une règle sans devoir la supprimer de la liste des règles d'exclusion.

- Modifier les paramètres d'une règle d'exclusion existante.

  Après avoir créé une règle d'exclusion, vous pouvez toujours revenir à la configuration des paramètres de cette règle et modifier les paramètres requis.

- Supprimer la règle d'exclusion.

  Vous pouvez supprimer la règle d'exclusion si vous ne souhaitez pas que Kaspersky Endpoint Security applique cette règle lors de l'analyse de l'ordinateur.

- Composer la liste des applications de confiance.

  Vous pouvez composer la liste des applications de confiance pour lesquelles Kaspersky Endpoint Security ne contrôle pas l'activité de fichier et de réseau (y compris l'activité suspecte), ni les requêtes adressées à la base de registres système.

- Suspendre l'exclusion de l'analyse par Kaspersky Endpoint Security d'une application de confiance.

  Vous pouvez suspendre temporairement l'exclusion d'une application de confiance de l'analyse de Kaspersky Endpoint Security sans devoir la supprimer de la liste des applications de confiance.

DANS CETTE SECTION

CREATION D'UNE REGLE D'EXCLUSION

Kaspersky Endpoint Security n'analyse pas l'objet si le disque dur ou le dossier dans lequel se trouve cet objet est indiqué au moment de lancer une des tâches d'analyse. Cependant, lors du lancement de la tâche d'analyse personnalisée, une règle d'exclusion n'est pas appliquée à cet objet.

Pour créer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvrira sous l'onglet **Règles d'exclusion**.
4. Cliquez sur le bouton **Ajouter**.

   La fenêtre **Règle d'exclusion** s'ouvre.
5. Si vous souhaitez exclure de l'analyse de Kaspersky Endpoint Security le fichier ou le dossier, procédez comme suit :

   a. Dans le groupe **Propriétés**, cochez la case **Objet**.

   b. A l'aide du lien **sélectionnez l'objet** situé dans le groupe **Description de la règle**, ouvrez la fenêtre **Nom de l'objet**. Cette fenêtre permet de saisir le nom du fichier, du dossier ou le masque du nom de l'objet ou de sélectionner l'objet dans l'arborescence des dossiers Microsoft Windows.

   c. Après avoir sélectionné l'objet, cliquez sur le bouton **OK** dans la fenêtre **Nom de l'objet**.

   Le lien sur l'objet ajouté apparaîtra dans le groupe **Description de la règle** de la fenêtre **Règle d'exclusion**.
6. Si vous voulez exclure de l'analyse de Kaspersky Endpoint Security les objets selon le type déterminé de menace, procédez comme suit :

   a. Dans le groupe **Propriétés**, cochez la case **Type de menace**.

   Le *type de menace* est un état qui correspond à l'état assigné par Kaspersky Endpoint Security à un objet au cours de la recherche d'éventuels virus et autres programmes dangereux. Cet état est attribué en fonction du classement des applications malveillantes et d'autres applications présentes dans l'encyclopédie des virus de Kaspersky Lab.

   b. A l'aide du lien **saisissez le nom de la menace** situé dans le groupe **Description de la règle**, ouvrez la fenêtre **Type de menaces**. Cette fenêtre permet de saisir le nom ou le masque du nom du type de menaces selon le classement de l'Encyclopédie de virus de Kaspersky Lab.

   c. Cliquez sur le bouton **OK** dans la fenêtre **Type de menaces**.
7. Saisissez un bref commentaire à la règle d'exclusion à créer dans le champ **Commentaires**.
8. Définissez les modules de Kaspersky Endpoint Security qui doivent appliquer la règle d'exclusion.

   a. Cliquez sur le lien **quelconque** situé dans le groupe **Description de la règle** pour ouvrir le lien **sélectionnez les modules**.

   b. Cliquez sur le lien **sélectionnez les modules** pour ouvrir la fenêtre **Modules de la protection**. Cette fenêtre permet de sélectionner les modules nécessaires.

c. Cliquez sur le bouton **OK** dans la fenêtre **Modules de la protection**.

Si les modules sont indiqués dans les paramètres de la règle d'exclusion, l'objet n'est pas analysé que par ces modules de Kaspersky Endpoint Security.

Si les modules ne sont pas indiqués dans les paramètres de la règle d'exclusion, l'objet n'est pas analysé par tous les modules de Kaspersky Endpoint Security.

9. Cliquez sur **OK** dans la fenêtre **Règle d'exclusion**.

La règle d'exclusion ajoutée apparaît dans la liste des règles d'exclusion de l'onglet **Règles d'exclusion** dans la fenêtre **Zone de confiance**. Le groupe **Description de la règle** affiche les paramètres de cette règle d'exclusion.

10. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

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

MODIFICATION D'UNE REGLE D'EXCLUSION

Pour modifier une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvrira sous l'onglet **Règles d'exclusion**.

4. Sélectionnez la règle requise dans la liste des règles d'exclusion.

5. Cliquez sur le bouton **Modifier**.

La fenêtre **Règle d'exclusion** s'ouvre.

6. Modifier les paramètres d'une règle d'exclusion.

7. Cliquez sur **OK** dans la fenêtre **Règle d'exclusion**.

Le groupe **Description de la règle** affiche les modifications des paramètres de cette règle d'exclusion.

8. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

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

SUPPRESSION D'UNE REGLE D'EXCLUSION

Pour supprimer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).

2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.

3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

La fenêtre **Zone de confiance** s'ouvrira sous l'onglet **Règles d'exclusion**.

4. Sélectionnez la règle requise dans la liste des règles d'exclusion.
5. Cliquez sur le bouton **Supprimer**.

   La règle d'exclusion disparaît de la liste.
6. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

LANCEMENT ET ARRET DU FONCTIONNEMENT D'UNE REGLE D'EXCLUSION

Pour lancer ou arrêter une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvrira sous l'onglet **Règles d'exclusion**.
4. Sélectionnez la règle requise dans la liste des règles d'exclusion.
5. Exécutez une des actions suivantes :
   - Cochez la case en regard du nom de la règle d'exclusion si vous souhaitez activer cette règle.
   - Décochez la case en regard du nom de la règle d'exclusion si vous souhaitez suspendre temporairement le fonctionnement de cette règle.
6. Cliquez sur le bouton **OK**.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

COMPOSITION DE LA LISTE DES APPLICATIONS DE CONFIANCE

Pour composer une liste des applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvrira.
4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.

5. Si vous voulez ajouter une application à la liste des applications de confiance, procédez comme suit :

   a. Cliquez sur le bouton **Ajouter**.

   b. Dans le menu déroulant ouvert, exécutez une des actions suivantes :

      - Sélectionnez l'option **Applications** si vous voulez trouver l'application dans la liste des applications installées sur l'ordinateur. La fenêtre **Sélection de l'application** s'ouvrira.

      - Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin au fichier exécutable de l'application nécessaire. La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

   Suite à des actions exécutées, la fenêtre **Exclusions pour l'application** s'ouvrira.

   c. Cochez les cases pour les types d'activité à ne pas analyser de l'application :

      - **Ne pas analyser les fichiers ouverts**.

      - **Ne pas surveiller l'activité de l'application**.

      - **Restriction non héritée du processus parent (application)**.

      - **Ne pas surveiller l'activité des applications enfants**.

      - **Autoriser l'interaction avec l'interface de l'application**.

      - **Ne pas analyser le trafic réseau**.

   d. Cliquez sur **OK** dans la fenêtre **Exclusions pour l'application**.

      L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.

6. Si vous voulez modifier les paramètres de l'application de confiance, procédez comme suit :

   a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

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

   c. La fenêtre **Exclusions pour l'application** s'ouvre.

   d. Modifiez les statuts des cases pour les types requis de l'activité de l'application.

   Si aucun type d'activité de l'application n'a été sélectionné dans la fenêtre **Exclusions pour l'application**, l'inclusion de l'application de confiance dans l'analyse a lieu (cf. section "Inclusion et exclusion de l'application de confiance de l'analyse" à la page 234). L'application de confiance n'est pas supprimée de la liste des applications de confiance, mais la case est décochée pour elle.

   e. Cliquez sur **OK** dans la fenêtre **Exclusions pour l'application**.

7. Si vous voulez supprimer l'application de confiance de la liste des applications de confiance, procédez comme suit :

   a. Sélectionnez l'application de confiance dans la liste des applications de confiance.

   b. Cliquez sur le bouton **Supprimer**.

8. Cliquez sur le bouton **OK** dans la fenêtre **Zone de confiance**.

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

INCLUSION ET EXCLUSION DE L'APPLICATION DE CONFIANCE DE L'ANALYSE

Pour inclure une application de confiance dans l'analyse ou pour l'exclure, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvrira.
4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.
5. Sélectionnez l'application de confiance requise dans la liste des applications de confiance.
6. Exécutez une des actions suivantes :
   - Cochez la case en regard du nom de l'application de confiance si vous souhaitez l'exclure de l'analyse de Kaspersky Endpoint Security.
   - Décochez la case en regard du nom de l'application de confiance si vous souhaitez l'inclure dans l'analyse de Kaspersky Endpoint Security.
7. Cliquez sur le bouton **OK**.
8. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

AUTODEFENSE DE KASPERSKY ENDPOINT SECURITY

Cette section contient les informations sur les mécanismes de l'autodéfense de Kaspersky Endpoint Security et contre l'administration externe de Kaspersky Endpoint Security, ainsi que les instructions sur la configuration des paramètres de ces mécanismes.

DANS CETTE SECTION

A PROPOS DE L'AUTODEFENSE DE KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security protège les ordinateurs contre les programmes malveillants, y compris ceux qui tentent de bloquer le fonctionnement de Kaspersky Endpoint Security, voire ou de le supprimer de l'ordinateur.

La stabilité du système de protection de l'ordinateur de l'utilisateur est garantie par les mécanismes d'autodéfense et de protection contre l'administration externe intégrés à Kaspersky Endpoint Security.

Le mécanisme d'autodéfense empêche la modification et la suppression des fichiers de l'application sur le disque dur, des processus dans la mémoire et des clés de la base de registres système.

Le mécanisme de protection contre l'administration externe permet de bloquer toutes les tentatives d'administration de l'application depuis un poste distant.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky Endpoint Security contre la modification et la suppression de fichiers de l'application sur le disque dur ou contre la modification ou la suppression de clés dans la base de registres système est accessible.

ACTIVATION ET DESACTIVATION DU MECANISME DE L'AUTODEFENSE

Par défaut, le mécanisme de l'autodéfense de Kaspersky Endpoint Security est activé. S'il faut, vous pouvez désactiver le mécanisme de l'autodéfense.

Pour activer ou désactiver l'autodéfense, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Activer l'autodéfense** si vous voulez activer le mécanisme d'autodéfense de l'application
   - Décochez la case **Activer l'autodéfense** si vous voulez désactiver le mécanisme d'autodéfense de l'application
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACTIVATION ET DESACTIVATION DU MECANISME DE L'AUTODEFENSE CONTRE L'ADMINISTRATION EXTERNE

Par défaut, le mécanisme de l'autodéfense contre l'administration externe est activé. Le cas échéant, vous pouvez désactiver le mécanisme de l'autodéfense contre l'administration externe.

Pour activer ou désactiver le mécanisme de l'autodéfense contre l'administration externe, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Désactiver la gestion externe du service système** si vous voulez activer le mécanisme de l'autodéfense contre l'administration externe.
   - Décochez la case **Désactiver la gestion externe du service système** si vous voulez désactiver le mécanisme de l'autodéfense contre l'administration externe.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ASSURANCE DE FONCTIONNEMENT DES APPLICATIONS DE L'ADMINISTRATION A DISTANCE

Il arrive souvent que lors de l'utilisation de mécanismes de protection contre l'administration externe il soit nécessaire d'appliquer une application d'administration externe.

Pour garantir le fonctionnement des applications d'administration à distance, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Exclusions et applications de confiance**, cliquez sur le bouton **Configuration**.

   La fenêtre **Zone de confiance** s'ouvrira.
4. Dans la fenêtre **Zone de confiance**, sélectionnez l'onglet **Applications de confiance**.
5. Cliquez sur le bouton **Ajouter**.
6. Dans le menu déroulant ouvert, exécutez une des actions suivantes :
   - Sélectionnez l'option **Applications** si vous voulez trouver l'application d'administration à distance dans la liste des applications installées sur l'ordinateur. La fenêtre **Sélection de l'application** s'ouvrira.
   - Sélectionnez l'option **Parcourir** si vous voulez indiquer le chemin au fichier exécutable de l'application d'administration à distance. La fenêtre standard de Microsoft Windows **Ouvrir** s'ouvre.

   Suite à des actions exécutées, la fenêtre **Exclusions pour l'application** s'ouvrira.
7. Cochez la case **Ne pas surveiller l'activité de l'application**.

8. Cliquez sur **OK** dans la fenêtre **Exclusions pour l'application**.

   L'application de confiance ajoutée apparaîtra dans la liste des applications de confiance.

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

PERFORMANCES DE KASPERSKY ENDPOINT SECURITY ET COMPATIBILITE AVEC D'AUTRES APPLICATIONS

Cette section contient les informations sur les performances de Kaspersky Endpoint Security et sur la compatibilité avec d'autres applications, ainsi que les instructions sur la sélection des types de menaces à détecter et le mode de fonctionnement de Kaspersky Endpoint Security.

DANS CETTE SECTION

A PROPOS DES PERFORMANCES DE KASPERSKY ENDPOINT SECURITY ET DE LA COMPATIBILITE AVEC D'AUTRES APPLICATIONS

Performances de Kaspersky Endpoint Security

Les performances de Kaspersky Endpoint Security désignent le nombre de types de menace qui peuvent être détectées et la consommation en ressources et en énergie de l'ordinateur.

Sélection des types de menaces détectées

Kaspersky Endpoint Security permet de configurer en souplesse la protection de l'ordinateur et de sélectionner les types de menace (cf. section "Sélection des types de menaces détectées" à la page 238) que l'application détectera pendant son exécution. Kaspersky Endpoint Security recherche toujours la présence éventuelle de virus, de vers et de chevaux de Troie dans le système d'exploitation. Vous ne pouvez pas désactiver l'analyse pour ces types de menace. Ces programmes peuvent infliger des dégâts considérables à l'ordinateur de l'utilisateur. Pour élargir la protection offerte à l'ordinateur, vous pouvez enrichir la liste des types de menace à détecter en activant le contrôle de l'activité des applications légitimes qui pourraient être utilisées par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

Utilisation du mode d'économie d'énergie

Quand vous utilisez un ordinateur portable, la consommation des applications est un élément dont il faut tenir compte. En général, les tâches planifiées de Kaspersky Endpoint Security sont très gourmandes en ressources. Quand l'ordinateur est alimenté par la batterie, pour économiser la charge vous pouvez utiliser le mode d'économie d'énergie.

Le mode d'économie d'énergie permet de reporter automatiquement l'exécution des tâches qui ont été programmées.

- tâche de mise à jour (cf. section "A propos de la mise à jour des bases et des modules de l'application" à la page 171) ;
- tâche d'analyse complète (cf. section "A propos des tâches d'analyse" à la page 181) ;
- tâche d'analyse rapide (cf. section "A propos des tâches d'analyse" à la page 181) ;
- tâche d'analyse personnalisée (cf. section "A propos des tâches d'analyse" à la page 181) ;
- recherche de vulnérabilités (cf. section "A propos de la tâche de recherche de vulnérabilités" à la page 198).

Transfert des ressources de l'ordinateur à d'autres applications

L'utilisation des ressources de l'ordinateur par Kaspersky Endpoint Security peut avoir un effet sur les performances des autres applications. Pour résoudre les problèmes liés à l'utilisation conjointe d'applications en cas de surcharge du processeur et des sous-systèmes de disque, Kaspersky Endpoint Security peut suspendre l'exécution des tâches programmées et céder les ressources à d'autres applications (cf. section "Activation et désactivation du mode d'économie d'énergie" à la page 239).

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas de l'exécution de ces applications, il ne faut pas leur céder les ressources du système d'exploitation.

Le cas échéant, ces tâches peuvent être lancées manuellement.

Application de la technologie de réparation de l'infection active

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. Quand Kaspersky Endpoint Security a détecté une activité malveillante dans le système d'exploitation, il exécute une procédure de réparation étendue en appliquant la technologie de réparation de l'infection active (cf. section "Activation et désactivation de la technologie de réparation de l'infection active" à la page 239). *La technologie de réparation de l'infection active* vise à supprimer du système d'exploitation les programmes malveillants qui ont déjà lancé leurs processus dans la mémoire vive et qui compliquent leur suppression par Kaspersky Endpoint Security à l'aide d'autres méthodes. La menace est ainsi neutralisée et supprimée. Pendant l'exécution de la réparation étendue, il est déconseillé de lancer de nouveaux processus ou de modifier la base de registres du système d'exploitation. La technologie de réparation de l'infection active est gourmande en ressource et peut ralentir d'autres applications.

A l'issue de la réparation étendue, Kaspersky Endpoint Security redémarre l'ordinateur sans demander l'avis de l'utilisateur. Par conséquent, il est conseillé à l'utilisateur de sauvegarder tous ses travaux et de quitter toutes les applications dès l'affichage de la notification sur l'infection active. Kaspersky Endpoint Security termine de supprimer les fichiers du programme malveillant directement après le redémarrage de l'ordinateur.

Il est conseillé de lancer la tâche d'analyse complète après le redémarrage de l'ordinateur.

SELECTION DES TYPES DE MENACES DETECTEES

Pour sélectionner les types de menaces à identifier, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Cliquez sur le bouton **Configuration** dans le groupe **Menaces**.

La fenêtre **Menaces** s'ouvrira.

4. Cochez les cases pour les types de menaces à détecter par Kaspersky Endpoint Security :
   - **Utilitaires malveillants**.
   - **Logiciels publicitaires (adwares,...)**.
   - **Numéroteurs automatiques**.
   - **Autres**.
   - **Fichiers compactés pouvant provoquer des dégâts**.
   - **Fichiers compactés à plusieurs reprises**.
5. Cliquez sur le bouton **OK**.

   La fenêtre **Menaces** se fermera. Le groupe **Menace** sous l'inscription **Détection des menaces suivantes activée** affichera les types de menaces que vous avez sélectionnés.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACTIVATION ET DESACTIVATION DE LA TECHNOLOGIE DE REPARATION DE L'INFECTION ACTIVE

La technologie de réparation de l'infection active est disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous un système d'exploitation Microsoft Windows pour les postes de travail. La technologie de réparation de l'infection active n'est pas disponible si Kaspersky Endpoint Security a été installé sur un ordinateur tournant sous un système d'exploitation Microsoft Windows pour les serveurs de fichiers (cf. section "Configurations logicielle et matérielle" à la page 19).

Pour activer ou désactiver la technologie de réparation de l'infection active, procédez comme suit :

1. Ouvrez la fenêtre de configuration des paramètres de l'application (cf. page 51).
2. Dans la partie gauche de la fenêtre, sélectionnez le groupe **Protection antivirus**.

   Les paramètres de la protection antivirus s'afficheront dans la partie droite de la fenêtre.
3. Dans la partie droite de la fenêtre, exécutez une des actions suivantes :
   - Cochez la case **Appliquer la technologie de réparation de l'infection active** si vous souhaitez activer la technologie de réparation de l'infection active.
   - Décochez la case **Appliquer la technologie de réparation de l'infection active** si vous ne souhaitez pas activer la technologie de réparation de l'infection active.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACTIVATION ET DESACTIVATION DU MODE D'ECONOMIE D'ENERGIE

Pour activer ou désactiver le mode d'économie d'énergie, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Mode de fonctionnement**, procédez comme suit :

   - Cochez la case **Ne pas lancer les tâches planifiées en cas d'alimentation par batterie** si vous voulez activer le mode d'économie d'énergie.

     Quand le mode d'économie d'énergie est activé, les tâches suivantes ne sont pas exécutées, mais si elles sont programmées :

     - tâche de mise à jour ;
     - tâche d'analyse complète ;
     - tâche d'analyse rapide ;
     - tâche d'analyse personnalisée ;
     - tâche de recherche de vulnérabilités.
   - Décochez la case **Ne pas lancer les tâches planifiées en cas d'alimentation par batterie** si vous voulez désactiver le mode d'économie d'énergie.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

ACTIVATION ET DESACTIVATION DU MODE DE TRANSFERT DES RESSOURCES VERS D'AUTRES APPLICATIONS

Pour activer ou désactiver le mode de transfert des ressources vers d'autres applications, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Sélectionnez le groupe **Paramètres complémentaires** dans la partie gauche de la fenêtre.

   Les paramètres complémentaires de l'application s'afficheront dans la partie droite de la fenêtre.
3. Dans le groupe **Mode de fonctionnement**, procédez comme suit :

   Cochez la case **Céder les ressources aux autres applications** si vous voulez activer le mode de transfert des ressources vers d'autres applications. Si ce mode est activé, Kaspersky Endpoint Security reporte l'exécution des tâches si, pour ces tâches, le lancement planifié a été défini et leur exécution ralentit le fonctionnement d'autres applications :

   - tâche de mise à jour ;
   - tâche d'analyse complète ;
   - tâche d'analyse rapide ;

- tâche d'analyse personnalisée ;
- tâche de recherche de vulnérabilités.

- Décochez la case **Céder les ressources aux autres applications** si vous voulez désactiver le mode de transfert des ressources vers d'autres applications. Dans ce cas, Kaspersky Endpoint Security exécute les tâches planifiées peu importe le fonctionnement d'autres applications.

Le mode de transfert des ressources vers d'autres applications est désactivé par défaut.

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

PROTECTION PAR MOT DE PASSE

Cette section contient les informations sur les restrictions d'accès à Kaspersky Endpoint Security à l'aide du mot de passe.

DANS CETTE SECTION

A PROPOS DES RESTRICTIONS D'ACCES A KASPERSKY ENDPOINT SECURITY

L'ordinateur peut être utilisé par plusieurs personnes dont les connaissances informatiques varient. L'accès illimité des utilisateurs à Kaspersky Endpoint Security et à ses paramètres peut entraîner une réduction du niveau de protection de l'ordinateur dans son ensemble.

Pour limiter l'accès à Kaspersky Endpoint Security, vous devez définir un mot de passe et désigner les opérations qui ne pourront être exécutées qu'après la saisie du mot de passe en question :

- toutes les opérations (sauf les notifications de danger) ;
- modification des paramètres de fonctionnement de l'application ;
- arrêt de l'application ;
- désactivation des modules de la protection et arrêt des tâches d'analyse ;
- désactivation des modules de contrôle ;
- suspension de la tâche d'analyse complète ;
- suppression de la licence ;
- suppression de l'application.

ACTIVATION ET DESACTIVATION DE LA PROTECTION PAR MOT DE PASSE

Pour activer ou désactiver la protection par mot de passe, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** de la partie gauche de la fenêtre, sélectionnez la section **Apparence**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.
3. Si vous souhaitez limiter l'accès à Kaspersky Endpoint Security via un mot de passe, procédez comme suit :
   a. Cochez la case **Activer la protection par mot de passe**.
   b. Cliquez sur le bouton **Configuration**.

La fenêtre **Protection par mot de passe** s'ouvre.

c. Dans le champ **Nouveau mot de passe**, saisissez le mot de passe d'accès à l'application.

d. Dans le champ **Confirmation du mot de passe**, saisissez à nouveau le mot de passe.

e. Dans le groupe **Zone d'action du mot de passe**, indiquez les opérations de l'application que l'utilisateur pourra exécuter uniquement après avoir saisi le mot de passe :

- Choisissez l'option **Toutes les opérations (sauf les notifications de danger)** si vous souhaitez limiter l'accès à toutes les opérations de l'application.
- Choisissez l'option **Opérations distinctes** si vous souhaitez désigner les opérations manuellement.

f. Si vous avez choisi l'option **Opérations distinctes**, cochez les cases en regard des noms des opérations concernées :

- **Configuration des paramètres de l'application**.
- **Arrêt de l'application**.
- **Désactivation des modules de la protection et arrêt des tâches d'analyse**.
- **Désactivation des modules de contrôle**.
- **Suppression d'une licence**.
- **Suppression de l'application**.

g. Cliquez sur le bouton **OK**.

Il est conseillé d'être prudent au moment de décider de limiter l'accès à l'application par mot de passe. Si vous avez oublié le mot de passe, il faudra contacter le service du Support technique de Kaspersky Lab afin d'obtenir les instructions sur l'annulation de la protection par mot de passe (http://support.kaspersky.com/fr/corporate).

4. Si vous souhaitez lever la restriction d'accès par mot de passe à Kaspersky Endpoint Security, procédez comme suit :

a. Décochez la case **Activer la protection par mot de passe**.

b. Cliquez sur le bouton **Exporter**.

L'application vérifie si l'opération d'annulation de la restriction d'accès est protégée.

- Si l'annulation de la restriction de l'accès aux applications n'est pas protégée par un mot de passe, alors la restriction de l'accès à Kaspersky Endpoint Security est levée.
- Si l'opération d'annulation de la restriction de l'accès à l'application est protégée par un mot de passe, la fenêtre **Vérification du mot de passe** s'ouvre. Cette fenêtre apparaît chaque fois que l'utilisateur exécute une opération protégée par un mot de passe.

c. Saisissez le mot de passe dans le champ **Mot de passe** de la fenêtre **Vérification du mot de passe**.

d. Cochez la case **Enregistre le mot de passe pour cette session** si vous souhaitez ne pas devoir saisir le mot de passe pour exécuter à nouveau cette opération au cours de la même session. La restriction de l'accès à l'application sera levée après le prochain lancement de Kaspersky Endpoint Security.

Si la case **Mémoriser le mot de passe pour la session actuelle du fonctionnement de l'application** n'est pas cochée, cela signifie que l'application demandera le mot de passe à chaque tentative d'exécution de cette application.

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

5. Cliquez sur le bouton **Enregistrer** dans la fenêtre de configuration des paramètres de l'application afin d'enregistrer les modifications introduites.

MODIFICATION DU MOT DE PASSE D'ACCES A KASPERSKY ENDPOINT SECURITY

Pour modifier le mot de passe d'accès à Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** de la partie gauche de la fenêtre, sélectionnez la section **Apparence**.

   Les paramètres de l'interface utilisateur apparaissent dans la partie droite de la fenêtre.
3. Si la protection par mot de passe est désactivée, cochez la case **Activer la protection par mot de passe**.
4. Cliquez sur le bouton **Configuration**.

   La fenêtre **Protection par mot de passe** s'ouvre.
5. Dans le champ **Ancien mot de passe**, saisissez le mot de passe d'accès actuel à l'application.
6. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe d'accès à l'application.
7. Dans le champ **Confirmation du mot de passe**, saisissez à nouveau le nouveau mot de passe.
8. Cliquez sur le bouton **OK**.

   L'application vérifie les valeurs saisies.

   - Si l'ancien mot de passe est correct et si le nouveau mot de passe et sa confirmation correspondent, alors le nouveau mot de passe entre en vigueur.

     La fenêtre **Protection par mot de passe** se ferme.
   - Si le mot de passe saisi dans le champ **Ancien mot de passe** est incorrect, un message contextuel propose de retenter la saisie. Répétez l'étape 5 des instructions, puis cliquez sur **Ok**.

     La fenêtre **Protection par mot de passe** se ferme.
   - Si le mot de passe saisi dans le champ **Confirmation du mot de passe** est incorrect, un message contextuel propose de retenter la saisie. Répétez l'étape 7 des instructions, puis cliquez sur **OK**.

     La fenêtre **Protection par mot de passe** se ferme.
9. Cliquez sur le bouton **Enregistrer** dans la fenêtre de configuration des paramètres de l'application afin d'enregistrer les modifications introduites.

ADMINISTRATION A DISTANCE VIA KASPERSKY SECURITY CENTER

Cette section présente l'administration à distance de Kaspersky Endpoint Security via Kaspersky Security Center.

DANS CETTE SECTION

ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY

L'application Kaspersky Security Center a été développée pour l'exécution centralisée des principales tâches d'administration du système de protection antivirus des ordinateurs du réseau d'une entreprise impliquant des applications appartenant à la suite Kaspersky Open Space Security. Kaspersky Security Center prend en charge toutes les configurations réseau utilisant le protocole TCP/IP.

Kaspersky Security Center permet de lancer et d'arrêter Kaspersky Endpoint Security à distance sur un poste client et de configurer les paramètres de fonctionnement de l'application.

DANS CETTE SECTION

LANCEMENT ET ARRET DE KASPERSKY ENDPOINT SECURITY SUR LE POSTE CLIENT

Pour lancer ou arrêter Kaspersky Endpoint Security sur le poste client, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.
4. Dans la liste des postes client, sélectionnez l'ordinateur sur lequel vous souhaitez lancer ou arrêter Kaspersky Endpoint Security.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Sélectionnez l'option **Propriétés**.
   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.

6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.

   Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky Lab installées sur le poste client.

7. Choisissez l'application Kaspersky Endpoint Security 8 for Windows.

8. Réalisez les opérations suivantes :

   - Si vous souhaitez lancer Kaspersky Endpoint Security, cliquez sur le bouton  à droite de la liste des applications de Kaspersky Lab ou procédez comme suit :

     a. Cliquez-droit pour ouvrir le menu contextuel de l'application Kaspersky Endpoint Security 8 for Windows et choisissez l'option **Propriétés** ou cliquez sur le bouton **Propriétés** situé sous la liste des applications de Kaspersky Lab.

        La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Windows** s'ouvre à l'onglet **Général**.

     b. Cliquez sur **Lancer**.

   - Si vous souhaitez arrêter Kaspersky Endpoint Security, cliquez sur le bouton  à droite de la liste des applications de Kaspersky Lab ou procédez comme suit :

     a. Cliquez-droit pour ouvrir le menu contextuel de l'application Kaspersky Endpoint Security 8 for Windows et choisissez l'option **Propriétés** ou cliquez sur le bouton **Propriétés** situé sous la liste des applications.

        La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Windows** s'ouvre à l'onglet **Général**.

     b. Cliquez sur le bouton **Arrêter**.

CONFIGURATION DES PARAMETRES DE KASPERSKY ENDPOINT SECURITY

Pour configurer les paramètres de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.
4. Dans la liste des postes client, choisissez l'ordinateur pour lequel vous souhaitez configurer les paramètres de Kaspersky Endpoint Security.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Sélectionnez l'option **Propriétés**.
   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.

6. Dans la fenêtre des propriétés du poste client, choisissez la section **Applications**.

   Dans la partie droite de la fenêtre des propriétés du poste client figure la liste des applications de Kaspersky Lab installées sur le poste client.

7. Choisissez l'application Kaspersky Endpoint Security 8 for Windows.

8. Exécutez une des actions suivantes :

   - Cliquez-droit afin d'ouvrir le menu contextuel de l'application Kaspersky Endpoint Security 8 for Windows. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés** sous la liste des applications de Kaspersky Lab.

   La fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Windows** s'ouvre.

9. Dans la section **Paramètres complémentaires**, configurez les paramètres de fonctionnement de Kaspersky Endpoint Security, ainsi que les paramètres des rapports et des sauvegardes.

   Les autres sections de la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Windows** sont standard pour l'application Kaspersky Security Center. Elles sont décrites dans le *Guide de l'administrateur de Kaspersky Security Center*.

   Si l'application est soumise à une stratégie qui interdit la modification de certains paramètres, ceux-ci ne seront pas accessibles lors de la configuration des paramètres.

10. Dans la fenêtre **Paramètres de l'application Kaspersky Endpoint Security 8 for Windows**, cliquez sur le bouton **OK** afin d'enregistrer les modifications.

GESTION DES TACHES

Cette section fournit des informations sur la gestion des tâches pour Kaspersky Endpoint Security. Pour en savoir plus sur le concept de gestion des tâches via Kaspersky Security Center, consultez le *Guide de l'administrateur de Kaspersky Security Center*.

DANS CETTE SECTION

PRESENTATION DES TACHES POUR KASPERSKY ENDPOINT SECURITY

Kaspersky Security Center utilise des tâches pour gérer le fonctionnement des applications de Kaspersky Lab installées sur les postes client. Les tâches se chargent des fonctions de gestion principales telles que l'installation de licences, l'analyse de l'ordinateur ou la mise à jour des bases et des modules de l'application.

Pour utiliser Kaspersky Endpoint Security via Kaspersky Security Center, vous devez créer les types de tâches suivants :

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe définies pour des ordinateurs clients appartenant à un ou plusieurs groupes d'administration différents ;
- des tâches pour des sélections d'ordinateurs qui n'appartiennent pas à des groupes d'administration.

> Les tâches pour les sélections d'ordinateurs qui n'appartiennent pas à des groupes d'administration sont exécutées uniquement pour les postes clients définis dans les paramètres de la tâche. Si de nouveaux postes client sont ajoutés à une sélection d'ordinateurs pour laquelle une tâche a été créée, cette tâche ne s'applique pas à ces nouveaux postes. Dans ce cas, il faut créer une tâche ou modifier les paramètres de la tâche existante.

Dans le cadre de l'administration à distance de Kaspersky Endpoint Security, vous pouvez travailler avec les tâches suivantes :

- **Inventaire**. Pendant l'exécution de la tâche Kaspersky Endpoint Security collecte des informations sur tous les fichiers exécutables des applications de l'ordinateur.
- **Mise à jour**. Pendant l'exécution de la tâche Kaspersky Endpoint Security actualise les bases et les modules de l'application conformément aux paramètres de mise à jour définis.
- **Restauration de la mise à jour**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security revient à la dernière mise à jour des bases et des modules.
- **Recherche de virus**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security recherche la présence éventuelle de virus et d'autres programmes dangereux dans les secteurs de l'ordinateur définis via les paramètres de la tâche.
- **Recherche de vulnérabilités**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security recherche des vulnérabilités dans les applications installées sur l'ordinateur.
- **Installation du fichier de licence**. Pendant l'exécution de la tâche, Kaspersky Endpoint Security installe le fichier de licence pour l'activation de l'application ou pour l'installation d'une licence complémentaire.

Vous pouvez réaliser les opérations suivantes sur les tâches :

- lancer, arrêter, suspendre ou reprendre l'exécution de la tâche ;
- créer des tâches ;
- modifier les paramètres des tâches.

CREATION D'UNE TACHE LOCALE

Pour créer une tâche locale, procédez comme suit:

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.
4. Sélectionnez, dans la liste des postes client, l'ordinateur pour lequel vous souhaitez créer une tâche locale.
5. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Sélectionnez l'option **Propriétés**.
   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.
6. Choisissez l'onglet **Tâches**.
7. Cliquez sur le bouton **Ajouter**.

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

CREATION D'UNE TACHE DE GROUPE

Pour créer une tâche de groupe, procédez comme suit:

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Ouvrez le dossier **Ordinateurs administrés** de l'arborescence de la console.
3. Dans le volet des résultats, choisissez l'onglet **Tâches**.
4. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Créer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Créer** → **Tâche**.

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

CREATION D'UNE TACHE POUR UNE SELECTION D'ORDINATEURS

Pour créer une tâche pour une sélection d'ordinateurs, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Ouvrez le dossier **Tâches pour des sélections d'ordinateurs** de l'arborescence de la console.
3. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Créer**.
   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Créer** → **Tâche**.

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

LANCEMENT, ARRET, SUSPENSION ET REPRISE DE L'EXECUTION D'UNE TACHE

Si l'application Kaspersky Endpoint Security est exécutée sur le poste client, vous pouvez lancer, arrêter, suspendre ou reprendre l'exécution d'une tâche sur celui-ci via Kaspersky Security Center. Si Kaspersky Endpoint Security est arrêté, les tâches en cours d'exécution sont arrêtées et il n'est plus possible de gérer le lancement, l'arrêt, la suspension et la reprise des tâches via Kaspersky Security Center.

Pour lancer, arrêter, suspendre ou reprendre l'exécution d'une tâche locale, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.
4. Choisissez dans la liste le poste client sur lequel vous souhaitez lancer, arrêter, suspendre ou reprendre une tâche locale.
5. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Sélectionnez l'option **Propriétés**.
   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.
6. Choisissez l'onglet **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.
7. Sélectionnez la tâche locale que vous voulez lancer, arrêter, suspendre ou reprendre.

8. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche locale. Sélectionnez **Démarrer/Arrêter/Suspendre/Reprendre**.
   - Cliquez sur le bouton  à droite de la liste des tâches locales afin de lancer ou d'arrêter une tâche locale.
   - Cliquez sur le bouton **Propriétés** sous la liste des tâches locales. La fenêtre **Propriétés de la tâche <nom de la tâche>** s'ouvre. Sous l'onglet **Général** de la fenêtre **Propriétés de la tâche <nom de la tâche>**, cliquez sur le bouton **Lancer/Arrêter/Suspendre/Reprendre**.

Pour lancer, arrêter, suspendre ou reprendre une tâche de groupe, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration pour lequel vous souhaitez lancer/arrêter/suspendre/reprendre une tâche de groupe.
3. Dans le volet des résultats, choisissez l'onglet **Tâches**.

   La liste des tâches de groupe apparaît dans la partie droite de la fenêtre.
4. Dans la liste des tâches de groupe, sélectionnez la tâche que vous voulez lancer, arrêter, suspendre ou reprendre.
5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche de groupe. Sélectionnez **Démarrer/Arrêter/Suspendre/Reprendre**.
   - Cliquez sur le bouton  à droite de la liste des tâches de groupe afin de lancer ou d'arrêter une tâche de groupe.

Pour lancer, arrêter, suspendre ou reprendre l'exécution d'une tâche pour une sélection d'ordinateurs, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Tâches pour les sélections d'ordinateurs** de l'arborescence de la console, choisissez la tâche pour la sélection d'ordinateurs que vous souhaitez lancer, arrêter, suspendre ou reprendre.
3. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche pour la sélection d'ordinateurs. Sélectionnez **Démarrer/Arrêter/Suspendre/Reprendre**.
   - Cliquez sur le bouton  à droite de la liste des tâches pour les sélections d'ordinateurs afin de lancer ou d'arrêter la tâche.

MODIFICATION DES PARAMETRES DE LA TACHE

Les paramètres des tâches de Kaspersky Endpoint Security que vous pouvez configurer via l'interface de Kaspersky Security Center sont identiques aux paramètres des tâches configurables via l'interface locale de Kaspersky Endpoint Security. Vous pouvez configurer les paramètres de la tâche lors de la création de celle-ci ou modifier ses paramètres après sa création.

Pour modifier les paramètres d'une tâche locale, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration auquel appartient le poste client qui vous intéresse.
3. Dans le volet des résultats, choisissez l'onglet **Ordinateurs**.
4. Dans la liste des postes client, choisissez l'ordinateur pour lequel vous souhaitez configurer les paramètres de Kaspersky Endpoint Security.
5. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel du poste client. Sélectionnez l'option **Propriétés**.
   - Dans le menu **Actions**, choisissez l'option **Propriétés de l'ordinateur**.

   La fenêtre des propriétés du poste client s'ouvre.
6. Choisissez la section **Tâches**.

   La liste des tâches locales apparaît dans la partie droite de la fenêtre.
7. Sélectionnez la tâche locale requise dans la liste des tâches locales.
8. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel de la tâche. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés**.

   La fenêtre **Propriétés : <nom de la tâche de groupe>** s'ouvre
9. Dans la fenêtre **Propriétés: <nom de la tâche locale>**, choisissez la section **Paramètres**.
10. Modifiez les paramètres de la tâche locale.
11. Dans la fenêtre **Propriétés: <nom de la tâche locale>**, cliquez sur **OK** afin d'enregistrer les modifications introduites.

Pour modifier les paramètres d'une tâche de groupe, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe d'administration souhaité.
3. Dans le volet des résultats, choisissez l'onglet **Tâches**.

   La liste des tâches de groupe apparaît dans la partie inférieure du volet des tâches.
4. Sélectionnez la tâche de groupe requise dans la liste des tâches de groupe.

5. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Modifier les paramètres de la tâche** situé à droite de la liste des tâches de groupe.

   La fenêtre **Propriétés de la tâche <nom de la tâche de groupe>** s'ouvre.

6. Dans la fenêtre **Propriétés: <nom de la tâche de groupe>**, choisissez la section **Paramètres**.
7. Modifiez les paramètres de la tâche de groupe.
8. Dans la fenêtre **Propriétés: <nom de la tâche de groupe>**, cliquez sur **OK** afin d'enregistrer les modifications introduites.

Pour modifier les paramètres de la tâche pour une sélection d'ordinateurs, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Tâches pour des sélections d'ordinateurs** de l'arborescence de la console, sélectionnez la tâche dont vous souhaitez modifier les paramètres.
3. Exécutez une des actions suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche pour la sélection d'ordinateurs. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Modifier les paramètres de la tâche** situé à droite de la liste des tâches pour des sélections d'ordinateurs.

   La fenêtre **Propriétés: <nom de la tâche pour une sélection d'ordinateurs>** s'ouvre.

4. Dans la fenêtre **Propriétés: <nom de la tâche pour une sélection d'ordinateurs>**, choisissez la section **Paramètres**.
5. Modifiez les paramètres de la tâche pour une sélection d'ordinateurs.
6. Dans la fenêtre **Propriétés: <nom de la tâche pour une sélection d'ordinateurs>**, cliquez sur **OK** afin d'enregistrer les modifications introduites.

Tous les onglets de la fenêtre des propriétés des tâches, à l'exception de l'onglet **Paramètres**, sont standards pour Kaspersky Security Center. Ils sont décrits en détail dans le *Guide de l'administrateur de Kaspersky Security Center*. L'onglet **Paramètres** contient les paramètres spécifiques à Kaspersky Endpoint Security. Son contenu varie en fonction du type de tâche sélectionné.

ADMINISTRATION DES STRATEGIES

Cette section explique comment créer et configurer des stratégies pour Kaspersky Endpoint Security 8 for Windows. Pour en savoir plus sur le concept de gestion des stratégies via Kaspersky Security Center, consultez le *Guide de l'administrateur de Kaspersky Security Center*.

DANS CETTE SECTION

PRESENTATION DES STRATEGIES

Les stratégies permettent de définir des valeurs identiques pour les paramètres de fonctionnement de Kaspersky Endpoint Security sur tous les postes client appartenant au groupe d'administration.

Les paramètres définis par une stratégie peuvent être redéfinis pour des ordinateurs particuliers au sein du groupe d'administration. Vous pouvez réaliser cette opération localement à l'aide de Kaspersky Endpoint Security. Vous ne pouvez modifier localement que les paramètres dont la modification n'est pas interdite par la stratégie.

L'état du cadenas près du paramètre de la stratégie définit si ce paramètre peut être modifié sur le poste client :

- Si le paramètre est verrouillé à l'aide d'un cadenas (), vous ne pouvez pas modifier sa valeur localement. Tous les postes client du groupe d'administration utilisent alors la valeur du paramètre définie par la stratégie.
- Si le paramètre n'est pas verrouillé à l'aide d'un cadenas (), cela signifie que vous pouvez modifier localement la valeur du paramètre. Les valeurs des paramètres définies localement sont utilisées pour tous les postes clients du groupe d'administration. La valeur du paramètre définie dans la stratégie n'est pas appliquée.

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

Vous pouvez réaliser les opérations suivantes sur les stratégies :

- créer une stratégie ;
- modifier les paramètres d'une stratégie ;
- supprimer une stratégie ;
- modifier l'état d'une stratégie.

Les informations relatives aux stratégies qui ne concernent pas l'interaction avec Kaspersky Endpoint Security sont reprises dans le *Guide de l'administrateur de Kaspersky Security Center*.

CREATION D'UNE STRATEGIE

Pour créer une stratégie, procédez comme suit:

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs gérés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration dont fait partie le poste client.
3. Dans le volet des résultats, choisissez l'onglet **Stratégies**.
4. Exécutez une des actions suivantes :
   - Cliquez sur le bouton **Nouvelle stratégie**.
   - Cliquez-droit pour ouvrir le menu contextuel. Sélectionnez l'option **Créer** → **Stratégie**.

   L'Assistant de création de stratégie démarre.
5. Suivez les instructions de l'Assistant de création de stratégie.

MODIFICATION DES PARAMETRES DE LA STRATEGIE

Pour modifier les paramètres de la stratégie, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Dans le dossier **Ordinateurs administrés** de l'arborescence de la console, ouvrez le dossier portant le nom du groupe d'administration dont vous souhaitez modifier les paramètres de la stratégie.
3. Dans le volet des résultats, choisissez l'onglet **Stratégies**.
4. Sélectionnez la stratégie requise.
5. Exécutez une des actions suivantes :
   - Cliquez-droit pour ouvrir le menu contextuel de la stratégie. Sélectionnez l'option **Propriétés**.
   - Cliquez sur le bouton **Modifier la stratégie** situé à droite de la liste des stratégies.

   La fenêtre **Propriétés: <nom de la stratégie>** s'ouvre.

   Les paramètres de la stratégie pour Kaspersky Endpoint Security 8 comprennent les paramètres des tâches (cf. section "Modification des paramètres de la tâche" à la page 251) et les paramètres de l'application (cf. section "Configuration des paramètres de Kaspersky Endpoint Security" à la page 246). Les sections **Protection** et **Contrôle** de la fenêtre **Propriétés: <nom de la stratégie>** reprennent les paramètres des tâches, tandis que la section **Paramètres complémentaires** contient les paramètres de l'application.
6. Modifiez les paramètres de la stratégie.
7. Dans la fenêtre **Propriétés: <nom de la tâche de la stratégie>**, cliquez sur **OK** afin d'enregistrer les modifications introduites.

CONSULTATION DES RECLAMATIONS DES UTILISATEURS DANS LE REFERENTIEL DES EVENEMENTS DE KASPERSKY SECURITY CENTER

Une fonction des modules Contrôle du lancement des applications (cf. section "Modification des modèles de messages du Contrôle du lancement des applications" à la page 129), Contrôle des périphériques (cf. section "Modification des modèles des messages du Contrôle des périphériques" à la page 156) et Contrôle Internet (cf. section "Modification des modèles de messages du Contrôle Internet" à la page 169) permet aux utilisateurs du réseau local de l'organisation dont les ordinateurs sont dotés de Kaspersky Endpoint Security permet d'envoyer des réclamations.

Il existe deux méthodes pour envoyer une réclamation :

- Sous la forme d'un événement dans le référentiel des événements de Kaspersky Security Center. La réclamation de l'utilisateur est envoyée dans le référentiel des événements de Kaspersky Security Center si la version de Kaspersky Endpoint Security installée sur l'ordinateur de l'utilisateur fonctionne sous une stratégie active.
- Via courrier électronique. La réclamation de l'utilisateur est envoyée par courrier électronique si la version Kaspersky Endpoint Security installée sur l'ordinateur de l'utilisateur ne fonctionne pas sous une stratégie ou une stratégie mobile.

Pour consulter la réclamation de l'utilisateur dans le référentiel des événements de Kaspersky Security Center, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Security Center.
2. Ouvrez le dossier **Sélection d'événements\Evénements\Avertissements** de l'arborescence de la console.

   La liste de tous les avertissements, y compris les réclamations envoyées par les utilisateurs du réseau local de l'entreprise, apparaît dans la zone de travail de Kaspersky Security Center. La zone de travail de Kaspersky Security Center se trouve à droite de l'arborescence de la console.
3. Sélectionnez la réclamation dans la liste des événements.
4. Ouvrez la liste des événements d'une des méthodes suivantes :

   - Double-cliquez gauche sur l'événement dans la liste.
   - Cliquez-droit pour ouvrir le menu contextuel de l'événement. Choisissez l'option **Propriétés** dans le menu contextuel des événements.
   - Cliquez sur le bouton **Ouvrir les propriétés de l'événement** à droite de la liste des événements.

PARTICIPATION AU KASPERSKY SECURITY NETWORK

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

DANS CETTE SECTION

PRESENTATION DE LA PARTICIPATION AU KASPERSKY SECURITY NETWORK

Pour renforcer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs du monde entier. Le réseau *Kaspersky Security Network* permet de récolter ces données.

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

L'implication des utilisateurs dans le Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des moyens de neutralisation et de réduire le nombre de faux positifs.

De plus, la participation au Kaspersky Security Network donne accès aux données sur la réputation des applications et des sites Internet.

Si vous participez au Kaspersky Security Network, certaines statistiques obtenues suite au fonctionnement de Kaspersky Endpoint Security sur votre ordinateur sont transmises automatiquement à Kaspersky Lab.

Si l'ordinateur est administré par le serveur d'administration Kaspersky Security Center, il est possible d'utiliser le service *KSN Proxy.*

KSN Proxy est un service qui garantit l'interaction entre l'infrastructure du Kaspersky Security Network et de l'ordinateur de l'utilisateur.

Le recours au service KSN Proxy offre les possibilités suivantes :

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

Pour en savoir plus sur le service KSN Proxy, lisez le *Guide de l'administrateur de Kaspersky Security Center*.

La configuration des paramètres d'utilisation du service KSN Proxy s'opère via les propriétés des stratégies de *Kaspersky Security Center* (cf. section "*Administration des stratégies*" à la page 253).

Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Les données que Kaspersky Endpoint Security transmet au Kaspersky Security Network sont décrites dans l'accord KSN.

La participation au Kaspersky Security Network est volontaire. La décision de participer ou non à Kaspersky Security Network est prise lors de l'installation de Kaspersky Endpoint Security. Il est toutefois possible de la modifier à tout moment (cf. section "Activation et désactivation de l'utilisation de Kaspersky Security Network" à la page 258).

ACTIVATION ET DESACTIVATION DE L'UTILISATION DE KASPERSKY SECURITY NETWORK

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

1. Ouvrez la fenêtre de configuration de l'application (cf. page 51).
2. Dans le groupe **Paramètres avancés** de la partie gauche de la fenêtre, sélectionnez la section **Paramètres de KSN**.

   Les paramètres de Kaspersky Security Network apparaissent dans la partie droite de la fenêtre.
3. Exécutez une des actions suivantes :
   - Cochez la case **Utiliser KSN dans le logiciel** si vous souhaitez activer l'utilisation des services de Kaspersky Security Network.
   - Décochez la case **Utiliser KSN dans le logiciel** si vous ne souhaitez pas activer l'utilisation des services de Kaspersky Security Network.
4. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées.

VERIFICATION DE CONNEXION A KASPERSKY SECURITY NETWORK

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Cloud-based protection KSN**.

   La fenêtre **Kaspersky Security Network** s'ouvre.

   La partie gauche de la fenêtre **Kaspersky Security Network** affiche le mode de connexion aux services Kaspersky Security Network sous la forme du bouton rond **KSN** :
   - Si Kaspersky Endpoint Security est connecté aux services de Kaspersky Security Network, alors le bouton **KSN** est vert. L'état *Activé* s'affiche sous le bouton **KSN**. Les statistiques relatives à la réputation des fichiers et des ressources Internet apparaissent dans la partie droite de la fenêtre.

     Kaspersky Endpoint Security récolte les statistiques d'utilisation du KSN lors de l'ouverture de la fenêtre **Kaspersky Security Network**. Les statistiques ne sont pas mises à jour en temps réel.
   - Si Kaspersky Endpoint Security n'est pas connecté aux services de Kaspersky Security Network, alors le bouton **KSN** est gris. L'état *Désactivé* s'affiche sous le bouton **KSN**.

     La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :
     - Votre ordinateur n'est pas connecté à Internet.
     - Vous ne participez pas au Kaspersky Security Network.
     - Votre licence d'utilisation de Kaspersky Endpoint Security est limitée.

APPEL AU SERVICE D'ASSISTANCE TECHNIQUE

Cette section présente les différentes méthodes d'obtention de l'assistance technique et les conditions à remplir pour pouvoir bénéficier de l'aide du service d'assistance technique.

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation de l'application ou dans une des sources des informations relatives à l'application (cf. section "Sources d'informations sur l'application" à la page 13), contactez le service du Support Technique de Kaspersky Lab. Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application. Si l'ordinateur est infecté, les experts du service d'assistance technique essayeront de vous aider à supprimer les conséquences de l'exécution des programmes malveillants.

Avant de contacter le Service du Support Technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/support/rules).

Vous pouvez contacter les experts du service d'assistance technique d'une des manières suivantes :

- Via téléphone. Vous pouvez contacter les experts du service d'assistance technique en France.
- Via une demande depuis Mon Espace Personnel sur le site Internet du service d'assistance technique. Cette méthode permet de contacter les experts du service d'assistance technique via un formulaire.

Pour obtenir l'assistance technique, vous devez être un utilisateur inscrit de la version commerciale de Kaspersky Endpoint Security 8 for Windows. Les utilisateurs des versions d'évaluation n'ont pas accès à l'assistance technique.

COLLECTE D'INFORMATIONS POUR LE SERVICE D'ASSISTANCE TECHNIQUE

Une fois que les experts du Service d'assistance technique sont au courant du problème survenu, ils peuvent vous demander de créer un *fichier de trace*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

De plus, les experts du Service d'assistance technique peuvent avoir besoin d'informations complémentaires sur le système d'exploitation, les processus lancés sur l'ordinateur, ainsi que des rapports détaillés sur le fonctionnement des modules de l'application et de vidage de la mémoire.

A l'aide de Kaspersky Endpoint Security vous pouvez récolter toutes les informations nécessaires. Vous pouvez télécharger les informations recueillies sur le serveur de Kaspersky Lab ou les enregistrer sur le disque dur pour les envoyer plus tard à un moment opportun.

DANS CETTE SECTION

CREATION D'UN FICHIER DE TRACE

Pour créer un fichier de trace, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le bouton **Suivi du système**.

   La fenêtre **Informations pour le service d'assistance technique** s'ouvre.
4. **Choisissez le niveau de traçage** dans la liste déroulante Niveau.

   Il est recommandé de demander au spécialiste du Support technique le niveau du traçage requis. Si les indications du Support technique sont absentes, il est recommandé d'installer le niveau de traçage **Normal (500)**.
5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation où le problème apparaît.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Une fois le fichier de trace créé, vous pouvez procéder au téléchargement des résultats de traçage sur le serveur de Kaspersky Lab (cf. section "Envoi des fichiers de données sur le serveur du Service d'assistance technique" à la page 260).

ENVOI DES FICHIERS DE DONNEES SUR LE SERVEUR DU SERVICE D'ASSISTANCE TECHNIQUE

Il faut envoyer l'archive contenant les informations sur le système d'exploitation, les traçages et les vidages de la mémoire aux experts du Service d'assistance technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du Support technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans Mon Espace Personnel sur le site Internet du Support technique lorsque des requêtes actives sont présentes.

Pour envoyer les fichiers de données sur le serveur du Support technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le bouton **Suivi du système**.

   La fenêtre **Informations pour le service d'assistance technique** s'ouvre.
4. Dans la fenêtre **Informations pour le service d'assistance technique** dans le groupe **Actions**, cliquez sur le bouton **Charger des informations en vue d'un soutien sur le serveur**.

La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.

5. Dans la fenêtre **Chargement des informations pour l'assistance sur le serveur**, cochez les cases à côté des fichiers que vous souhaitez envoyer au Service d'assistance technique.

6. Cliquez sur le bouton **Envoyer**.

   La fenêtre **Numéro de requête** s'ouvre.

7. Saisissez le numéro attribué à votre requête par le Service d'assistance technique que vous avez contacté depuis Mon Espace Personnel dans la fenêtre **Numéro de requête**.

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

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du Support technique.

ENREGISTREMENT DES FICHIERS DE DONNEES SUR LE DISQUE DUR

S'il est impossible de contacter le Service d'assistance technique pour une raison ou pour une autre, vous pouvez enregistrer les fichiers de données sur votre ordinateur et les envoyer plus tard depuis votre Espace Personnel.

Pour enregistrer les fichiers de données sur le disque dur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page 49).

2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Support Technique**.

3. Dans la fenêtre **Assistance technique**, cliquez sur le bouton **Suivi du système**.

   La fenêtre **Informations pour le service d'assistance technique** s'ouvre.

4. Dans la fenêtre **Informations pour le service d'assistance technique** dans le groupe **Actions**, cliquez sur le bouton **Charger des informations en vue d'un soutien sur le serveur**.

   La fenêtre **Chargement des informations pour l'assistance sur le serveur** s'ouvre.

5. Dans la fenêtre **Chargement des informations pour l'assistance sur le serveur**, cochez les cases à côté des fichiers de données que vous souhaitez envoyer au Service d'assistance technique.

6. Cliquez sur le bouton **Envoyer**.

   La fenêtre **Numéro de requête** s'ouvre.

7. Dans la fenêtre **Numéro de requête**, cliquez sur le bouton **Annuler**.

8. Confirmez dans la fenêtre déroulante que vous voulez enregistrer les fichiers des données sur le disque dur, en cliquant sur le bouton **Oui**.

   La fenêtre standard de Microsoft Windows s'ouvre pour enregistrer une archive.

9. Dans le champ **Nom du fichier**, saisissez le nom de l'archive et cliquez sur le bouton **Enregistrer**.

ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du service d'assistance Français (http://www.kaspersky.com/fr/support).

Avant de contacter le service du Support Technique, vous devez recueillir des informations sur l'ordinateur et les logiciels antivirus installés (http://support.kaspersky.com/support/details). Ceci permettra nos experts à vous venir en aide le plus vite possible.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

Mon Espace Personnel : c'est un espace qui vous est réservé (https://support.kaspersky.com/fr/PersonalCabinet) sur le site du Service du Support Technique.

Pour accéder à Mon Espace Personnel, vous devez procéder à l'enregistrement sur la page d'enregistrement (https://support.kaspersky.com/fr/personalcabinet/registration/) et obtenir votre numéro client et votre mot de passe pour Mon Espace Personnel. Pour ce faire, vous devez saisir votre code d'activation (cf. section "Présentation du code d'activation" à la page 42) ou indiquer le chemin d'accès au fichier clé (cf. section "Présentation du fichier clé" à la page 42).

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au support technique et au laboratoire d'étude des virus.
- Communiquer avec le support technique sans devoir envoyer des messages électroniques.
- Suivre l'état de vos demandes en temps réel.
- Consulter l'historique complet de votre interaction avec le support technique.
- Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.

Requête électronique adressée au Service d'assistance technique

Vous pouvez envoyer une demande par voie électronique au service d'assistance technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- type de demande ;
- nom et numéro de version de l'application ;
- texte de la demande ;
- numéro de client et mot de passe ;
- adresse de messagerie.

Demande électronique adressée au laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au service d'assistance technique mais au laboratoire d'étude des virus.

Vous pouvez envoyer les types de demandes suivantes au laboratoire d'étude des virus :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Endpoint Security ne détecte aucune infection.

  Les experts du laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de découverte d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif du logiciel antivirus* : Kaspersky Endpoint Security considère un certain fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas.

Demande de description d'un programme malveillant : vous souhaitez obtenir la description d'un virus découvert par Kaspersky Endpoint Security sur la base du nom de ce virus.

Vous pouvez également envoyer des demandes au laboratoire d'étude des virus sans vous enregistrer dans Mon Espace Personnel. Utilisez pour ce faire le formulaire de demande en ligne (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr). Pour ce faire, vous ne devez pas indiquer le code d'activation de l'application.

GLOSSAIRE

A

Agent d'administration

Module de l'application Kaspersky Security Center qui assure l'interaction entre le serveur d'administration et les applications de Kaspersky Lab installées sur un nœud spécifique du réseau (poste de travail ou serveur). Ce module est unique pour toutes les applications Windows du portefeuille de la société. Il existe une version distincte de l'Agent d'administration pour les versions Novell, Unix et Mac des logiciels de Kaspersky Lab.

Analyse heuristique

La technologie d'identification des menaces impossibles à reconnaître à l'aide des bases des applications de Kaspersky Lab. Permet d'identifier les fichiers probablement infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

Après avoir identifié le code malveillant, l'analyse heuristique attribue aux fichiers concernés l'état potentiellement infecté.

Analyse sur la base de signatures

La technologie d'identification des menaces qui utilise les bases de Kaspersky Endpoint Security contenant les descriptions des menaces connues et les méthodes de leur élimination. La protection selon cette méthode offre le niveau minimum de sécurité. Conformément aux recommandations des spécialistes de Kaspersky Lab, cette méthode est toujours activée.

Analyseur heuristique

La fonction composée de Kaspersky Endpoint Security qui exécute l'analyse heuristique.

Archive

Fichier qui contient un ou plusieurs fichiers qui peuvent être des archives.

B

Base des URL de phishing

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Base des URL suspectes

Liste des d'adresses des sites Internet dont le contenu pourrait constituer une menace. La liste est composée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

Bases

Bases de données composées par les experts de Kaspersky Lab et contenant une description détaillée de toutes les menaces informatiques connues de Kaspersky Lab à ce jour ainsi que les moyens de les détecter et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

F

FAUX POSITIF

Situation où un objet non infecté est considéré comme infecté par l'application de Kaspersky Lab car son code évoque celui d'un virus.

FICHIER INFECTE

Le fichier qui contient un code malveillant (pendant l'analyse un code de menace connue a été découvert). Les experts de Kaspersky Lab vous déconseillent de manipuler de tels fichiers car ils pourraient infecter votre ordinateur.

FICHIER POTENTIELLEMENT INFECTE

Fichier qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

FICHIER POTENTIELLEMENT INFECTE

Le fichier qui contient le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

FORME NORMALISEE DE L'ADRESSE DU SITE INTERNET

La forme normalisée de l'adresse du site Internet est une représentation écrite de l'adresse du site Internet obtenue grâce à la normalisation. La normalisation est un processus de modification de la représentation écrite de l'adresse du site Internet conformément aux règles spécifiques (par exemple, exclusion de login HTTP, de mot de passe et de port de connexion de la représentation écrite de l'adresse du site Internet, conversion des caractères majuscules de l'adresse du site Internet en caractères minuscules).

Le but de la normalisation des adresses des sites Internet dans le contexte de la protection antivirus est de vérifier une seule fois les adresses des sites Internet qui ont une équivalence physique, mais qui sont différentes du point de vue de la syntaxe.

Exemple :

La forme non normalisée de l'adresse : www.Example.com\.

La forme normalisée de l'adresse : www.example.com.

G

GROUPE D'ADMINISTRATION

Ensemble d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour faciliter l'administration. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

L

LISTE "NOIRE" DES ADRESSES

Liste des adresses de messagerie électronique bloquées par l'application de Kaspersky Lab, quel que soit le contenu des messages.

M

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques.

Pour créer le masque de fichier, vous pouvez utiliser tous les caractères autorisés dans les noms des fichiers y compris caractères spéciaux :

- ***** : remplace zéro ou plus de caractère de n'importe quel type.
- **?** : remplace n'importe quel caractère.

Il faut prendre en considération que le nom est toujours séparé de l'extension du fichier par un point.

MISE EN QUARANTAINE D'OBJETS

Mode de traitement d'un objet potentiellement infecté dans le cadre duquel l'accès à l'objet est bloqué et l'objet est déplacé de son dossier d'origine vers le dossier de quarantaine où il est conservé sous forme codée, ce qui évite le risque d'infection.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

MODULE EXTERNE DE L'AGENT D'ADMINISTRATION

Fonction de l'application qui garantit la communication avec l'agent d'administration. L'agent d'administration permet d'administrer l'application à distance via Kaspersky Security Center.

MODULES DU LOGICIEL

Fichiers qui font partie de la distribution d'une application de Kaspersky Lab et qui sont responsables de la réalisation des tâches principales. Chaque type de tâche exécutée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) a son propre module exécutable. En lançant l'analyse complète de votre ordinateur depuis la fenêtre principale, vous lancez le module de cette tâche.

O

OBJET OLE

Fichier attaché ou intégré à un autre fichier. Les applications de Kaspersky Lab permettent de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel® dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJETS DE DEMARRAGE

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur l'ordinateur. Le système d'exploitation lance ces objets à chaque démarrage. Il existe des virus capables d'infecter ces objets, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

P

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche et responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performances de l'application, les paramètres de création de rapports ou les paramètres de la sauvegarde.

PARAMETRES DE TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

PHISHING

Type d'escroquerie sur Internet qui consiste à envoyer aux victimes potentielles des messages électroniques, prétendument envoyés en général par une banque, dans le but d'obtenir des informations confidentielles.

Q

QUARANTAINE

Dossier déterminé qui accueille les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

R

REPARATION D'OBJETS

Mode de traitement des objets infectés qui entraîne la restauration totale ou partielle des données ou qui débouche sur la constatation de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements contenus dans les bases. Il se peut qu'une partie des données soient perdues pendant la réparation.

S

SAUVEGARDE

Stockage spécial prévu pour l'enregistrement des copies de sauvegarde des objets créés avant leur première réparation ou suppression.

SERVEUR D'ADMINISTRATION

Module de Kaspersky Security Center qui permet de réaliser l'enregistrement centralisé des informations relatives aux applications de Kaspersky Lab installées sur le réseau et de les administrer.

T

TACHE

Fonction de l'application de Kaspersky Lab exécutée sur la forme de tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

KASPERSKY LAB

Kaspersky Lab est un éditeur mondialement reconnu de solutions de protection des ordinateurs contre les menaces telles que les virus et autres programmes malveillants, le courrier indésirable et les attaques de réseau et de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon l'étude COMCON TGI-Russia 2009, Kaspersky Lab est l'éditeur de solution de sécurité préféré des particuliers en Russie.

Kaspersky Lab a été fondée en Russie en 1997. A l'heure actuelle, Kaspersky Lab est devenue un groupe international qui compte un bureau central à Moscou et cinq bureaux régionaux chargés du développement des activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen-Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts.

Produits. Les logiciels développés par Kaspersky Lab protègent aussi bien les ordinateurs du grand public que les ordinateurs dans les réseaux des entreprises.

La gamme de solutions grand public reprend des applications pour la protection des ordinateurs de bureau et portables, pour les ordinateurs de poche, les téléphones intelligents et autres périphériques nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions et des outils centralisés d'administration permet de configurer et d'exploiter une protection automatisée de l'entreprise contre les menaces informatiques. Les logiciels de Kaspersky Lab sont certifiés par de grands laboratoires de test. Ils sont compatibles avec les produits de nombreux éditeurs et sont optimisés pour le fonctionnement sur de nombreuses plateformes matérielles.

Les experts de la lutte contre les virus chez Kaspersky Lab travaillent 24h/24. Ils découvrent chaque jour des centaines de nouvelles menaces informatiques, créent les outils pour les détecter et supprimer leurs effets et ajoutent ceux-ci aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont mises à jour tous les heures*, *les bases de l'Anti-Spam, quant à elles, sont actualisées toutes les 5 minutes*.

Technologies. Kaspersky Lab a été à l'origine de nombreuses technologies sans lesquelles il est difficile de se représenter un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Lab est utilisé dans les logiciels de nombreux autres éditeurs tels que SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israël), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Irlande), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taïwan). De nombreuses technologies de la société sont brevetées.

Réalisations. Au fil des années de lutte contre les menaces informatiques, Kaspersky Lab a décroché de nombreuses récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu quelques-uns des résultats les plus élevés dans les tests Advanced+ réalisé par le laboratoire antivirus autrichien renommé. AV-Comparatives. Mais la plus grande récompense pour Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les logiciels et les technologies développées par la société protègent plus de 300 millions d'utilisateurs. La société compte plus de 200 000 entreprises parmi ses clients.

Site de Kaspersky Lab :	http://www.kaspersky.com/fr/
Encyclopédie des virus :	http://www.viruslist.com/fr/
Laboratoire antivirus :	newvirus@kaspersky.com
	(uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

NOTICE SUR LES MARQUES

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Microsoft, Windows, Active Directory, Internet Explorer, Excel, Outlook, Outlook Express, Windows Vista, Windows Server sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Intel, Pentium sont des marques d'Intel Corporation déposées aux Etats-Unis et dans d'autres pays.

Adobe et Acrobat sont des marques ou des marques déposées d'Adobe Systems Incorporated enregistrées aux Etats-Unis et/ou dans d'autres pays.

Radmin et Remote Administrator sont des marques déposées de Famatech.

Mozilla et Thunderbird sont des marques de Mozilla Foundation.

ICQ est une marque ou une marque de service de ICQ LLC.

Mail.ru est une marquée déposée qui appartient à la société "Mail.Ru".

INDEX

A

B

C

D

E

F

I

K

L

M

N

P

Q

R

S

T

V

Z