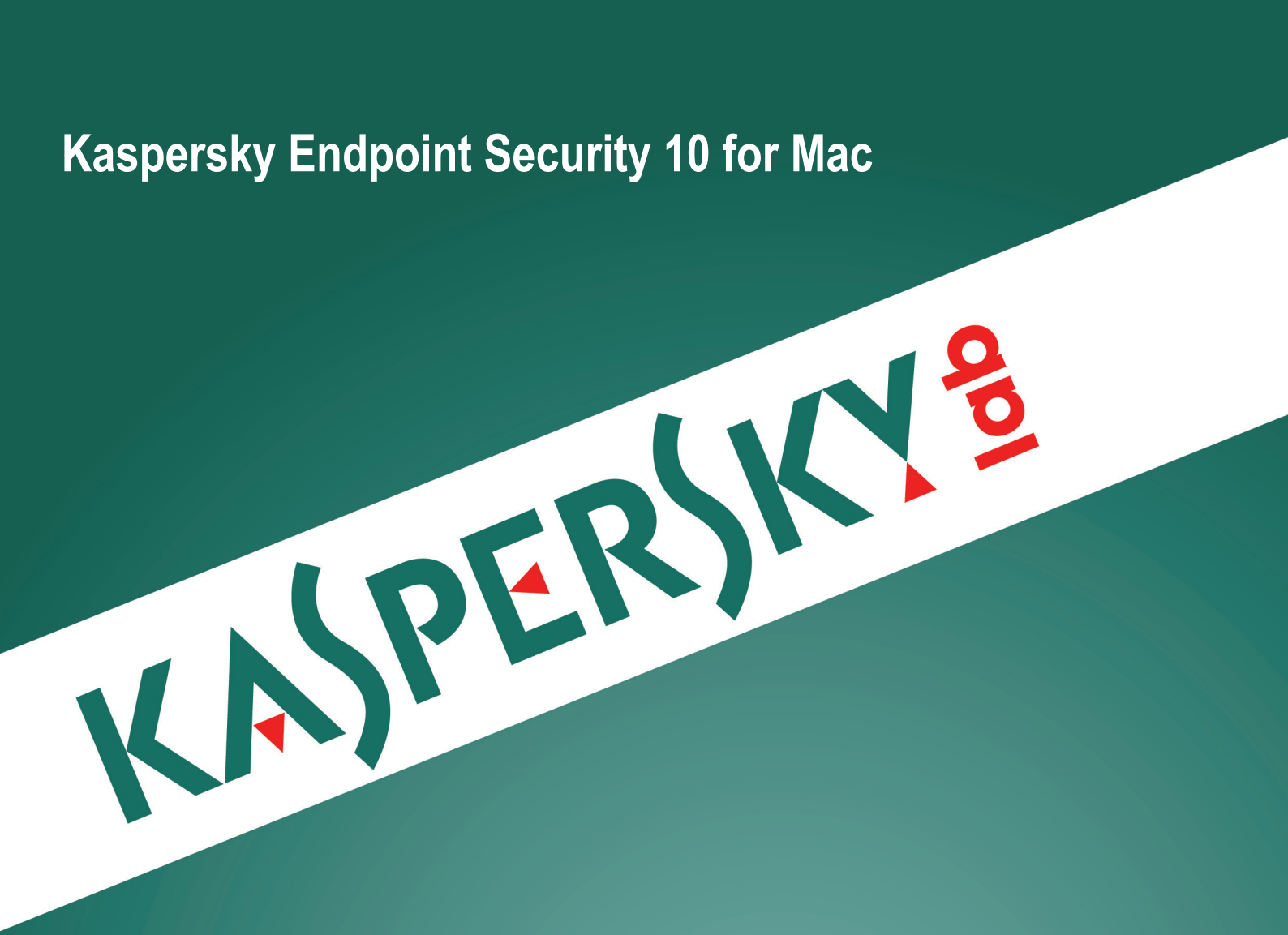
Kaspersky Endpoint Security 10 for Mac



Manuel de l'administrateur

VERSION DE L'APPLICATION : 10.0

Cher utilisateur,

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

Ce document peut être modifié sans préavis. La version la plus récente du manuel est disponible sur le site de Kaspersky Lab, à l'adresse suivante : http://www.kaspersky.com/fr/docs.

Date d'édition : 15/07/2015

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

TABLE DES MATIERES

PRESENTATION DE CE DOCUMENT 8
Dans ce document 8
Conventions 10
SOURCES D'INFORMATIONS SUR L'APPLICATION 11
Sources d'informations pour une recherche indépendante 11
Discussion des applications de Kaspersky Lab sur le forum 12
KASPERSKY ENDPOINT SECURITY 13
Présentation de Kaspersky Endpoint Security 13
Distribution 14
Configuration matérielle et logicielle 15
INSTALLATION ET SUPPRESSION DE L'APPLICATION 16
Préparatifs pour l'installation de l'application 16
Modes d'installation de l'application 16
Installation standard de Kaspersky Endpoint Security 17
Installation personnalisée de Kaspersky Endpoint Security 18
Préparation de l'application au travail 19
Suppression de l'application 20
INTERFACE DE L'APPLICATION 21
Icône de Kaspersky Endpoint Security 21
Dissimulation de l'icône de l'application dans la barre de menus 22
Fenêtre principale de l'application 22
Fenêtre de configuration de l'application 23
Fenêtres de notification et fenêtres contextuelles 24
Présentation des fenêtres de notification 24
Présentation des types d'événement 24
Présentation des fenêtres contextuelles 25
Désactivation des notifications 25
LICENCE DE L'APPLICATION 26
Présentation du Contrat de licence 26
Présentation de la licence 26
Présentation du certificat de licence 27
Présentation de la clé 27
Présentation du code d'activation 28
Consultation des informations sur la licence 28
Achat d'une licence 29
Renouvellement de la licence 29
Activation de Kaspersky Endpoint Security 29
Activation de la version d'évaluation de l'application 30
Activation de l'application à l'aide du code d'activation 30
LANCEMENT ET ARRET DE L'APPLICATION 32
ETAT DE LA PROTECTION DE L'ORDINATEUR 33
Evaluation de l'état de la protection de l'ordinateur 33
Désactivation de la protection de l'ordinateur 34

Rétablissement de la protection de l'ordinateur ... 35
Utilisation du Centre de Protection ... 35
RESOLUTION DES PROBLEMES TYPES ... 37
Procédure d'exécution d'une analyse complète de l'ordinateur ... 37
Réalisation d'une analyse rapide de l'ordinateur ... 38
Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque ... 38
Comment planifier le lancement automatique de l'analyse contre les virus ... 39
Procédure de mise à jour des bases de l'application ... 39
Que faire si l'application a bloqué l'accès au fichier ... 40
Que faire si l'application a placé le fichier en quarantaine ? ... 40
Que faire si vous soupçonnez l'infection d'un fichier par un virus ... 41
Procédure de restauration d'un fichier supprimé ou réparé par l'application ... 42
Emplacement du rapport sur le fonctionnement de l'application ... 42
Que faire en cas d'affichage de fenêtres de notification et de messages contextuels ... 43
CONFIGURATION ETENDUE DE L'APPLICATION ... 44
Zone de protection de l'ordinateur ... 44
Sélection des catégories d'objets détectés ... 44
Constitution de la zone de confiance ... 45
Anti-Virus Fichiers ... 46
Désactivation de l'Anti-Virus Fichiers ... 47
Activation de l'Anti-Virus Fichiers ... 48
Constitution de la zone de protection ... 48
Sélection des actions de l'Anti-Virus Fichiers sur les objets ... 49
Consultation du rapport de fonctionnement de l'Anti-Virus Fichiers ... 49
Anti-Virus Internet ... 50
Désactivation de l'Anti-Virus Internet ... 51
Activation de l'Anti-Virus Internet ... 51
Sélection de l'action à réaliser sur les objets dangereux du trafic Internet ... 52
Analyse des liens sur les pages Internet pour déterminer s'il s'agit de liens de phishing ... 52
Consultation du rapport de fonctionnement de l'Anti-Virus Internet ... 52
Prévention des intrusions ... 53
Désactivation de la prévention des intrusions ... 54
Activation de la prévention des intrusions ... 54
Composition de la liste des ordinateurs de confiance ... 55
Affichage et modification de la liste des ordinateurs bloqués ... 55
Consultation du rapport relatif à la prévention des intrusions ... 56
Analyse ... 57
Lancement et arrêt des tâches d'analyse ... 58
Constitution de la zone d'analyse ... 59
Configuration des paramètres des tâches d'analyse contre les virus ... 60
Sélection du niveau de sécurité ... 60
Sélection des actions à réaliser sur les objets lors de l'analyse ... 61
Configuration de la planification du lancement de la tâche d'analyse contre les virus ... 62
Restauration des paramètres d'analyse par défaut ... 62
Consultation du rapport sur l'exécution des tâches d'analyse ... 63
Mise à jour de l'application ... 63
Lancement de la mise à jour des bases de l'application ... 64
Annulation de la dernière mise à jour ... 65

Mise à jour depuis une source locale 65
Configuration des paramètres de la mise à jour 66
Sélection du mode de lancement de la mise à jour de Kaspersky Endpoint Security 67
Configuration des paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security 68
Désactivation du téléchargement automatique et de l'installation des mises à jour des modules de l'application sur l'ordinateur 68
Sélection de la source des mises à jour 68
Configuration des paramètres de connexion au serveur proxy 70
Consultation du rapport sur l'exécution de la mise à jour 70
Rapports et stockages 71
Quarantaine 71
Affichage de la quarantaine 72
Actions sur les fichiers potentiellement infectés 72
Activation de l'analyse automatique du contenu de la quarantaine après la mise à jour des bases antivirus 72
Sauvegarde 73
Consultation du contenu de la Sauvegarde 73
Actions sur les copies de sauvegarde des fichiers 73
Consultation des rapports 74
Exportation des rapports 75
Activation de la consignation des événements à caractère informatif 75
Configuration de la durée de conservation des fichiers en quarantaine et dans la sauvegarde 76
Participation au Kaspersky Security Network 76
UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE 78
Consultation de l'aide 79
Recherche de virus 79
Mise à jour de l'application 81
Annulation de la dernière mise à jour 82
Lancement/arrêt d'un composant ou d'une tâche 82
Etat et statistiques du fonctionnement du composant ou de la tâche 83
Exportation des paramètres de protection 83
Importation des paramètres de protection 84
Activation de l'application 84
Arrêt de l'application 84
Codes de retour de la ligne de commande 84
ADMINISTRATION A DISTANCE VIA KASPERSKY SECURITY CENTER 86
Schéma de déploiement type de Kaspersky Endpoint Security 86
Installation du plug-in d'administration de Kaspersky Endpoint Security 87
Préparatifs pour l'installation de Kaspersky Endpoint Security 87
Installation locale de l'Agent d'administration 88
Installation de l'Agent d'administration à l'aide du protocole SSH 89
Gestion de l'Agent d'administration via la ligne de commande 90
Lancer/arrêt de l'Agent d'administration sur l'ordinateur distant 90
Connexion manuelle de l'ordinateur distant au Serveur d'administration. Utilitaire klmover 91
Vérification manuelle de la connexion de l'ordinateur distant au Serveur d'administration Utilitaire klnagchk 92
Installation et suppression de Kaspersky Endpoint Security 92
Installation de l'application à l'aide du protocole SSH 93

Installation de l'application via Kaspersky Security Center 94
Etape 1. Définition du nom de la tâche 95
Etape 2. Sélection du type de tâche 95
Etape 3. Création du paquet d'installation 95
Etape 4. Installation d'applications complémentaires 96
Etape 5. Configuration des paramètres d'installation 96
Etape 6. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 97
Etape 7. Sélection des postes client 97
Etape 8. Planification du lancement de la tâche 97
Etape 9. Fin de la création de la tâche 97
Suppression de l'application via Kaspersky Security Center 97
Etape 1. Définition du nom de la tâche 98
Etape 2. Sélection du type de tâche. Suppression à distance de l'application 99
Etape 3. Sélection de l'application à supprimer 99
Etape 4. Sélection des paramètres de suppression 99
Etape 5. Sélection de l'option de redémarrage du système d'exploitation 99
Etape 6. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 99
Etape 7. Sélection des postes client 99
Etape 8. Sélection du compte utilisateur pour le lancement de la tâche 100
Etape 9. Planification du lancement de la tâche 100
Etape 10. Fin de la création de la tâche 100
Lancement et arrêt de l'application 100
Administration des stratégies 101
Création d'une stratégie 102
Etape 1. Saisie des données générales sur la stratégie 103
Etape 2. Sélection de l'application 103
Etape 3. Configuration de la protection 103
Etape 4. Configuration des paramètres de l'Anti-Virus Fichiers 103
Etape 5. Configuration des paramètres de l'Anti-Virus Internet 104
Etape 6. Configuration de la protection contre les attaques réseau 104
Etape 7. Configuration de la mise à jour 104
Etape 8. Configuration des paramètres d'utilisation de KSN 104
Etape 9. Configuration de l'interaction avec l'utilisateur 105
Etape 10. Configuration de l'interaction avec le réseau 105
Etape 11. Configuration des paramètres des rapports, de la quarantaine et de la sauvegarde 105
Etape 12. Sélection de l'état de la stratégie 105
Etape 13. Fin de la création de la stratégie 105
Configuration des paramètres d'une stratégie 106
Modification de l'état d'une stratégie 108
Importation d'une stratégie depuis un fichier 109
Ouverture de la liste des stratégies 109
Exportation d'une stratégie dans un fichier 109
Administration des tâches 110
Création d'une tâche 111
Création d'une tâche locale pour un poste client distinct 112
Création d'une tâche pour des postes client du groupe d'administration 113
Création d'une tâche pour des postes client en dehors du groupe d'administration 113
Etape 1. Saisie des données générales sur la tâche 114
Etape 2. Sélection de l'application et du type de tâche 114

Etape 3. Configuration des paramètres du type de tâche sélectionné 114
Etape 4. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 116
Etape 5. Sélection des postes client 116
Etape 6. Paramètres de planification 116
Etape 7. Fin de la création de la tâche 117
Lancement et arrêt manuels des tâches 117
Consultation des paramètres d'une tâche 117
Consultation de la liste des tâches pour les ordinateurs qui appartiennent au groupe d'administration 118
Consultation de la liste des tâches pour les ordinateurs en dehors du groupe d'administration 118
Consultation de la liste des tâches locales 119
Consultation et modification des paramètres de la tâche d'Analyse rapide 119
Consultation et modification des paramètres de la tâche d'Analyse complète 120
Consultation et modification des paramètres de la tâche de l'Anti-Virus Internet 121
Consultation et modification des paramètres de la tâche d'ajout d'une clé 122
Consultation et modification des paramètres de la tâche de protection contre les attaques réseau 123
Consultation et modification des paramètres de la tâche de mise à jour 124
Consultation et modification des paramètres de la tâche d'analyse définie par l'utilisateur 125
Consultation et modification des paramètres de la tâche de l'Anti-Virus Fichiers 126

COMPOSITION DU RAPPORT SUR LES OBJETS QUE L'APPLICATION A DETECTE SUR LE POSTE CLIENT 128

CONTACTER LE SUPPORT TECHNIQUE 129
Présentation du Support Technique 129
Support technique par téléphone 129
Support technique via Kaspersky CompanyAccount 130
Utilisation du fichier de trace 130
Création d'un fichier de traçage 130
Collecte d'informations pour le Support Technique 131

ANNEXES 132
Liste des objets analysés en fonction de l'extension 132
Masques dans les chemins d'accès aux fichiers et aux dossiers 137

GLOSSAIRE 138

AO KASPERSKY LAB 142

INFORMATIONS SUR LE CODE TIERS 143

NOTIFICATIONS SUR LES MARQUES DE COMMERCE 144

INDEX 145

PRESENTATION DE CE DOCUMENT

Le manuel de l'administrateur de Kaspersky Endpoint Security 10 for Mac (ci-après Kaspersky Security) est destiné aux experts chargés de l'installation et de l'administration de Kaspersky Endpoint Security et aux spécialistes du support technique au sein des organisations qui utilisent Kaspersky Endpoint Security.

Vous pouvez utiliser les informations de ce manuel pour exécuter les tâches suivantes :

- préparatifs de l'installation, installation et activation de Kaspersky Endpoint Security ;
- configuration et utilisation de Kaspersky Endpoint Security.

Il renseigne également les sources d'informations sur l'application et explique la marche à suivre pour bénéficier du Support Technique.

DANS CETTE SECTION

Dans ce document.....8

Conventions 10

DANS CE DOCUMENT

Les sections suivantes sont incluses dans le Manuel de l'administrateur de Kaspersky Endpoint Security :

Sources d'informations sur l'application (à la page 11)

Cette section décrit les sources d'informations relatives à l'application.

Kaspersky Endpoint Security (à la page 13)

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Endpoint Security. Elle reprend la configuration matérielle et logicielle requise pour l'application, ainsi que les informations relatives au service pour les utilisateurs.

Installation et suppression de l'application (à la page 16)

Cette section explique, étape par étape, comment installer et désinstaller Kaspersky Endpoint Security.

Interface de l'application (à la page 21)

Cette section décrit les principaux éléments de l'interface utilisateur graphique de Kaspersky Endpoint Security : icône de l'application et son menu contextuel, fenêtre principale et fenêtre des paramètres de l'application. Cette section contient également des informations sur les fenêtres de notification et les messages contextuels.

Licence de l'application (à la page 26)

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

Lancement et arrêt de l'application (à la page 32)

Cette rubrique explique comment lancer et arrêter l'application.

Cher utilisateur,

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

Ce document peut être modifié sans préavis. La version la plus récente du manuel est disponible sur le site de Kaspersky Lab, à l'adresse suivante : http://www.kaspersky.com/fr/docs.

Date d'édition : 15/07/2015

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

CONVENTIONS

Le présent document respecte des conventions (cf. tableau ci-dessous).

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Ils contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
Mise à jour – est... L'événement *Bases dépassées* survient.	Les éléments de texte suivants apparaissent en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Command-A.	Les noms des touches du clavier sont en caractères mi-gras. Deux noms de touche unis par le caractère "-" (moins) représentent une combinaison de 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".
kav update	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 à l'aide du clavier.
<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 décrit les sources d'informations relatives à 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 une recherche indépendante 11

Discussion des applications de Kaspersky Lab sur le forum 12

SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDEPENDANTE

Vous pouvez vous servir des sources suivantes pour rechercher vous-même les informations sur Kaspersky Endpoint Security :

- page de Kaspersky Endpoint Security sur le site Internet de Kaspersky Lab ;
- page de Kaspersky Endpoint Security sur le site Internet du Support Technique (base de solutions) ;
- aide électronique ;
- la documentation.

Si vous n'avez pas trouvé la solution à votre problème, contactez le Support Technique de Kaspersky Lab.

La consultation des sources d'informations en ligne requiert une connexion à Internet.

Page de Kaspersky Endpoint Security sur le site de Kaspersky Lab

La page de Kaspersky Endpoint Security (http://www.kaspersky.com/fr/business-security/endpoint-mac) fournit des informations générales sur l'application, ses possibilités et particularités de fonctionnement.

La page de Kaspersky Endpoint Security propose un lien vers la boutique en ligne. Vous pouvez y acheter l'application ou renouveler la licence.

Page de Kaspersky Endpoint Security dans la base de connaissance

La *Base de connaissances* est une section du site du Support technique.

La page de Kaspersky Endpoint Security dans la base de connaissances (http://support.kaspersky.com/kes10mac) propose des articles reprenant des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles de la base de connaissances peuvent répondre à des questions concernant non seulement Kaspersky Endpoint Security, mais également d'autres applications de Kaspersky Lab. Ils peuvent également contenir des nouvelles du Support Technique.

Pour accéder à la banque de solutions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton  .
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Base de connaissances**.

Aide électronique

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

L'aide contextuelle vous renseigne sur les fenêtres de Kaspersky Endpoint Security : description des paramètres de Kaspersky Endpoint Security et liens vers les descriptions des tâches qui utilisent ces paramètres.

L'aide complète reprend des informations sur la configuration et l'utilisation de Kaspersky Endpoint Security.

Documentation

Le manuel de l'administrateur propose des informations qui permettent de réaliser les tâches suivantes :

- préparatifs de l'installation, installation et activation de Kaspersky Endpoint Security ;
- configuration et utilisation de Kaspersky Endpoint Security ;
- administration à distance de Kaspersky Endpoint Security via Kaspersky Security Center.

DISCUSSION DES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs sur notre forum (http://forum.kaspersky.com/index.php?showforum=129).

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

Pour accéder au forum, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton  .
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Forum**.

KASPERSKY ENDPOINT SECURITY

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Endpoint Security. Elle reprend la configuration matérielle et logicielle requise pour l'application, ainsi que les informations relatives au service pour les utilisateurs.

DANS CETTE SECTION

Présentation de Kaspersky Endpoint Security 13

Distribution 14

Configuration matérielle et logicielle 15

PRESENTATION DE KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security a été développé pour assurer la protection des ordinateurs régis par le système d'exploitation OS X contre l'action des virus et autres programmes menaçant la sécurité de l'ordinateur.

Les composants suivants font partie du programme :

Anti-Virus Fichiers

Le module Anti-Virus Fichiers protège en temps réel le système de fichiers de l'ordinateur : il assure l'interception et l'analyse des requêtes adressées aux fichiers. Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés.

Anti-Virus Internet

Le module Anti-Virus Internet protège les informations entrantes et sortantes de l'ordinateur via les navigateurs Safari, Google Chrome™ et Firefox™, et les protocoles HTTP et HTTPS.

Prévention des intrusions

Le module Protection contre les attaques réseau protège le système d'exploitation de l'ordinateur contre les intrusions. Ce module assure la protection contre les actions malveillantes exécutées par les malfaiteurs (par exemple, le balayage des ports et l'appairage des mots de passe). Il assure également la protection contre les actions entreprises par les programmes malveillants installés par les malfaiteurs sur l'ordinateur attaqué (par exemple, la communication de données protégées au malfaiteur).

L'application offre les fonctions suivantes :

Analyse

Kaspersky Endpoint Security recherche et neutralise les virus et autres programmes menaçant la sécurité de l'ordinateur, à votre demande dans la zone d'analyse définie. Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés. Kaspersky Endpoint Security exécute l'analyse complète de l'ordinateur, l'analyse rapide des zones importantes et l'analyse de la zone définie.

Mise à jour

Kaspersky Endpoint Security met à jour les bases et les modules de l'application depuis les serveurs de mises à jour de Kaspersky Lab ou depuis Kaspersky Security Center t et crée une sauvegarde de tous les fichiers actualisés au cas où il serait nécessaire de revenir à l'état antérieur à la dernière mise à jour. Kaspersky Endpoint Security permet de copier les mises à jour récupérées dans une source locale qui sera accessible aux autres ordinateurs du réseau de l'entreprise, dans le but de réduire le volume du trafic Internet.

Quarantaine

Kaspersky Endpoint Security place les fichiers potentiellement infectés en quarantaine. Vous pouvez les analyser à l'aides des bases anti-virus actualisées et les restaurer depuis la quarantaine.

Sauvegarde

Kaspersky Endpoint Security crée une copie du fichier infecté dans la Sauvegarde avant de le réparer ou de le supprimer. Vous pourrez ainsi restaurer ce fichier.

Rapports

Kaspersky Endpoint Security génère un rapport sur le fonctionnement de l'application.

Notifications

Kaspersky Endpoint Security signale les événements qui surviennent au cours de son fonctionnement à l'aide de fenêtres de notification ou de messages contextuels. La fenêtre de notification peut être accompagnée de notifications sonores.

Centre de protection

Lors de son fonctionnement, Kaspersky Endpoint Security affiche des messages sur l'état de la protection dans le Centre de protection. Le Centre de protection permet d'obtenir des informations sur l'état actuel de la protection de l'ordinateur et d'éliminer les problèmes et les menaces concernant la sécurité de ce dernier.

Administration à distance de l'application via Kaspersky Security Center

Kaspersky Security Center permet d'administrer à distance la protection de l'ordinateur doté de Kaspersky Endpoint Security. Il est ainsi possible de : recevoir des informations sur l'état actuel de la protection de l'ordinateur et de corriger à distance les problèmes et les menaces à l'encontre de la sécurité de l'ordinateur, activer et désactiver la protection des modules (Anti-virus Fichiers, Anti-virus Internet, prévention des intrusions), lancer l'analyse antivirus, mettre à jour les bases de l'application et administrer les licences de Kaspersky Endpoint Security.

DISTRIBUTION

La distribution de Kaspersky Endpoint Security contient les fichiers suivants :

- Les fichiers indispensables à l'installation de l'application à l'aide de toutes les méthodes disponibles.
- Le fichier ksn.rtf qui présente les conditions de participation à Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 76).
- Le fichier license.rtf qui contient le texte du Contrat de licence (cf. section "Présentation du contrat de licence" à la page 26). Le Contrat de licence reprend les conditions d'utilisation de l'application.

Pour pouvoir accéder aux fichiers de la distribution diffusée au format ZIP, il faut la décompacter.

CONFIGURATION MATERIELLE ET LOGICIELLE

Pour pouvoir utiliser Kaspersky Endpoint Security, la machine virtuelle ou physique doit répondre aux configurations logicielle et matérielle suivantes :

- système d'exploitation OS X 10.7, OS X 10.8, 10.9, 10.10 ;
- 550 Mo d'espace disponible sur le disque dur (selon la taille des bases antivirus).

Kaspersky Endpoint Security prend en charge les outils de virtualisation suivants :

- Parallels Desktop 9 for Mac Standard Edition ;
- Parallels Desktop 9 for Mac Enterprise Edition ;
- Parallels Desktop 10 for Mac Standard Edition ;
- Parallels Desktop 10 for Mac Enterprise Edition ;
- VMware Fusion™ 6 ;
- VMware Fusion 6 Professional ;
- VMware Fusion 7 ;
- VMware Fusion 7 Professional.

Il est possible d'administrer Kaspersky Endpoint Security via Kaspersky Security Center. Le plug-in d'administration de Kaspersky Endpoint Security via Kaspersky Security Center doit répondre à la configuration logicielle suivante :

- Kaspersky Security Center 10 ;
- Kaspersky Security Center 10 Service Pack 1.

INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section explique, étape par étape, comment installer et désinstaller Kaspersky Endpoint Security.

Le paquet d'installation de Kaspersky Endpoint Security contient le programme d'installation et le programme de suppression de Kaspersky Endpoint Security.

DANS CETTE SECTION

Préparatifs pour l'installation de l'application 16

Modes d'installation de l'application 16

Préparation de l'application au travail 19

Suppression de l'application 20

PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Avant d'installer Kaspersky Endpoint Security sur l'ordinateur, il est recommandé d'exécuter les actions suivantes :

- Assurez-vous que votre ordinateur correspond aux exigences système (cf. section "Configuration matérielle et logicielle" à la page 15).
- Supprimer les autres applications antivirus de l'ordinateur pour éviter l'apparition des conflits de système et le ralentissement de la rapidité du système d'exploitation.

MODES D'INSTALLATION DE L'APPLICATION

Les experts de Kaspersky Lab conseillent d'installer Kaspersky Endpoint Security uniquement selon les méthodes décrites dans ce manuel.

Vous pouvez installer l'application d'une des manières suivantes :

- Localement depuis la distribution de Kaspersky Endpoint Security (cf. section "Installation standard de Kaspersky Endpoint Security" à la page 17).
- A distance, via Kaspersky Security Center (cf. section "Installation de l'application via Kaspersky Security Center" à la page 94).

DANS CETTE SECTION

Installation standard de Kaspersky Endpoint Security 17

Installation personnalisée de Kaspersky Endpoint Security 18

INSTALLATION STANDARD DE KASPERSKY ENDPOINT SECURITY

Les fenêtres **Contrat de licence** et **Participation au Kaspersky Security Network** du programme d'installation apparaissent uniquement lors de l'installation de Kaspersky Endpoint Security en allemand et en russe. Dans les autres cas, pour lire les textes du contrat de licence et les informations relatives à la participation au Kaspersky Security Network, il suffit de cliquer sur les liens correspondants dans la fenêtre du programme d'installation de Kaspersky Endpoint Security.

Pour réaliser l'installation standard de Kaspersky Endpoint Security, procédez comme suit :

1. Lancez le programme d'installation de Kaspersky Endpoint Security d'une des manières suivantes :
   - Exécutez le fichier au format ISO.
   - Décompactez l'archive ZIP et exécutez le fichier au format DMG.
2. Lancez l'installation de l'application d'un double clic de la souris sur l'icône **Kaspersky Endpoint Security**.

   La fenêtre de confirmation du lancement du programme d'installation s'ouvre.
3. Cliquez sur le bouton **Continuer** pour confirmer le lancement de l'installation de l'application.

   La fenêtre **Introduction** qui offre des informations sur Kaspersky Endpoint Security s'ouvre.
4. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.
5. Dans la fenêtre **Licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Endpoint Security, qui a été conclu entre vous et AO Kaspersky Lab.
6. Après avoir lu le texte du Contrat de licence, cliquez sur **Continuer**.

   La fenêtre **Avant de pouvoir continuer l'installation de l'application, il faut accepter le Contrat de licence** s'ouvre.
7. Réalisez une des opérations suivantes dans la fenêtre **Avant de pouvoir continuer l'installation de l'application, il faut accepter le Contrat de licence** :
   - Si vous acceptez les termes du Contrat de licence, cliquez sur **J'accepte**.

     L'installation de Kaspersky Endpoint Security se poursuit.
   - Si vous n'acceptez pas les termes du Contrat de licence, cliquez sur **Je refuse**.

     L'installation de Kaspersky Endpoint Security se poursuit.
   - Si vous souhaitez revenir à la fenêtre contenant le texte du Contrat de licence, cliquez sur le bouton **Lire la licence**.
8. Lisez les informations relatives à la participation au Kaspersky Security Network dans la fenêtre **Participation au Kaspersky Security Network**.

   La participation au Kaspersky Security Network signifie que les statistiques obtenues pendant l'utilisation de Kaspersky Endpoint Security sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

   Aucune donnée personnelle n'est collectée, traitée et conservée.
9. Après avoir lu les informations relatives à la participation au Kaspersky Security Network, réalisez une des opérations suivantes :
   - Si vous souhaitez participer au Kaspersky Security Network, cochez la case **J'accepte les conditions de participation à KSN**.
   - Si vous ne souhaitez pas participer au Kaspersky Security Network, décochez la case **J'accepte les conditions de participation à KSN**.

Sachez qu'à tout moment de votre utilisation de Kaspersky Endpoint Security vous pouvez décider de rejoindre le Kaspersky Security Network ou vous en retirer.

10. Dans la fenêtre **Participation au Kaspersky Security Network** qui s'ouvre, cliquez sur **Continuer**.
11. Dans la fenêtre **Type d'installation** qui s'ouvre, cliquez sur le bouton **Arrêter**.
12. Dans la fenêtre de confirmation de l'installation de l'application qui s'ouvre, saisissez les données du compte administrateur de l'ordinateur, puis cliquez sur **Installer l'application**.

    L'installation de Kaspersky Endpoint Security sur l'ordinateur démarre.
13. Une fois l'installation terminée, cliquez sur **Fermer** pour quitter le programme d'installation.

Kaspersky Endpoint Security démarre automatiquement. Le redémarrage de l'ordinateur n'est pas requis.

INSTALLATION PERSONNALISEE DE KASPERSKY ENDPOINT SECURITY

Les fenêtres **Contrat de licence** et **Participation au Kaspersky Security Network** du programme d'installation apparaissent uniquement lors de l'installation de Kaspersky Endpoint Security en allemand et en russe. Dans les autres cas, pour lire les textes du contrat de licence et les informations relatives à la participation au Kaspersky Security Network, il suffit de cliquer sur les liens correspondants dans la fenêtre du programme d'installation de Kaspersky Endpoint Security.

Pour réaliser la mise à jour personnalisée de Kaspersky Endpoint Security, procédez comme suit :

1. Lancez le programme d'installation de Kaspersky Endpoint Security d'une des manières suivantes :
   - Exécutez le fichier au format ISO.
   - Décompactez l'archive ZIP et exécutez le fichier au format DMG.
2. Lancez l'installation de l'application d'un double clic de la souris sur l'icône **Kaspersky Endpoint Security**.

   La fenêtre de confirmation du lancement du programme d'installation s'ouvre.
3. Cliquez sur le bouton **Continuer** pour confirmer le lancement de l'installation de l'application.

   La fenêtre **Introduction** qui offre des informations sur Kaspersky Endpoint Security s'ouvre.
4. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.
5. Dans la fenêtre **Licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Endpoint Security, qui a été conclu entre vous et AO Kaspersky Lab.
6. Après avoir lu le texte du Contrat de licence, cliquez sur **Continuer**.

   La fenêtre **Avant de pouvoir continuer l'installation de l'application, il faut accepter le Contrat de licence** s'ouvre.
7. Réalisez une des opérations suivantes dans la fenêtre **Avant de pouvoir continuer l'installation de l'application, il faut accepter le Contrat de licence** :
   - Si vous acceptez les termes du Contrat de licence, cliquez sur **J'accepte**.

     L'installation de Kaspersky Endpoint Security se poursuit.

- Si vous n'acceptez pas les termes du Contrat de licence, cliquez sur **Je refuse**.

  L'installation de Kaspersky Endpoint Security se poursuit.

- Si vous souhaitez revenir à la fenêtre contenant le texte du Contrat de licence, cliquez sur le bouton **Lire la licence**.

8. Lisez les informations relatives à la participation au Kaspersky Security Network dans la fenêtre **Participation au Kaspersky Security Network**.

   La participation au Kaspersky Security Network signifie que les statistiques obtenues pendant l'utilisation de Kaspersky Endpoint Security sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

   Aucune donnée personnelle n'est collectée, traitée et conservée.

9. Après avoir lu les informations relatives à la participation au Kaspersky Security Network, réalisez une des opérations suivantes :

   - Si vous souhaitez participer au Kaspersky Security Network, cochez la case **J'accepte les conditions de participation à KSN**.

   - Si vous ne souhaitez pas participer au Kaspersky Security Network, décochez la case **J'accepte les conditions de participation à KSN**.

   Sachez qu'à tout moment de votre utilisation de Kaspersky Endpoint Security vous pouvez décider de rejoindre le Kaspersky Security Network ou vous en retirer.

10. Dans la fenêtre **Participation au Kaspersky Security Network** qui s'ouvre, cliquez sur **Continuer**.

11. Dans la fenêtre **Type d'installation** qui s'ouvre, cliquez sur le bouton **Configurer**.

    La fenêtre qui permet de sélectionner les modules que vous souhaitez installer s'ouvre.

12. Décochez la case en regard du nom des composants que vous ne souhaitez pas installer.

    Si vous décidez de ne pas installer le composant **Interface utilisateur graphique**, vous ne pourrez pas activer Kaspersky Endpoint Security et utiliser l'application via l'interface graphique locale, ni configurer les paramètres de fonctionnement et d'utilisation de Kaspersky Security Network via cette même interface.

13. Cliquez sur le bouton **Installer**.

14. Dans la fenêtre de confirmation de l'installation de l'application qui s'ouvre, saisissez les données du compte administrateur de l'ordinateur, puis cliquez sur **Installer l'application**.

    L'installation de Kaspersky Endpoint Security sur l'ordinateur démarre.

15. Une fois l'installation terminée, cliquez sur **Fermer** pour quitter le programme d'installation.

Kaspersky Endpoint Security démarre automatiquement. Le redémarrage de l'ordinateur n'est pas requis.

PREPARATION DE L'APPLICATION AU TRAVAIL

Après l'installation de Kaspersky Endpoint Security, il est conseillé de procéder comme suit :

- Activer Kaspersky Endpoint Security (cf. section "Activation de Kaspersky Endpoint Security" à la page 29). L'activation de l'application vous permettra d'actualiser régulièrement les bases antivirus et les modules de l'application et assurera l'accès aux services du Support Technique.

- Evaluer l'état actuel de la protection de l'ordinateur (cf. section "Evaluation de l'état de la protection de l'ordinateur" à la page 33).

- Mettre à jour Kaspersky Endpoint Security (cf. section "Procédure de mise à jour des bases et des modules de l'application" à la page 39).

- Lancer une analyse complète de l'ordinateur sur les virus et sur les autres applications qui présentent une menace pour la sécurité de l'ordinateur (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page 37).

SUPPRESSION DE L'APPLICATION

Si vous supprimez Kaspersky Endpoint Security; la sécurité de votre ordinateur et de vos données risque d'être menacée.

Pour supprimer Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Endpoint Security.

   Si vous avez acheté Kaspersky Endpoint Security en ligne et que vous avez téléchargé la distribution au format DMG depuis le site de Kaspersky Lab, ouvrez le fichier dmg.

2. Dans la fenêtre contenant la distribution, double-cliquez sur **Supprimer Kaspersky Endpoint Security**.

   Le programme d'installation de Kaspersky Endpoint Security se lance. Suivez les étapes du programme de suppression pour supprimer Kaspersky Endpoint Security.

3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Supprimer**.

4. Confirmez la suppression de l'application dans la fenêtre de saisie des informations d'identification de l'administrateur de l'ordinateur.

   La suppression de Kaspersky Endpoint Security démarre.

5. Dans la fenêtre **Fin**, lisez les informations sur la fin du processus de suppression et cliquez sur le bouton **Terminer** pour quitter le programme de suppression.

Il n'est pas nécessaire de redémarrer l'ordinateur après la suppression de Kaspersky Endpoint Security.

INTERFACE DE L'APPLICATION

Cette section décrit les principaux éléments de l'interface utilisateur graphique de Kaspersky Endpoint Security : icône de l'application et son menu contextuel, fenêtre principale et fenêtre des paramètres de l'application. Cette section contient également des informations sur les fenêtres de notification et les messages contextuels.

DANS CETTE SECTION

Icône de Kaspersky Endpoint Security 21

Dissimulation de l'icône de l'application dans la barre de menus 22

Fenêtre principale de l'application 22

Fenêtre de configuration de l'application 23

Fenêtres de notification et fenêtres contextuelles 24

ICONE DE KASPERSKY ENDPOINT SECURITY

Juste après l'installation de Kaspersky Endpoint Security, son icône apparaît dans la barre de menus. L'icône de l'application indique l'état de fonctionnement de l'application. Quand l'icône de l'application est active  , la protection en temps réel contre les virus et autres programmes dangereux pour la sécurité de l'ordinateur est activée.

L'icône de l'application inactive  indique que la protection est désactivée.

L'icône de Kaspersky Endpoint Security se place par défaut dans la barre de menus. Vous pouvez désactiver l'affichage de l'icône de l'application dans la barre de menus (cf. section "Dissimulation de l'icône de l'application dans la barre de menus" à la page 22). Si l'une des fenêtres de Kaspersky Endpoint Security est ouverte, l'icône de l'application apparaît également dans le volet de lancement rapide du **Dock**.

Le menu contextuel de l'icône de l'application permet d'accéder aux commandes principales de Kaspersky Endpoint Security :

- accès à la fenêtre principale de l'application ;
- activation et désactivation de la protection en temps réel de l'ordinateur ;
- accès au Centre de protection ;
- lancement de l'analyse rapide de l'ordinateur pour trouver des virus out tout autre programme dangereux pour la sécurité de l'ordinateur ;
- lancement de la tâche de mise à jour des bases et des modules de l'application ;
- accès à la fenêtre de configuration de l'application.

Pour ouvrir le menu contextuel de l'icône de Kaspersky Endpoint Security,

cliquez sur l'icône de l'application dans la barre de menus.

DISSIMULATION DE L'ICONE DE L'APPLICATION DANS LA BARRE DE MENUS

Pour désactiver l'affichage de l'icône de l'application dans la barre de menus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Décochez la case **Afficher dans la barre de menus** du groupe **Icône de l'application** dans l'onglet **Apparence**.

FENETRE PRINCIPALE DE L'APPLICATION

Pour ouvrir la fenêtre principale de l'application, procédez comme suit :

1. Cliquez sur l'icône de Kaspersky Endpoint Security dans la barre de menus.

   Le menu contextuel de l'icône de l'application s'ouvre.
2. Sélectionnez l'option **Kaspersky Endpoint Security**.

Tâches de la fenêtre principale de l'application

La fenêtre principale de Kaspersky Endpoint Security vous permet de consulter les informations sur l'état de la protection de l'ordinateur, le fonctionnement de l'Anti-Virus Fichiers, l'Anti-Virus Internet et sur l'exécution des tâches d'analyse et de mise à jour.

De plus, la fenêtre principale de l'application permet d'accéder aux tâches suivantes :

- gestion de l'analyse contre les virus et des mises à jour ;
- gestion des clés de l'application ;
- Centre de protection ;
- configuration de l'application ;
- consultation des rapports sur le fonctionnement de l'application.

Eléments d'administration de la fenêtre principale de l'application

La fenêtre principale de l'application comprend les éléments suivants pour l'administration :

- indicateur de l'état de la protection sous la forme d'un ordinateur ;
- boutons dans la partie inférieure de la fenêtre principale de l'application ;
- panneau de navigation dans la partie supérieure de la fenêtre principale de l'application.

L'indicateur de l'état de la protection indique l'état de la protection de l'ordinateur en temps réel (cf. section "Evaluation de l'état de la protection de l'ordinateur" à la page 33) :

- vert signifie que la protection de l'ordinateur est garantie au niveau requis ;
- jaune ou rouge indiquent l'existence d'un problème dans la configuration des paramètres ou dans le fonctionnement de Kaspersky Endpoint Security.

Outre l'indicateur sur l'état de la protection de l'ordinateur, la partie droite de la fenêtre principale de l'application affiche des informations textuelles sur l'état de la protection. La partie droite de la fenêtre principale de l'application peut également afficher une liste des problèmes et des menaces sur la sécurité de l'ordinateur qu'il est possible d'éliminer à l'aide du Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35) Si une analyse ou une mise à jour est en cours d'exécution à ce moment donné, la progression de celle-ci (exprimée en pour cent) apparaît également dans la partie droite de la fenêtre principale de l'application.

Les boutons de la partie inférieure de la fenêtre principale de l'application permettent de réaliser les tâches suivantes :

Passer aux tâches d'analyse contre les virus : Analyse rapide, Analyse complète et Analyse personnalisée.

Ouvrir la fenêtre Mise à jour.

Ouvrir la fenêtre Licence (cf.section "Consultation des informations relatives à la licence" à la page 28).

La partie supérieure de la fenêtre principale de l'application contient une barre de navigation. Les boutons de la barre de navigation permettent de réaliser les opérations suivantes :

Ouvrir la fenêtre des rapports (cf. section "Consultation des rapports" à la page 74) de Kaspersky Endpoint Security.

Ouvrir la fenêtre de configuration de l'application (à la page 23).

Ouvre la fenêtre contenant les informations sur les moyens d'obtenir l'assistance technique (cf. section "Contacter le Support Technique" à la page 129).

Ouvrir l'aide électronique de Kaspersky Endpoint Security.

FENETRE DE CONFIGURATION DE L'APPLICATION

Pour ouvrir la fenêtre de configuration de Kaspersky Endpoint Security, exécutez l'une des actions suivantes :

- cliquez sur le bouton  dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) ;
- dans le menu contextuel de l'icône de Kaspersky Endpoint Security (cf. section "Icône de Kaspersky Endpoint Security" à la page 21), sélectionnez l'option **Paramètres**.

Vous pouvez utiliser les onglets suivants, situés dans la partie supérieure de la fenêtre des préférences de l'application, pour accéder rapidement aux paramètres de l'application :

- **Protection**. Cet onglet permet de configurer les paramètres de l'Anti-Virus Fichiers, de l'Anti-Virus Internet et de la prévention des intrusions.
- **Analyse**. Cet onglet permet de configurer les paramètres de l'analyse contre les virus et de lancer l'analyse programmée.
- **KSN**. Cet onglet permet de participer à Kaspersky Security Network ou de refuser la participation au Kaspersky Security Network et de configurer les paramètres d'utilisation de Kaspersky Security Network.
- **Menaces**. Cet onglet permet de sélectionner la catégorie d'objets détectés et de créer une zone de confiance.
- **Mise à jour**. Cet onglet permet de configurer les paramètres de la mise à jour de l'application ou de revenir à une version antérieure des bases anti-virus.

- **Rapports**. Cet onglet permet de configurer les paramètres des rapports de Kaspersky Endpoint Security, de la quarantaine et de la sauvegarde, d'activer ou de désactiver la consignation des informations de débogage dans le fichier de traçage.

- **Apparence**. Cet onglet permet de configurer les paramètres d'affichage des fenêtres de notification Kaspersky Endpoint Security et de l'icône de l'application.

Le bouton  permet d'empêcher la modification des paramètres de fonctionnement de Kaspersky Endpoint Security par un utilisateur qui ne disposerait pas des privilèges d'administrateur de l'ordinateur. Le bouton se trouve dans la partie inférieure de la fenêtre des paramètres de l'application. La modification des paramètres requiert la connexion en tant qu'administrateur de l'ordinateur.

Le bouton  ouvre l'aide de Kaspersky Endpoint Security qui décrit tous les paramètres de la fenêtre active de l'application. Vous pouvez également ouvrir l'aide pour la fenêtre actuelle de l'application, en sélectionnant l'option **Ouvrir l'aide pour cette fenêtre** dans le menu **Aide**.

FENETRES DE NOTIFICATION ET FENETRES CONTEXTUELLES

Des événements présentant différents degrés de gravité se produisent lors du fonctionnement de Kaspersky Endpoint Security.

L'application signale les événements via des *fenêtres de notification* et des *messages contextuels*. La fenêtre de notification peut être accompagnée de notifications sonores.

DANS CETTE SECTION

Présentation des fenêtres de notification 24

Présentation des types d'événement 24

Présentation des fenêtres contextuelles 25

Désactivation des notifications 25

PRESENTATION DES FENETRES DE NOTIFICATION

Kaspersky Endpoint Security affiche une fenêtre de notification si l'événement nécessite que vous sélectionniez une action. Par exemple, lorsque l'application détecte un objet malveillant, l'utilisateur choisit de le supprimer ou de le réparer. La fenêtre de notification disparaît une fois que vous avez sélectionné une des actions proposées.

PRESENTATION DES TYPES D'EVENEMENT

Les événements qui apparaissent au cours du fonctionnement de Kaspersky Endpoint Security se divisent en trois catégories, selon leur niveau de gravité :

- **Critiques** : événements présentant un danger sérieux pour l'ordinateur (objets malveillants ou vulnérabilités détectés, problèmes dans le fonctionnement de Kaspersky Endpoint Security). L'apparition d'événements critiques exige une action immédiate de la part de l'utilisateur. Il est conseillé de ne pas désactiver les notifications à propos des événements critiques.

- **Importants** : événements ne nécessitant pas une action immédiate de la part de l'utilisateur mais qui peuvent s'avérer dangereux à long terme pour l'ordinateur.

- **Informatives** : simples informations.

PRESENTATION DES FENETRES CONTEXTUELLES

Kaspersky Endpoint Security affiche des *fenêtres contextuelles* pour vous signaler les événements qui ne requièrent pas nécessairement la sélection d'une action. En fonction de la version du système d'exploitation de l'ordinateur, les messages contextuels apparaîtront sous l'icône de l'application dans la barre de menus ou dans le Centre de notification du système d'exploitation OS X (pour les versions OS X 10.8 et suivantes).

DESACTIVATION DES NOTIFICATIONS

Par défaut, Kaspersky Endpoint Security signale (cf. section "Fenêtres de notification et fenêtres contextuelles" à la page 24) uniquement les événements critiques. Vous pouvez désactiver l'affichage des notifications ou sélectionner les événements pour lesquels vous souhaitez recevoir des notifications, ainsi que désactiver la notification sonore.

Que la remise des notifications soit activée ou non, les informations relatives aux événements survenus pendant le fonctionnement de Kaspersky Endpoint Security sont consignées dans le rapport sur le fonctionnement de l'application (cf. section "Consultation des rapports" à la page 74)

- *Pour désactiver la remise des notifications, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application (à la page 22).
  2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

     La fenêtre des paramètres de l'application s'ouvre.
  3. Décochez la case **Activer les notifications** du groupe **Notifications** dans l'onglet **Apparence** pour ne pas afficher les fenêtres de notification.

- *Pour sélectionner le type d'événement pour lequel vous ne souhaitez pas recevoir de notification, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application (à la page 22).
  2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

     La fenêtre des paramètres de l'application s'ouvre.
  3. Dans l'onglet **Apparence**, groupe **Notifications**, décochez les cases en regard des types d'événement (cf. section "Présentation des types d'événements" à la page 24) au sujet desquels vous ne souhaitez pas recevoir de notification.

- *Pour désactiver la notification sonore quand une fenêtre de notification s'affiche, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application (à la page 22).
  2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

     La fenêtre des paramètres de l'application s'ouvre.
  3. Décochez la case **Activer les notifications sonores** du groupe **Notifications** dans l'onglet **Apparence** pour ne pas afficher les fenêtres de notification.

LICENCE DE L'APPLICATION

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

DANS CETTE SECTION

Présentation du Contrat de licence 26

Présentation de la licence 26

Présentation du certificat de licence 27

Présentation de la clé 27

Présentation du code d'activation 28

Consultation des informations sur la licence 28

Acquisition d'une licence 29

Renouvellement de la licence 29

Activation de Kaspersky Endpoint Security 29

PRESENTATION DU CONTRAT DE LICENCE

Le *contrat de licence* est l'accord légal conclu entre vous et AO Kaspersky Lab qui précise les conditions d'utilisation du logiciel.

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

Vous pouvez prendre connaissance des conditions du Contrat de licence d'une des méthodes suivantes :

- pendant l'installation de Kaspersky Endpoint Security ;
- en lisant le document license.txt. Ce document est repris dans la distribution de l'application.

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

PRESENTATION 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 donne droit aux services suivants :

- utilisation de l'application conformément aux dispositions du Contrat de licence ;
- Support Technique.

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

Il existe les types de licence suivants :

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

  La durée de validité de la licence d'évaluation est courte. Une fois que la licence d'évaluation de Kaspersky Endpoint Security arrive à échéance, toutes les fonctions de l'application sont désactivées. Pour continuer à utiliser l'application, il faut acheter une licence commerciale.

  Vous pouvez activer l'application à l'aide d'une licence d'évaluation une seule fois uniquement.

- *Commerciale* : licence payante délivrée lors de l'achat de l'application.

  A l'expiration de la durée de validité de la licence commerciale, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour des bases de Kaspersky Endpoint Security n'est pas disponible). Pour pouvoir profiter de toutes les fonctionnalités de Kaspersky Endpoint Security, il faut renouveler la licence commerciale.

Il est conseillé de renouveler la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre les menaces.

PRESENTATION DU CERTIFICAT DE LICENCE

Le *certificat de licence* est un document qui vous est remis avec le fichier clé ou le code d'activation.

Le certificat de licence contient les informations suivantes sur la licence octroyée :

- numéro de commande ;
- informations relatives à l'utilisateur qui reçoit la licence ;
- informations relatives à l'application qui peut être activée à l'aide de la licence octroyée ;
- restrictions associées au niveau du nombre (par exemple, le nombre de périphériques sur lesquels la licence permet l'utilisation de l'application) ;
- début de validité de la licence ;
- date d'expiration de la licence ou de l'abonnement ou durée de validité de la licence ;
- type de licence.

PRESENTATION DE LA CLE

La *clé* est une séquence de bits qui permet d'activer, puis d'utiliser l'application conformément aux dispositions du Contrat de licence. La clé est générée par les experts de Kaspersky Lab.

Vous pouvez ajouter la clé à l'application d'une des méthodes suivantes : appliquer une *clé* ou saisir un *code d'activation*. La clé apparaît dans l'interface de l'application sous la forme de séquence de caractères alpha-numériques uniques une fois que vous l'avez ajoutée à l'application.

La clé peut être bloquée par Kaspersky Lab en cas de non respect des dispositions du Contrat de licence. Si la clé est bloquée, il faudra ajouter une autre clé pour utiliser l'application.

Il existe des clés actives et des clés de réserve.

La *Clé active* est une clé utilisée au moment actuel pour faire fonctionner l'application. Une clé pour une licence d'évaluation ou une licence commerciale peut être ajoutée en tant que clé active. L'application ne peut compter qu'une seule clé active.

La *Clé de réserve* est une clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée en ce moment. Une clé de réserve devient automatiquement une clé active à l'échéance de la licence associée à la clé active en cours. La clé de réserve ne peut être ajoutée que si une clé active existe déjà.

La clé de la licence d'évaluation peut uniquement être ajoutée en tant que clé active. Il est impossible d'ajouter une clé pour licence d'évaluation en tant que clé de réserve.

PRESENTATION DU CODE D'ACTIVATION

Le *code d'activation* est une séquence unique de 20 caractères alpha-numériques latins. La saisie du code d'activation permet d'ajouter la clé qui va activer Kaspersky Endpoint Security. Le code d'activation est envoyé à l'adresse de messagerie électronique que vous avez indiquée après l'achat de Kaspersky Endpoint Security ou après la commande de la version d'évaluation de Kaspersky Endpoint Security.

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

Si vous perdez le code d'activation après l'activation de l'application, vous pouvez le récupérer. Le code d'activation est nécessaire pour ouvrir un Kaspersky CompanyAccount par exemple. Pour récupérer un code d'activation, contactez le Support Technique de Kaspersky Lab (https://companyaccount.kaspersky.com).

CONSULTATION DES INFORMATIONS SUR LA LICENCE

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

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans la partie inférieure droite de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre **Licence** s'ouvre.

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

- la clé active ;
- la clé de réserve, si elle a été ajoutée ;
- l'état de la clé ;
- le nombre d'ordinateurs sur lesquels vous pouvez utiliser l'application avec le licence ;
- la date et l'heure d'expiration de la licence ;
- le nombre de jours restant avant l'expiration de la licence.

Si l'application n'a pas été activée, la fenêtre **Licence** vous en informe. Vous pouvez activer l'application (cf. section "Activation de Kaspersky Endpoint Security" à la page 29).

Si vous utilisez une version d'évaluation de l'application, vous pouvez acheter une licence (cf. section "Achat d'une licence" à la page 29).

Si aucune clé de réserve n'a été ajoutée et que la licence associée à la clé active expire, vous pouvez la renouveler (cf. section "Renouvellement de la licence" à la page 29).

ACHAT D'UNE LICENCE

Si vous ne possédez pas de licence pour Kaspersky Endpoint Security ou si vous utilisez la version d'évaluation, vous pouvez acheter une licence.

Pour acheter une licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans la partie inférieure droite de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Acheter**.

Une page Internet qui fournit les informations sur les conditions d'achat d'une licence via la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la Société s'ouvre.

RENOUVELLEMENT DE LA LICENCE

La licence doit être renouvelée quand la licence associée à la clé active a expiré et qu'aucune clé de réserve n'a été ajoutée. A l'expiration de la durée de validité de la licence, l'application continue à fonctionner, mais ses fonctionnalités sont limitées (par exemple, la mise à jour et l'utilisation de Kaspersky Security Network ne sont pas disponibles). Vous pouvez continuer à utiliser tous les modules de l'application et réaliser des analyses contre les virus, mais uniquement à l'aide des bases anti-virus installées avant l'expiration de la validité de la licence.

Si les bases anti-virus sont dépassées, votre ordinateur est exposé au risque d'infection.

Pour renouveler la licence, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans la partie inférieure droite de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Renouveler**, cliquez sur le bouton **Arrêter**.

Une page Internet qui fournit les informations sur les conditions de renouvellement de la licence via la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la Société s'ouvre.

ACTIVATION DE KASPERSKY ENDPOINT SECURITY

Avant d'activer Kaspersky Endpoint Security, assurez-vous que la date et l'heure de l'ordinateur correspondent bel et bien à la date et à l'heure réelles.

Activer l'application consiste à ajouter une clé à l'application.

Quand l'application n'est pas activée, vous avez accès à toutes les fonctions de Kaspersky Endpoint Security, à l'exception de la réception des mises à jour. La mise à jour des bases anti-virus pourra être réalisée une seule fois après l'installation de l'application.

DANS CETTE SECTION

Activation de la version d'évaluation de l'application.....30

Activation de l'application à l'aide du code d'activation 30

ACTIVATION DE LA VERSION D'EVALUATION DE L'APPLICATION

L'activation de la version d'évaluation de Kaspersky Endpoint Security est possible uniquement si l'application installée sur l'ordinateur n'avait pas déjà été activée.

Il est conseillé d'activer la version d'évaluation de l'application si vous souhaitez explorer les capacités de l'application avant de décider d'acheter une licence. La version d'évaluation de Kaspersky Endpoint Security est opérationnelle durant une brève période. A l'issue de cette période, Kaspersky Endpoint Security ne remplit plus aucune de ses fonctions. Pour activer la version d'évaluation de l'application, vous recevrez une clé gratuite.

L'activation de l'application requiert une connexion à Internet.

Pour ouvrir activer la version d'évaluation de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans la partie inférieure droite de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Version d'évaluation**.
4. Dans la fenêtre **Activation de la version d'évaluation de l'application**, cliquez sur le bouton **Activer la version d'évaluation**.

   Kaspersky Endpoint Security contacte les serveurs d'activation de Kaspersky Lab et envoie les données à vérifier. Si la vérification donne un résultat valide, l'application reçoit et ajoute une clé gratuite.
5. Cliquez sur le bouton **Terminer** pour terminer l'activation de l'application.

Une fois que la version d'évaluation de l'application a été activée, la fenêtre **Licence** affiche les informations suivantes :

- l'état de la clé ;
- les restrictions sur le nombre d'ordinateurs sur lesquels vous pouvez utiliser l'application ;
- la date et l'heure d'expiration de la licence ;
- le nombre de jours restant avant l'expiration de la licence.

Une fois que la licence de la version d'évaluation de Kaspersky Endpoint Security arrive à échéance, le message correspond s'affiche. Pour renouveler la licence, vous devez acheter une licence (cf. section "Achat d'une licence" à la page 29).

ACTIVATION DE L'APPLICATION A L'AIDE DU CODE D'ACTIVATION

Le code d'activation permet à l'application de recevoir et d'ajouter automatiquement la clé qui garantit l'accès aux fonctions de Kaspersky Endpoint Security pendant la durée de validité de la licence.

L'activation de l'application requiert une connexion à Internet.

Pour activer l'application à l'aide du code d'activation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans la partie inférieure droite de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre **Licence** s'ouvre.

3. Dans la fenêtre **Licence**, cliquez sur le bouton **Arrêter**.

4. Dans la fenêtre **Activation de l'application**, saisissez le code d'activation obtenu lors de l'achat de Kaspersky Endpoint Security.

   Le code d'activation est une séquence unique de 20 caractères alpha-numériques latins au format xxxxx-xxxxx-xxxxx-xxxxx.

   Kaspersky Endpoint Security contacte les serveurs d'activation de Kaspersky Lab et envoie le code d'activation pour confirmer sa validité. Si le code d'activation est reconnu comme valide, l'application reçoit et installe automatiquement une clé.

5. Cliquez sur le bouton **Terminer** pour terminer l'activation de l'application.

   La fenêtre principale de l'application s'ouvre (cf. page 22).

   Si l'authenticité du code d'activation n'a pas été confirmée, le message correspondant s'affiche. Dans ce cas, contactez l'organisation qui vous a fourni le code d'activation pour obtenir des informations.

Une fois que l'application a été activée à l'aide de la clé, la fenêtre **Licence** affiche les informations suivantes :

- la clé ;
- l'état de la clé ;
- les restrictions sur le nombre d'ordinateurs sur lesquels vous pouvez utiliser l'application ;
- la date et l'heure d'expiration de la licence ;
- le nombre de jours restant avant l'expiration de la licence.

LANCEMENT ET ARRET DE L'APPLICATION

L'application est lancée automatiquement après l'installation et l'icône de Kaspersky Endpoint Security (cf. page 21) apparaît dans la barre de menus.

Pour quitter Kaspersky Endpoint Security, procédez comme suit :

1. Cliquez sur l'icône de Kaspersky Endpoint Security (à la page 21).
2. Dans le menu contextuel qui s'ouvre, choisissez l'option **Quitter**.

Le fonctionnement de l'application s'arrête et le processus sera supprimé dans la mémoire vive de l'ordinateur.

Une fois que vous avez quitté Kaspersky Endpoint Security, l'ordinateur continue à fonctionner sans protection. Il risque d'être infecté et vos données sont menacées.

ETAT DE LA PROTECTION DE L'ORDINATEUR

Cette section explique comment déterminer la présence de problèmes et de menaces contre la sécurité de l'ordinateur et comment configurer le niveau de protection. Vous apprendrez également à activer ou désactiver la protection pendant l'utilisation de l'application.

L'état de la protection de votre ordinateur reflète la présence ou l'absence de menaces qui influencent le niveau général de sécurité du système d'exploitation. Dans ce cas, les menaces sont non seulement les programmes malveillants découverts, mais aussi l'utilisation de bases anti-virus dépassées, la désactivation de l'Anti-Virus Fichiers ou de l'Anti-Virus Internet ou l'expiration prochaine de la validité de la licence.

Le Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35) permet d'examiner les menaces existantes et de les éliminer.

DANS CETTE SECTION

Evaluation de l'état de la protection de l'ordinateur 33

Désactivation de la protection de l'ordinateur 34

Rétablissement de la protection de l'ordinateur 35

Utilisation du Centre de protection 35

EVALUATION DE L'ETAT DE LA PROTECTION DE L'ORDINATEUR

L'indicateur de l'état de la protection de l'ordinateur représenté par un ordinateur et situé dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) signale les problèmes qui surviennent dans la protection. La couleur de l'indicateur change en fonction de l'état de la protection. Si une menace est présente dans le l'ordinateur, l'indicateur de couleur sera accompagné d'un message relatif aux menaces.

L'indice peut prendre une des valeurs suivantes :

- **Vert**. La protection de l'ordinateur est assurée au niveau adéquat.

  Un indicateur vert signale que les bases anti-virus de l'application sont mises à jour et que l'ensemble des composants de l'application fonctionne conformément aux paramètres recommandés par les spécialistes de Kaspersky Lab. Aucun objet malveillant n'a été décelé ou les objets malveillants découverts ont été neutralisés.

- **Jaune**. Le niveau de protection de votre ordinateur est abaissé.

  Un indicateur jaune signale un problème de fonctionnement de Kaspersky Endpoint Security. Par exemple, l'écart par rapport au mode de fonctionnement recommandé est négligeable, les bases de l'application n'ont pas été mises à niveau pendant quelques jours.

- **Rouge**. Votre ordinateur est exposé à un risque d'infection.

  Un indicateur rouge signale l'existence de problèmes graves qui pourraient entraîner l'infection de l'ordinateur ou la perte de données. Par exemple, les bases anti-virus de l'application sont sérieusement dépassées, l'application n'est pas activée ou un objet malveillant a été détecté.

Il est conseillé d'éliminer les problèmes et les menaces sur la sécurité de l'ordinateur.

DESACTIVATION DE LA PROTECTION DE L'ORDINATEUR

Kaspersky Endpoint Security est lancé par défaut au démarrage du système d'exploitation et protège l'ordinateur pendant la session. Tous les modules de la protection en temps réel (Anti-virus Fichiers, Anti-virus Internet et protection contre les attaques réseau) sont activés et fonctionnent.

Vous pouvez désactiver la protection par Kaspersky Endpoint Security complètement ou partiellement.

Les experts de Kaspersky Lab vous déconseillent vivement de désactiver la protection en temps réel de l'ordinateur, car cela pourrait entraîner l'infection de votre ordinateur et la perte de données.

Les éléments suivants témoignent de la désactivation de la protection en temps réel de l'ordinateur :

- icône de l'application inactive (cf. section "Icône de Kaspersky Endpoint Security" à la page 21) dans la barre de menus, si l'affichage de l'icône de l'application dans la barre de menus est activée ;
- couleur rouge de l'indicateur de l'état de la protection de l'ordinateur dans la fenêtre principale de l'application.

La protection en temps réel de l'ordinateur est garantie par Anti-Virus Fichiers (à la page 46), Anti-Virus Internet (à la page 50) et Protection contre les attaques réseau (à la page 53). La désactivation ou la suspension de ces modules n'a aucun impact sur l'exécution des tâches d'analyse (cf. section "Analyse" à la page 57) et de la tâche de mise à jour (cf. section "Mise à jour" à la page 63).

Pour désactiver la protection en temps réel de l'ordinateur, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Endpoint Security (à la page 21) dans la barre de menus et sélectionnez l'option **Désactiver la Protection** dans le menu contextuel.
- Ouvrez la fenêtre de configuration de l'application (à la page 23), choisissez l'onglet **Protection** et dans le groupe **Général**, décochez la case **Activer la Protection**.

Si vous avez désactivé la protection en temps réel de l'ordinateur, elle ne sera pas activée automatiquement après le redémarrage de Kaspersky Endpoint Security. Vous devez activer manuellement la protection en temps réel de l'ordinateur (cf. section "Restauration de la protection de l'ordinateur" à la page 35).

Pour désactiver un module de la protection en temps réel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres, dans le groupe **<nom du composant>**, décochez la case **Activer <nom du composant>**.

Si vous avez désactivé un module de la protection en temps réel, il ne se réactivera pas automatiquement après le redémarrage de Kaspersky Endpoint Security. Vous devez activer manuellement le module de protection en temps réel (cf. section "Restauration de la protection de l'ordinateur" à la page 35).

RETABLISSEMENT DE LA PROTECTION DE L'ORDINATEUR

Si la protection en temps réel de l'ordinateur ou un module de la protection en temps réel (Anti-Virus Fichiers, Anti-Virus Internet ou protection contre les attaques réseau) est désactivé, la seule manière de rétablir cette protection ou le fonctionnement d'un module de celle-ci est de procéder manuellement. Le rétablissement automatique de la protection en temps réel de l'ordinateur ou d'un module de la protection en temps réel après le redémarrage du système d'exploitation ou de Kaspersky Endpoint Security n'a pas lieu.

Pour activer la protection en temps réel de l'ordinateur, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Endpoint Security (à la page 21) dans la barre de menus et sélectionnez l'option **Activer la Protection** dans le menu contextuel.
- Ouvrez la fenêtre des paramètres de l'application (à la page 23), choisissez l'onglet **Protection** et dans le groupe **Général**, cochez la case **Activer la protection**.

Pour activer le module de la protection en temps réel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres, dans le groupe **<nom du composant>**, cochez la case **Activer <nom du composant>**.

De même, pour activer la protection en temps réel de l'ordinateur ou un module de la protection, vous pouvez utiliser le Centre de protection (cf. section "Centre de protection" à la page 35). La désactivation de la protection de l'ordinateur ou la désactivation des composants de la protection augmente considérablement le risque d'infection de l'ordinateur. Pour cette raison, les informations sur la désactivation sont conservées dans le Centre de protection.

UTILISATION DU CENTRE DE PROTECTION

Le *Centre de protection* est une fonction de Kaspersky Endpoint Security qui permet d'analyser et de supprimer les problèmes et les menaces existants sur la sécurité de l'ordinateur.

Pour ouvrir le Centre de protection,

cliquez sur le bouton **En savoir plus** dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) ;

La fenêtre Centre de protection permet d'afficher la liste des problèmes et des menaces contre la sécurité de l'ordinateur existants. Pour chaque problème ou menace, des actions sont proposées pour la résolution ou l'élimination. Vous pouvez résoudre le problème, éliminer la menace immédiatement ou traiter le problème ultérieurement.

Pour résoudre le problème ou éliminer la menace immédiatement,

cliquez sur le bouton reprenant le nom de l'action recommandée.

Par exemple, si des fichiers infectés ont été découverts sur l'ordinateur, il faut cliquer sur **Réparer**. Si les bases anti-virus sont dépassées, il faut cliquer sur **Mettre à jour**. L'application exécute l'action sélectionnée.

Pour reporter l'élimination du problème ou de la menace,

cliquez sur le bouton **Masquer**.

Le message concernant le problème ou la menace sera masqué dans la liste. Vous pourrez revenir à l'élimination de ce problème ou de cette menace ultérieurement.

Vous ne pouvez pas reporter l'élimination des menaces sérieuses sur la sécurité de l'ordinateur. Les menaces sérieuses sont, par exemple, la présence d'objets malveillants non réparés, un échec de fonctionnement des modules de la protection ou l'endommagement des bases anti-virus de Kaspersky Endpoint Security.

Si vous quittez le Centre de protection sans avoir éliminé les menaces sérieuses, la couleur de l'indicateur d'état de la protection de l'ordinateur dans la fenêtre principale de l'application ne change pas.

La fenêtre Centre de protection permet également de consulter les informations relatives à la tâche de mise en cours d'exécution et le cas échéant, d'arrêter la tâche.

RESOLUTION DES PROBLEMES TYPES

Cette section explique comment exécuter pas à pas les principales fonctions de l'application.

DANS CETTE SECTION

Procédure d'exécution d'une analyse complète de l'ordinateur 37

Réalisation d'une analyse rapide de l'ordinateur 38

Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque 38

Comment planifier le lancement automatique de l'analyse contre les virus 39

Procédure de mise à jour des bases de l'application 39

Que faire si l'application a bloqué l'accès au fichier 40

Que faire si l'application a placé le fichier en quarantaine ? 40

Que faire si vous soupçonnez l'infection d'un fichier par un virus 41

Procédure de restauration d'un fichier supprimé ou réparé par l'application 42

Emplacement du rapport sur le fonctionnement de l'application 42

Que faire en cas d'affichage de fenêtres de notification et de messages contextuels 43

PROCEDURE D'EXECUTION D'UNE ANALYSE COMPLETE DE L'ORDINATEUR

La tâche d'analyse complète (créée par défaut) de l'ordinateur fait partie de Kaspersky Endpoint Security. Dans le cadre de cette tâche, l'application analyse tous les disques durs de l'ordinateur à la recherche de virus et d'autres programmes dangereux.

Pour lancer la tâche d'analyse complète de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse complète**.

La tâche d'analyse complète de l'ordinateur démarre.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63).

REALISATION D'UNE ANALYSE RAPIDE DE L'ORDINATEUR

La tâche d'analyse rapide (créée par défaut) de l'ordinateur fait partie de Kaspersky Endpoint Security. Dans le cadre de cette tâche, l'application recherche la présence éventuelle de virus et autres programmes dangereux dans les secteurs critiques de l'ordinateur : dossiers contenant les fichiers du système d'exploitation et les bibliothèques système dont l'infection par des programmes malveillants pourrait endommager le système d'exploitation de l'ordinateur.

Pour lancer la tâche d'analyse rapide de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse rapide**.

La tâche d'analyse rapide de l'ordinateur démarre.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63).

COMMENT RECHERCHER D'EVENTUELS VIRUS DANS UN FICHIER, UN REPERTOIRE OU UN DISQUE

Si vous devez rechercher la présence éventuelle de virus et d'autres programmes dangereux dans un objet distinct (un des disques internes, un dossier ou un fichier en particulier ou un périphérique externe), vous pouvez utiliser la tâche préconfigurée **Analyse personnalisée**.

Pour rechercher la présence éventuelle de virus ou d'autres programmes dangereux dans un fichier, un dossier ou un disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse personnalisée**.

   La liste déroulante de composition de la zone d'analyse s'ouvre.
5. Dans la liste déroulante, choisissez l'option **Fichiers et dossiers** et désignez le fichier ou le dossier requis ou faites glisser sur la fenêtre les fichiers ou les dossiers pour lesquels vous souhaitez réaliser une analyse contre les programmes malveillants.

L'analyse contre les virus de la zone définie est lancée.

Pour lancer l'analyse, vous pouvez également faire glisser le fichier et le dossier sur l'icône de l'application dans le **Dock** ou dans la fenêtre principale de l'application (cf. page 22) ouverte.

Les résultats de l'exécution de la tâche de recherche de virus sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63).

COMMENT PLANIFIER LE LANCEMENT AUTOMATIQUE DE L'ANALYSE CONTRE LES VIRUS

Vous pouvez planifier l'exécution des tâches Analyse rapide et Analyse complète. Conformément à la planification établie, Kaspersky Endpoint Security lancera automatiquement la tâche et réalisera l'analyse sur l'ensemble de l'ordinateur ou dans les secteurs les plus critiques.

Pour configurer la planification du lancement des tâches Analyse rapide et Analyse complète, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.
4. Dans le groupe **Planification**, cochez la case dont le nom reprend la fréquence et l'heure de lancement de l'analyse contre les virus.
5. Si vous souhaitez modifier la planification du lancement de la tâche d'analyse contre les virus, cliquez sur le bouton **Planification**.

   La fenêtre qui permet de modifier la planification du lancement de la tâche d'analyse contre les virus s'ouvre.
6. Configurer la fréquence et l'heure du lancement de la tâche d'analyse contre les virus.
7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées à la planification du lancement de la tâche d'analyse contre les virus.

Les résultats de l'exécution des tâches d'analyse sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63).

PROCEDURE DE MISE A JOUR DES BASES DE L'APPLICATION

Par défaut, Kaspersky Endpoint Security récupère les mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Les *serveurs de mises à jour de Kaspersky Lab* sont des serveurs HTTP de Kaspersky Lab d'où les applications de Kaspersky Lab peuvent récupérer les mises à jour des bases et des modules.

Pour télécharger des mises à jour depuis les serveurs de mise à jour de Kaspersky Lab, l'ordinateur doit être connecté à Internet.

Par défaut, Kaspersky Endpoint Security recherche périodiquement la présence de mises à jour sur les serveurs de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Endpoint Security les télécharge en arrière-plan et les installe sur l'ordinateur.

Pour lancer la mise à jour manuelle de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton .

3. La fenêtre **Mise à jour** s'ouvre.

4. Dans la fenêtre **Mise à jour** qui s'ouvre, cliquez sur **Mettre à jour**.

Les résultats de l'exécution de la tâche de mise à jour sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution de la mise à jour" à la page 70).

QUE FAIRE SI L'APPLICATION A BLOQUE L'ACCES AU FICHIER

Kaspersky Endpoint Security bloque (cf. section Anti-Virus Fichiers" à la page 46) l'accès aux applications et aux fichiers infectés ou potentiellement infectés. Si un fichier est infecté, il est indispensable de le réparer pour y accéder.

Pour réparer les objets détectés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports, choisissez **Objets détectés**.

   La liste des objets détectés et de leur état sera affichée dans le groupe **Actifs** de la partie droite de la fenêtre. Pour développer la liste des objets, cliquez sur le bouton ▸.

4. Réparez tous les objets infectés détectés ou un d'entre eux :

   - Si vous souhaitez réparer tous les objets infectés détectés, cliquez sur le bouton **Tout réparer**.

     L'application commencera la réparation des objets détectés. Une fenêtre de notification apparaît lors de la réparation pour que vous puissiez sélectionner l'action à exécuter sur l'objet. Si, après la sélection des actions à réaliser sur les objets, vous cochez la case **Appliquer à tous les cas similaires** dans la fenêtre de notification, l'action sélectionnée sera appliquée à tous les fichiers de ce type.

   - Si vous souhaitez réparer un seul objet infecté détecté, sélectionnez-le dans la liste, puis cliquez sur le bouton **Réparer**.

     L'application commencera la réparation de l'objet sélectionné. Une fenêtre de notification apparaît lors de la réparation pour que vous puissiez sélectionner l'action à exécuter sur l'objet.

Si vous êtes convaincu que les fichiers bloqués par l'Anti-Virus Fichiers ne présentent aucun danger, vous pouvez les ajouter à la zone de confiance (cf. section "Constitution de la zone de confiance" à la page 45)

QUE FAIRE SI L'APPLICATION A PLACE LE FICHIER EN QUARANTAINE ?

Pour analyser, restaurer ou supprimer des fichiers potentiellement infectés placés en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**.

   La partie droite de la fenêtre reprend la liste des fichiers potentiellement infectés mis en quarantaine, ainsi que leur état.

4. Réalisez l'action requise sur l'ensemble des fichiers potentiellement infectés ou sur l'un d'entre eux :

   - Si vous souhaitez analyser tous les fichiers potentiellement infectés à l'aide de la version installée des bases anti-virus, cliquez sur le bouton **Tout analyser**. Suite à l'analyse, l'état du fichier en quarantaine peut devenir *faux positif*.

   - Si vous souhaitez restaurer un fichier potentiellement infecté, sélectionnez ce fichier dans la liste, puis cliquez sur le bouton **Restaurer**. La fenêtre dans laquelle vous devez saisir le nom du fichier et le dossier dans lequel il sera restauré s'ouvre.

     Il est conseillé de restaurer uniquement les fichiers portant l'état *faux positif* car la restauration de fichiers potentiellement infectés portant d'autres états peut constituer une menace pour votre ordinateur.

   - Si vous souhaitez supprimer un fichier potentiellement infecté de la quarantaine, sélectionnez-le dans la liste, puis cliquez sur le bouton **Supprimer**.

   - Si vous souhaitez supprimer tous les fichiers potentiellement infectés de la quarantaine, cliquez sur le bouton **Tout supprimer**.

Si vous êtes convaincu que les fichiers bloqués par l'Anti-Virus Fichiers ne présentent aucun danger, vous pouvez les ajouter à la zone de confiance (cf. section "Constitution de la zone de confiance" à la page 45)

QUE FAIRE SI VOUS SOUPÇONNEZ L'INFECTION D'UN FICHIER PAR UN VIRUS

Si vous soupçonnez l'infection potentielle d'un fichier, recherchez la présence éventuelle de virus ou d'autres programmes qui constituent une menace pour la sécurité de l'ordinateur (cf. section "Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque" à la page 38).

Si, à l'issue de l'analyse, Kaspersky Endpoint Security détermine que le fichier est sain et que vous pensez le contraire, placez ce fichier en *quarantaine*. Les fichiers placés en quarantaine sont compactés et représentent aucune menace pour votre ordinateur. Il se peut que Kaspersky Endpoint Security, après la mise à jour des bases anti-virus, soit en mesure d'identifier le programme malveillant qui a infecté le fichier et de le supprimer.

➧ *Pour placer le fichier en quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .
3. La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
4. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**.

   La partie droite de la fenêtre reprend la liste des fichiers potentiellement infectés mis en quarantaine, ainsi que leur état.

5. Cliquez sur le bouton **Ajouter un objet**.

   Le Finder s'ouvre.

6. Sélectionnez, dans la fenêtre du Finder, le fichier que vous souhaitez placer en quarantaine.

   Le fichier apparaîtra dans la liste des fichiers potentiellement infectés placés en quarantaine avec l'état *ajouté par l'utilisateur*.

PROCEDURE DE RESTAURATION D'UN FICHIER SUPPRIME OU REPARE PAR L'APPLICATION

Il n'est pas recommandé, sans urgence, de restaurer les copies de sauvegarde des fichiers. Cela pourrait en effet entraîner l'infection de votre ordinateur.

Il n'est pas toujours possible de préserver l'intégrité des fichiers infectés lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de le restaurer à partir de sa copie de sauvegarde.

Pour restaurer un fichier supprimé ou modifié lors de la réparation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la partie gauche de la fenêtre des rapports de l'application, choisissez **Sauvegarde**.
4. La partie droite de la fenêtre affichera le contenu de la Sauvegarde.
5. Dans la liste des copies de sauvegarde, sélectionnez les fichiers que vous souhaitez restaurer, puis cliquez sur le bouton **Restaurer**.

   La fenêtre dans laquelle vous devez saisir le nom du fichier et le dossier dans lequel il sera restauré s'ouvre. Le nom et l'emplacement d'origine du fichier sont proposés par défaut.
6. Indiquez le nom du fichier ou du dossier dans lequel le fichier va être restauré.
7. Cliquez sur le bouton **Enregistrer**.

L'application restaure le fichier dans l'emplacement indiqué avec le même nom.

Il est conseillé de réaliser une analyse contre les virus et autres programmes dangereux pour la sécurité de l'ordinateur directement après la restauration. Il sera possible de le réparer avec les bases anti-virus les plus récentes tout en préservant son intégrité.

EMPLACEMENT DU RAPPORT SUR LE FONCTIONNEMENT DE L'APPLICATION

Les informations relatives aux événements survenus pendant le fonctionnement de l'Anti-Virus Fichiers (cf. section "Anti-Virus Fichiers" à la page 46), de l'Anti-Virus Internet (cf. section "Anti-Virus Internet" à la page 50), de la Protection contre les attaques réseau (cf. section "Protection contre les attaques réseau" à la page 53), pendant l'exécution de l' analyse contre les virus (cf. section "Analyse contre les virus" à la page 57) ou lors de la mise à jour (cf. section "Mise à jour de l'application" à la page 63) sont présentées dans la fenêtre des rapports (cf. section "Consultation des rapports" à la page 74).

Pour ouvrir la fenêtre des rapports, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

QUE FAIRE EN CAS D'AFFICHAGE DE FENETRES DE NOTIFICATION ET DE MESSAGES CONTEXTUELS

Les notifications de l'application (cf. section "Fenêtres de notifications et fenêtres contextuelles" à la page 24) sous la forme de fenêtres de notification signalent les événements survenus pendant le fonctionnement de l'application et qui requièrent votre attention.

Quand un tel message apparaît, il faut sélectionner une des actions proposées. L'action optimale est celle qui est recommandée par les experts de Kaspersky Lab par défaut.

CONFIGURATION ETENDUE DE L'APPLICATION

Cette section contient les informations complémentaires sur la configuration des paramètres de chaque module de l'application.

DANS CETTE SECTION

Zone de protection de l'ordinateur 44

Anti-Virus Fichiers 46

Anti-Virus Internet 50

Prévention des intrusions 53

Analyse 57

Mise à jour de l'application 63

Rapports et stockages 71

Participation au Kaspersky Security Network 76

ZONE DE PROTECTION DE L'ORDINATEUR

La zone de protection de l'ordinateur dépend de la liste des catégories des objets détectés par l'application et des objets de la zone de confiance exclus de la protection de l'ordinateur. Pour constituer la zone de protection, il est nécessaire de sélectionner la catégorie d'objets détectée par l'application et d'ajouter les objets exclus de la protection de l'ordinateur dans la zone de confiance.

DANS CETTE SECTION

Sélection des catégories d'objets détectés 44

Constitution de la zone de confiance 45

SELECTION DES CATEGORIES D'OBJETS DETECTES

Les objets détectés par Kaspersky Endpoint Security sont répartis en différentes catégories selon diverses caractéristiques. L'application détecte toujours les virus, les vers, les chevaux de Troie et les utilitaires malveillants. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Pour garantir une plus grande sécurité de l'ordinateur, il est possible d'élargir la liste des objets détectés en activant le contrôle des actions des logiciels publicitaires ou autres applications légitimes qui pourraient être utilisées par un individu malintentionné pour nuire à l'ordinateur ou à vos données.

Les objets contre lesquels Kaspersky Endpoint Security vous protège sont répartis entre les catégories suivantes :

- **Virus, vers, chevaux de Troie et utilitaires malveillants**. Cette catégorie reprend tous les types d'applications malveillantes. Cette protection est le niveau minimal de sécurité admissible. Sur la recommandation des experts de Kaspersky Lab, Kaspersky Endpoint Security surveille toujours ce groupe de programmes malveillants.

- **Programme publicitaires**. Cette catégorie reprend les applications qui peuvent nuire au confort d'utilisation.

- **Numéroteurs**. Cette catégorie comprend les applications qui établissent des connexions téléphoniques via modem à l'insu de l'utilisateur.
- **Autres applications**. Cette catégorie reprend les programmes légitimes qui pourraient être utilisés par un individu malintentionné pour nuire à l'ordinateur ou aux données de l'utilisateur.

Pour sélectionner les catégories d'objets détectés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Menaces** de la fenêtre des paramètres de l'application, dans le groupe **Catégories des objets détectés**, cochez les cases en regard des catégories d'objets à détecter et contre lesquels Kaspersky Endpoint Security doit vous protéger.

   Kaspersky Endpoint Security assure toujours la protection de votre ordinateur contre les virus, les vers, les chevaux de Troie et les utilitaires malveillants. Pour cette raison, il est impossible de décocher la case à côté de cette catégorie.

En fonction de la catégorie d'objets à détecter sélectionnée, Kaspersky Endpoint Security utilise complètement ou partiellement les bases antivirus pendant le fonctionnement de l' Anti-Virus Fichiers (cf. section "Anti-Virus Fichiers" à la page 46), de l'Anti-Virus Internet (cf. section "Anti-Virus Internet" à la page 50) et lors de l'analyse contre les virus (cf. section "Analyse contre les virus" à la page 57).

Quand toutes les catégories d'objets sont sélectionnées, Kaspersky Endpoint Security garantit la protection maximale de l'ordinateur. Si seule la protection contre les virus, les vers, les chevaux de Troie et les utilitaires malveillants a été sélectionnée, Kaspersky Endpoint Security ne contrôle pas les programmes publicitaires ou autres qui peuvent être installés sur l'ordinateur et utilisés par des individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur.

Les experts de Kaspersky Lab vous recommandent de ne pas désactiver le contrôle des logiciels publicitaires et des numéroteurs automatiques. Si Kaspersky Endpoint Security place une application, qui d'après vous ne présente aucun danger, dans la catégorie des applications malveillantes, il est conseillé de l'ajouter à la zone de confiance (cf. section "Constitution de la zone de confiance" à la page 45).

CONSTITUTION DE LA ZONE DE CONFIANCE

La *Zone de confiance* est un ensemble d'objets constitué par l'utilisateur que Kaspersky Endpoint Security ne contrôle pas lors de son fonctionnement. En d'autres termes, il s'agit d'un ensemble d'exclusions de la protection de Kaspersky Endpoint Security.

La zone de confiance est composée sur la base des fichiers et des dossiers de confiance ainsi que selon la liste des adresses Internet considérées inoffensives par l'utilisateur. Lors de la composition de la zone de confiance, il faut tenir compte des particularités des objets que vous utilisez ainsi que des caractéristiques des applications installées. L'ajout d'objets à la zone de confiance peut s'imposer quand, par exemple, Kaspersky Endpoint Security bloque l'accès à un objet, une application ou un site Internet quelconque alors que vous êtes convaincu que cet objet, cette application ou ce site ne présente absolument aucun danger.

Quand une application est ajoutée à la liste des applications de confiance, l'activité de fichier et de réseau de celle-ci ne sera pas contrôlée (même les activités suspectes). C'est à ce moment que Kaspersky Endpoint Security analysera le fichier utilisé et le processus de l'application de confiance.

Pour consulter ou modifier la liste des fichiers et dossiers de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Menaces** de la fenêtre des paramètres, dans le groupe **Exclusions**, cliquez sur le bouton **Zone de confiance**.

   La fenêtre qui reprend la liste des objets qui ne sont pas contrôlés par Kaspersky Endpoint Security durant son fonctionnement sous l'onglet **Fichiers et dossiers de confiance** s'ouvre.

   Vous pouvez modifier la liste des fichiers et dossiers de confiance :

   - Ajouter un fichier ou un dossier à la liste.

     Cliquez sur le bouton + et dans la fenêtre standard qui s'ouvre, sélectionnez l'objet qui ne sera pas analysé par Kaspersky Endpoint Security.

   - Supprimer un fichier ou un dossier de la liste.

     Sélectionnez l'objet dans la liste, puis cliquez sur le bouton −.

Pour consulter ou modifier la liste des adresses Internet de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton ⚙.

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Menaces** de la fenêtre des paramètres, dans le groupe **Exclusions**, cliquez sur le bouton **Zone de confiance**.

   La fenêtre qui reprend la liste des adresses Internet qui ne sont pas contrôlées par Kaspersky Endpoint Security durant son fonctionnement sous l'onglet **Adresses Internet de confiance** s'ouvre.

   Vous pouvez modifier la liste des URL de confiance :

   - Ajouter une adresse Internet à la liste.

     Cliquez sur le bouton + et saisissez dans le champ l'adresse du site Internet que Kaspersky Endpoint Security n'analysera pas.

   - Supprimer une adresse Internet de la liste.

     Sélectionnez l'adresse Internet du site dans la liste, puis cliquez sur le bouton −.

ANTI-VIRUS FICHIERS

L'Anti-Virus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le module est lancé par défaut au démarrage du système d'exploitation. 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 les virus et autres applications présentant une menace. Si vous désactivez l'Anti-Virus Fichiers, il ne démarrera pas au lancement du système d'exploitation. Vous devrez lancer l'Anti-Virus Fichiers manuellement.

Vous pouvez définir une zone de protection (cf. section "Constitution de la zone de protection" à la page 48) et sélectionnez l'action qu'exécutera Kaspersky Endpoint Security en cas de détection d'un virus ou d'un autre programme qui constitue une menace pour la sécurité de l'ordinateur (cf. section "Sélection des actions de l'Anti-Virus Fichiers sur les objets" à la page 49).

Lorsque l'utilisateur ou l'application sollicite un fichier qui se trouve dans la zone de protection, l'Anti-Virus Fichier recherche la présence éventuelle de virus et autres applications présentant une menace pour la sécurité de l'ordinateur. Afin d'accélérer l'analyse contre les virus, Kaspersky Endpoint Security utilise la technologie iSwift.

Kaspersky Endpoint Security identifie les objets malveillants à l'aide de l' *analyse sur la base de signature*. La recherche d'éventuels virus et autres programmes dangereux pour la sécurité de l'ordinateur est organisée à l'aide des entrées de la base anti-virus de l'application. Outre l'analyse sur la base de signatures, l'Anti-Virus Fichiers utilise l'analyse heuristique et d'autres technologies d'analyse contre les virus.

En cas de détection d'un virus ou d'un autre programme qui présente un danger pour la sécurité de l'ordinateur dans un fichier, Kaspersky Endpoint Security attribue un des états suivants à l'objet détecté :

- L'état *infecté* si un programme malveillant a été détecté dans le fichier.
- L'état *potentiellement infecté* si le fichier contient un objet dont le code contient un segment modifié de code d'un programme malveillant ou un objet dont le comportement évoque un tel programme.

Kaspersky Endpoint Security affiche une notification sur l'objet détecté (cf. section "Présentation des fenêtres de notification" à la page 24) et exécute sur celui-ci l'action définie dans les paramètres de l'Anti-Virus Fichiers (cf. section "Sélection des actions de l'Anti-Virus Fichiers sur les objets" à la page 49).

Avant de réparer ou de supprimer un fichier infecté, Kaspersky Endpoint Security enregistre une copie dans la sauvegarde (cf. section "Sauvegarde" à la page 73)afin de pouvoir restaurer le fichier original le cas échéant. Kaspersky Endpoint Security place les fichiers potentiellement infectés en quarantaine (cf. page 71). Il sera peut-être possible de réparer ces fichiers plus tard à l'aide des bases anti-virus mises à jour.

Les informations relatives au fonctionnement de l'Anti-Virus Fichiers et à l'ensemble des objets détectés sont consignées dans le rapport de l'Anti-Virus Fichiers (cf. section "Consultation du rapport sur le fonctionnement de l'Anti-Virus Fichiers" à la page 49).

DANS CETTE SECTION

Désactivation de l'Anti-Virus Fichiers 47

Activation de l'Anti-Virus Fichiers 48

Constitution de la zone de protection 48

Sélection des actions de l'Anti-Virus Fichiers sur les objets 49

Consultation du rapport de fonctionnement de l'Anti-Virus Fichiers 49

DESACTIVATION DE L'ANTI-VIRUS FICHIERS

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

Pour désactiver l'Anti-Virus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Anti-Virus Fichiers**, décochez la case **Activer l'Anti-Virus Fichiers**.

Si vous avez désactivé l'Anti-Virus Fichiers, sachez qu'il ne sera pas réactivé automatiquement après le redémarrage de Kaspersky Endpoint Security ou du système d'exploitation. Vous devez activer manuellement l'Anti-Virus Fichiers (cf. section "Activation de l'Anti-Virus Fichiers" à la page 48).

ACTIVATION DE L'ANTI-VIRUS FICHIERS

Pour activer l'Anti-Virus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Anti-Virus Fichiers**, cochez la case **Activer l'Anti-Virus Fichiers**.

Vous pouvez également activer l'Anti-Virus Fichiers dans le Centre de protection (cf. section "Utilisation du centre de protection" à la page 35). La désactivation de la protection de l'ordinateur ou la désactivation des composants de la protection augmente considérablement le risque d'infection de l'ordinateur. Pour cette raison, les informations sur la désactivation sont conservées dans le Centre de protection.

CONSTITUTION DE LA ZONE DE PROTECTION

Par défaut, Anti-Virus Fichiers analyse tous les fichiers dès qu'une requête leur est adressée, quel que soit le support sur lequel ils se trouvent (disque interne, CD/DVD-ROM ou carte mémoire).

Pour composer la liste des zones de protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Anti-Virus Fichiers**, cliquez sur le bouton **Zone de protection**.

   La liste des objets qui seront analysés par l'Anti-Virus Fichiers apparaît dans la fenêtre qui s'ouvre. La protection est active par défaut pour tous les objets se trouvant sur des disques internes, des supports amovibles et les unités réseau connectées à l'ordinateur.

   Vous pouvez modifier la zone de protection :

   - Ajouter un objet à la zone de protection.

     Cliquez sur le bouton + et dans la fenêtre standard qui s'ouvre, sélectionnez le dossier ou le fichier.
   - Suspendre temporairement l'analyse d'un objet.

     Sélectionnez un objet et décochez la case à côté de cet objet. L'Anti-Virus Fichiers n'analyse pas cet objet tant que la case n'est pas à nouveau cochée.
   - Supprimer l'objet de la zone de protection (accessible uniquement pour les objets ajoutés par l'utilisateur).

     Sélectionnez un objet et faites-le glisser depuis la fenêtre ou cliquez sur le bouton −.

Utilisez une des méthodes suivantes pour limiter la zone de protection de l'Anti-Virus Fichiers :

- indiquer uniquement les répertoires, disques ou fichiers qui doivent être analysés ;
- composer une liste d'objets qu'il n'est pas nécessaire d'analyser (cf. section "Constitution de la zone de confiance" à la page 45) ;
- utiliser simultanément la première et la deuxième méthode, c.-à-d. définir une zone de protection dont sera exclue une série d'objets.

SELECTION DES ACTIONS DE L'ANTI-VIRUS FICHIERS SUR LES OBJETS

Si l'Anti-Virus Fichiers découvre un fichier infecté ou potentiellement infecté, il exécute une action en fonction de l'état de l'objet.

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

- L'état *infecté* si un programme malveillant a été détecté dans le fichier.
- L'état *potentiellement infecté* si le fichier contient un objet dont le code contient un segment modifié de code d'un programme malveillant ou un objet dont le comportement évoque un tel programme.

Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés. Kaspersky Endpoint Security affiche par défaut une fenêtre de notification dans laquelle il faudra sélectionner l'action à réaliser sur l'objet détecté.

Pour sélectionner l'action qui sera réalisée par l'Anti-Virus Fichiers lors de la détection d'un fichier infecté ou potentiellement infecté, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Anti-Virus Fichiers**, sélectionnez l'action de l'Anti-Virus Fichiers à exécuter sur l'objet malveillant détecté.

Avant de réparer ou de supprimer un fichier infecté, Kaspersky Endpoint Security enregistre une copie dans la sauvegarde (cf. section "Sauvegarde" à la page 73) afin de pouvoir restaurer le fichier original le cas échéant. Kaspersky Endpoint Security place les fichiers potentiellement infectés en quarantaine (cf. page 71). Il sera peut-être possible de réparer ces fichiers plus tard à l'aide des bases anti-virus mises à jour.

CONSULTATION DU RAPPORT DE FONCTIONNEMENT DE L'ANTI-VIRUS FICHIERS

Les statistiques de synthèse sur le fonctionnement en cours de l'Anti-Virus Fichiers (nombre d'objets analysés depuis le dernier lancement du module, nombre d'objets malveillants détectés et réparés) sont accessibles dans le Centre de protection, via le bouton **En savoir plus** dans la partie droite de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22).

Kaspersky Endpoint Security propose également un rapport détaillé sur le fonctionnement de l'Anti-Virus Fichiers dans la fenêtre des rapports.

Pour consulter le rapport de fonctionnement de l'Anti-Virus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la section **Tâches** de la fenêtre qui s'ouvre, choisissez **Anti-Virus Fichiers**.

Si le fonctionnement de l'Anti-Virus Fichiers s'est soldé par une erreur, consultez le rapport de l'Anti-Virus Fichiers et tentez de relancer le module. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 129).

La partie droite de la fenêtre des rapports reprend les informations suivantes sur le fonctionnement de l'Anti-Virus Fichiers :

- Toutes les périodes de fonctionnement de l'Anti-Virus Fichiers, avec la date et l'heure de lancement et d'arrêt du composant, ainsi que l'état du composant, sont affichées.
- Tous les objets détectés par l'Anti-Virus Fichiers et leur état sont affiché. Les objets sont regroupés par date et heure de lancement du module. Vous pouvez développer la liste des objets en cliquant sur l'icône ▸ située à côté de la date et de l'heure de lancement du module.

La partie inférieure de la fenêtre des rapports affiche, pour chaque fichier découvert, le nom et le chemin d'accès au dossier dans lequel il se trouve, ainsi que l'état que l'Anti-Virus Fichiers a attribué à l'objet. Si l'application a pu définir exactement le programme malveillant qui a infecté le fichier, elle lui attribue l'état *infecté*. S'il est impossible de définir avec exactitude le type de programme malveillant, le fichier recevra le statut *potentiellement infecté*.

La partie inférieure de la fenêtre des rapports affiche également des statistiques de synthèse sur le fonctionnement de l'Anti-Virus Fichiers. Les statistiques présentent des données sur le nombre d'objets analysés. L'heure de lancement de l'analyse contre les virus et sa durée sont également affichés.

ANTI-VIRUS INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur et les données qu'il contient à un risque d'infection par des virus et par d'autres applications présentant une menace pour sa sécurité. Ils peuvent s'infiltrer dans votre ordinateur quand vous téléchargez les programmes gratuits ou quand vous consultez les informations sur les sites Internet qui ont été soumis à des attaques d'individus malintentionnés avant votre visite. De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Internet ou le téléchargement d'un fichier, directement à l'ouverture de la connexion Internet.

Anti-Virus Internet protège les informations entrantes et sortantes de votre ordinateur via les navigateurs Safari, Google Chrome et Firefox sur les protocoles HTTP et HTTPS.

L'Anti-Virus Internet contrôle le trafic internet passant uniquement par les ports les plus fréquemment utilisés pour le transfert des données via le protocole HTTP et HTTPS.

L'Anti-Virus Internet analyse le trafic Internet conformément aux paramètres recommandés par les experts de Kaspersky Lab. Lorsque l'Anti-Virus Internet détecte une menace, il exécute l'action définie (cf. section "Sélection de l'action à réaliser sur les objets dangereux du trafic Internet" à la page 52). Les objets dangereux sont identifiés à l'aide des signatures, de l'analyse heuristique et des données fournies par le Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 76).

Algorithme d'analyse du trafic Internet

Chaque page Internet ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP ou HTTPS est intercepté et analysé par l'Anti-Virus Internet pour découvrir une présence éventuelle de code malveillant :

- Si la page Internet ou le fichier contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que le fichier ou la page Internet demandé est infecté.
- Si aucun code malveillant n'est détecté dans le fichier ou la page Internet, ceux-ci sont immédiatement accessibles.

Les informations relatives au fonctionnement de l'Anti-Virus Internet et à l'ensemble des objets détectés dans le trafic Internet sont consignées dans le rapport de l'Anti-Virus Internet (cf. section "Consultation du rapport sur le fonctionnement de l'Anti-Virus Internet" à la page 52).

DANS CETTE SECTION

Désactivation de l'Anti-Virus Internet 51

Activation de l'Anti-Virus Internet 51

Sélection de l'action à réaliser sur les objets dangereux du trafic Internet 52

Analyse des liens sur les pages Internet pour déterminer s'il s'agit de liens de phishing 52

Consultation du rapport de fonctionnement de l'Anti-Virus Internet 52

DESACTIVATION DE L'ANTI-VIRUS INTERNET

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

Pour désactiver l'Anti-Virus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres de l'application, dans le groupe **Anti-Virus Internet**, décochez la case **Activer l'Anti-Virus Internet**.

Si vous avez désactivé l'Anti-Virus Internet, alors après le redémarrage de Kaspersky Endpoint Security ou du système d'exploitation, il ne sera pas activé automatiquement. Vous devez activer manuellement l'Anti-Virus Internet (cf. section "Activation de l'Anti-Virus Internet" à la page 51).

ACTIVATION DE L'ANTI-VIRUS INTERNET

Pour activer l'Anti-Virus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres de l'application, dans le groupe **Anti-Virus Internet**, cochez la case **Activer l'Anti-Virus Internet**.

Vous pouvez également activer l'Anti-Virus Internet via le Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35). La désactivation de la protection de l'ordinateur ou la désactivation des composants de la protection augmente considérablement le risque d'infection de l'ordinateur. Pour cette raison, les informations sur la désactivation sont conservées dans le Centre de protection.

SELECTION DE L'ACTION A REALISER SUR LES OBJETS DANGEREUX DU TRAFIC INTERNET

En cas de détection d'objets dangereux dans le trafic Internet, l'application exécute l'action déterminée.

Pour sélectionner l'action à réaliser sur les objets dangereux détectés dans le trafic Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres de l'application, dans le groupe **Anti-Virus Internet**, sélectionnez l'action de l'Anti-Virus Internet sur l'objet.

ANALYSE DES LIENS SUR LES PAGES INTERNET POUR DETERMINER S'IL S'AGIT DE LIENS DE PHISHING

L'analyse des liens des pages Internet afin de déterminer s'il s'agit de liens de phishing ou de liens vers des URL dangereuses permet d'éviter les *attaques de phishing*. En règle générale, *les attaques de phishing* prennent la forme de messages électroniques envoyés par des individus malveillants au nom d'un organisme financier (ex. des banques) et comportent des liens qui renvoient vers un site Internet fictif de cet organisme. Dans ces messages, les individus malintentionnés proposent de passer sur le site fictif via les liens et d'y saisir des informations confidentielles (par ex. numéro de carte bancaire ou données d'identification pour l'accès aux services bancaires en ligne). L'exemple type est le message électronique envoyé par la banque dont vous êtes client et qui contient un lien vers son site officiel. Le lien vous renvoie vers la copie exacte du site Internet officiel de la banque, créée par les individus malintentionnés.

L'Anti-Virus Internet contrôle les tentatives d'accès à un site de phishing dans le cadre de l'analyse du trafic et bloque l'accès à de tels sites. Pour analyser les liens sur les pages Internet afin de déterminer s'il s'agit de liens de phishing ou de liens vers des adresses Internet dangereuses, Kaspersky Endpoint Security utilise les bases anti-virus de l'application, l'analyse heuristique et les données de Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network" à la page 76)

CONSULTATION DU RAPPORT DE FONCTIONNEMENT DE L'ANTI-VIRUS INTERNET

Kaspersky Endpoint Security offre un rapport détaillé sur le fonctionnement de l'Anti-Virus Internet.

Pour consulter le rapport de fonctionnement de l'Anti-Virus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la section **Tâches** de la fenêtre qui s'ouvre, choisissez **Anti-Virus Internet**.

Si le fonctionnement de l'Anti-Virus Internet s'est soldé par une erreur, consultez le rapport de l'Anti-Virus Internet et tentez de relancer le module. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 129).

La partie droite de la fenêtre des rapports reprend les informations suivantes sur le fonctionnement de l'Anti-Virus Internet :

- Toutes les périodes de fonctionnement de l'Anti-Virus Internet, avec la date et l'heure de lancement et d'arrêt de l'analyse, ainsi que l'état du fonctionnement du composant, sont affichées.

- Tous les objets dangereux détectés par l'Anti-Virus Internet dans le trafic Internet avec leur état sont affichés. Les objets sont regroupés par date et heure de lancement de l'analyse. Vous pouvez développer la liste des objets dangereux du trafic Internet d'un clic sur l'icône ▸ située à côté de la date et de l'heure du lancement de l'analyse.

La partie inférieure de la fenêtre des rapports indique pour chaque objet dangereux détecté dans le trafic Internet l'URL de la page où l'objet a été détecté, ainsi que l'état que lui a attribué l'Anti-Virus Internet.

La partie inférieure de la fenêtre des rapports affiche également des statistiques de synthèse sur le fonctionnement de l'Anti-Virus Internet. Les statistiques présentent des données sur le nombre d'objets analysés. L'heure de lancement de l'analyse et sa durée sont également affichés.

PREVENTION DES INTRUSIONS

Kaspersky Endpoint Security protège votre ordinateur contre les attaques réseau.

Une attaque réseau est une intrusion dans le système d'exploitation de l'ordinateur distant. Les individus mal intentionnés lancent des attaques réseau pour prendre la main sur le système d'exploitation, entraîner un déni de service ou accéder aux informations protégées.

Les attaques réseau sont des actions malveillantes exécutées par les malfaiteurs (par exemple, le balayage des ports et l'appairage des mots de passe). Il s'agit également d'actions entreprises par les programmes malveillants installés sur l'ordinateur attaqué (par exemple, la communication de données protégées au malfaiteur). Parmi les programmes malveillants impliqués dans les attaques réseau, il est possible de citer certains chevaux de Troie, les programmes pour les attaques DoS, les scripts malveillants et les différents vers réseau.

Les attaques réseau connues peuvent être classées dans les catégories suivantes :

- Balayage des ports. Ce type d'attaque réseau constitue généralement une étape de préparation à une attaque réseau plus importante. Les individus malintentionnés balaient les ports UDP- / TCP qui utilisent les services réseau sur l'ordinateur attaqué et définissent le degré de vulnérabilité de l'ordinateur attaqué face à des types d'attaques réseau plus dangereux. Le balayage des ports permet également aux individus malveillants de définir le type de système d'exploitation de l'ordinateur attaqué et de sélectionner les attaques réseau les mieux adaptées à ce type.

- *Attaques DoS*, ou attaques réseau, impliquant un déni de service. Il s'agit d'attaques réseau qui entraînent un dysfonctionnement partiel ou total du système d'exploitation.

  Types d'attaques DoS :

  - Envoi sur l'ordinateur distant de paquets réseau spécifiques imprévus qui entraînent des conflits dans le fonctionnement du système d'exploitation ou l'arrêt de ce dernier.

  - Envoi simultané à l'ordinateur distant d'une grande quantité de paquets réseau. Toutes les ressources de l'ordinateur attaqué sont occupées par le traitement des paquets envoyés par le malfaiteur et l'ordinateur arrête de remplir ses fonctions.

- *Intrusions réseau.* Il s'agit d'attaques réseau qui "kidnappent" le système d'exploitation de l'ordinateur attaqué. Il s'agit des attaques réseau les plus dangereuses car, si elles réussissent, le système d'exploitation passe intégralement sous le contrôle du malfaiteur.

  Ce type d'attaques réseau est utilisé lorsque les individus malintentionnés tentent d'obtenir des informations confidentielles à partir de l'ordinateur distant (par exemple, des numéros de carte bancaire, des mots de passe) ou d'utiliser l'ordinateur distant à leur avantage (par exemple, pour attaquer d'autres ordinateurs).

Lors que Kaspersky Endpoint Security détecte un attaque réseau, il consigne les informations relatives à celle-ci dans un rapport (cf. section "Consultation du rapport relatif à la prévention de intrusions" à la page 56).

DANS CETTE SECTION

Désactivation de la prévention des intrusions 54

Activation de la prévention des intrusions 54

Composition de la liste des ordinateurs de confiance 55

Affichage et modification de la liste des ordinateurs bloqués 55

Consultation du rapport relatif à la prévention des intrusions 56

DESACTIVATION DE LA PREVENTION DES INTRUSIONS

Par défaut, la protection contre les attaques réseau est activée et fonctionne selon le mode recommandé par les experts de Kaspersky Lab. En cas de nécessité, vous pouvez désactiver la Prévention des intrusions.

Pour désactiver la prévention des intrusions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Protection contre les attaques réseau**, décochez la case **Activer la protection contre les attaques réseau**.

Si vous avez désactivé la prévention des intrusions, sachez qu'elle ne sera pas réactivée automatiquement après le redémarrage de Kaspersky Endpoint Security ou du système d'exploitation. Vous devez activer manuellement la protection contre les attaques réseau (cf. section "Activation de la prévention des intrusions" à la page 54).

ACTIVATION DE LA PREVENTION DES INTRUSIONS

Pour activer la prévention des intrusions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Dans la fenêtre des paramètres, sous l'onglet **Protection**, dans le groupe **Protection contre les attaques réseau**, cochez la case **Activer la protection contre les attaques réseau**.

Vous pouvez également activer la protection contre les attaques réseau via le Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35). La désactivation de la protection de l'ordinateur ou la désactivation des composants de la protection augmente considérablement le risque d'infection de l'ordinateur. Pour cette raison, les informations sur la désactivation sont conservées dans le Centre de protection.

COMPOSITION DE LA LISTE DES ORDINATEURS DE CONFIANCE

Vous pouvez créer une liste des ordinateurs de confiance. Les adresses IP de ces ordinateurs ne seront pas bloquées automatiquement lors de la détection d'une activité réseau dangereuse.

Pour composer une liste des ordinateurs de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres de l'application, dans le groupe **Protection contre les attaques réseau**, cliquez sur le bouton **Exclusions**. Si la protection contre les attaques réseau est désactivée, il faudra l'activer (cf. section "Activation de la prévention des intrusions" à la page 54).

   La fenêtre comportant la liste des ordinateurs de confiance et la liste des ordinateurs bloqués s'ouvre.
4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Exclusions**.

   Vous pouvez exécuter les opérations suivantes :

   - Ajouter l'adresse IP de l'ordinateur de confiance à la liste.

     Cliquez sur le bouton + et saisissez l'adresse IP de l'ordinateur dont la fiabilité est assurée dans le champ prévu à cet effet.
   - Modifier l'adresse IP de l'ordinateur de confiance.

     Sélectionnez l'adresse IP dans la liste et cliquez sur le bouton **Modifier**.
   - Supprimer une adresse IP de la liste.

     Sélectionnez l'adresse IP dans la liste, puis cliquez sur le bouton −.
5. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées à la liste des ordinateurs de confiance.

AFFICHAGE ET MODIFICATION DE LA LISTE DES ORDINATEURS BLOQUES

Si une activité réseau dangereuse est détectée, l'adresse IP de l'ordinateur à l'origine de l'attaque est automatiquement ajoutée à la liste des ordinateurs bloqués, pour autant que cet ordinateur n'a pas été ajouté à la liste des ordinateurs de confiance (cf. section "Composition de la liste des ordinateurs de confiance" à la page 55).

Pour consulter et modifier la liste des ordinateurs bloqués, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres de l'application, dans le groupe **Protection contre les attaques réseau**, cliquez sur le bouton **Exclusions**. Si la protection contre les attaques réseau est désactivée, il faudra l'activer (cf. section "Activation de la prévention des intrusions" à la page 54).

   La fenêtre comportant la liste des ordinateurs de confiance et la liste des ordinateurs bloqués s'ouvre.

4. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Ordinateurs bloqués**. Cet onglet permet de consulter la liste des adresses IP des ordinateurs bloqués et l'heure de détection de l'activité réseau dangereuse qu'ils ont générée.

5. Si vous êtes certain de la fiabilité de l'ordinateur, sélectionnez l'adresse IP de cet ordinateur dans la liste et cliquez sur le bouton **Débloquer**.

6. Dans la fenêtre de confirmation, réalisez une des opérations suivantes :

   - Si vous souhaitez débloquer l'ordinateur, cliquez sur **Débloquer**.

     Kaspersky Endpoint Security débloque l'adresse IP.

   - Si vous souhaitez que Kaspersky Endpoint Security ne bloque jamais cette adresse IP, cliquez sur le bouton **Débloquer et ajouter aux exclusions**.

     Kaspersky Endpoint Security débloque l'adresse IP et l'ajoute à la liste des ordinateurs de confiance (cf. section "Composition de la liste des ordinateurs de confiance" à la page 55).

7. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées à la liste des ordinateurs bloqués.

CONSULTATION DU RAPPORT RELATIF A LA PREVENTION DES INTRUSIONS

La synthèse des statistiques de la prévention contre les intrusions (nombre d'ordinateurs bloqués, nombre d'événements enregistrés depuis le dernier lancement du module) est accessible dans le Centre de protection via le bouton **En savoir plus** de la partie droite de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22).

Kaspersky Endpoint Security propose également, dans la fenêtre des rapports, un rapport détaillé sur la prévention des intrusions.

Pour consulter le rapport sur la prévention des intrusions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la section **Tâches** de la fenêtre de rapports qui s'ouvre, choisissez **Protection contre les attaques réseau**.

Si le module Protection contre les attaques réseau rencontre une erreur, consultez le rapport et tentez de relancer le module. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 129).

La partie droite de la fenêtre des rapports reprend les informations suivantes sur le fonctionnement de la prévention des intrusions :

- Adresse IP de l'ordinateur pour lequel une activité réseau dangereuse a été détectée par Kaspersky Endpoint Security.

- Action exécutée par Kaspersky Endpoint Security lors de la détection d'une activité réseau dangereuse de l'ordinateur. Si l'adresse IP de l'ordinateur est bloquée et ajoutée à la liste des ordinateurs bloqués, la colonne **Action** indique Bloqué. Si l'adresse IP de l'ordinateur est ajoutée aux exclusions, la colonne **Action** indique Ignoré.

- Type d'attaque réseau détectée (cf. section "Protection contre les attaques réseau" à la page 53).
- Numéro du port local via lequel la tentative d'intrusion à eu lieu.
- Date et heure de la détection de l'activité réseau dangereuse de l'ordinateur.

ANALYSE

Outre la protection en temps réel de l'ordinateur à l'aide des composants Anti-Virus Fichiers (cf. section "Anti-Virus Fichiers" à la page 46) et Anti-Virus Internet (cf. section "Anti-Virus Internet" à la page 50), les experts de Kaspersky Lab conseillent de réaliser à intervalles réguliers une recherche de virus et autres programmes qui constituent une menace pour la sécurité de l'ordinateur. L'analyse contre les virus permet d'identifier les programmes malveillants qui n'ont pas été détectés par les modules de la protection, par exemple si la protection en temps réel avait été désactivée.

Kaspersky Endpoint Security comporte les tâches suivantes d'analyse contre les virus :

-  **Analyse complète**.

  Analyse antivirus de la mémoire, des objets de démarrage automatique et des disques internes de l'ordinateur.

-  **Analyse rapide**.

  Analyse antivirus, uniquement dans les zones importantes de l'ordinateur : dossiers contenant les fichiers du système d'exploitation et les bibliothèques système.

-  **Analyse personnalisée**.

  Recherche de virus sur un objet défini (fichier, dossier, disque, périphérique externe).

Lors du lancement de l'analyse contre les virus, Kaspersky Endpoint Security recherche la présence éventuelle de virus et autres programmes dangereux pour la sécurité de l'ordinateur dans la zone définie (cf. section "Constitution de la zone d'analyse" à la page 59). Vous pouvez lancer la tâche d'analyse manuellement (cf. section "Lancement et arrêt des tâches d'analyse" à la page 58). Vous pouvez également configurer le lancement automatique des tâches **Analyse complète** et **Analyse rapide** selon une planification définie (cf. section "Configuration de la planification du lancement de la tâche d'analyse contre les virus" à la page 62). Les tâches d'analyse sont exécutées par défaut selon les paramètres recommandés par les experts de Kaspersky Lab. Vous pouvez modifier les paramètres des tâches d'analyse (cf. section "Configuration de la planification du lancement de la tâche d'analyse contre les virus" à la page 60).

Kaspersky Endpoint Security identifie les objets malveillants à l'aide de l'analyse des signatures. Outre l'analyse sur la base de signatures, Kaspersky Endpoint Security utilise l'analyse heuristique et diverses technologies d'analyse.

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

- L'état *infecté* si un programme malveillant a été détecté dans le fichier.
- L'état *potentiellement infecté* si le fichier contient un objet dont le code contient un segment modifié de code d'un programme malveillant ou un objet dont le comportement évoque un tel programme.

En cas de détection d'un objet infecté ou potentiellement infecté, l'application affiche une notification qui invite l'utilisateur à choisir l'action à réaliser sur l'objet (cf. section "Présentation des fenêtres de notification" à la page 24). Vous pouvez modifier l'action exécutée en cas de détection d'un objet (cf. section "Sélection des actions à réaliser sur les objets lors de l'analyse" à la page 61).

Avant de réparer ou de supprimer un fichier infecté, Kaspersky Endpoint Security enregistre une copie dans la sauvegarde (cf. section "Sauvegarde" à la page 73) afin de pouvoir restaurer le fichier original le cas échéant. Kaspersky Endpoint Security place les fichiers potentiellement infectés en quarantaine (cf. page 71). Il sera peut-être possible de réparer ces fichiers plus tard à l'aide des bases anti-virus mises à jour. Par défaut, Kaspersky Endpoint Security analyse les fichiers en quarantaine après chaque mise à jour des bases anti-virus.

Les informations relatives aux résultats de l'exécution des tâches de recherche et de tous les objets détectés sont consignées dans le rapport sur l'exécution de la tâche d'analyse (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63).

DANS CETTE SECTION

Lancement et arrêt des tâches d'analyse 58

Constitution de la zone d'analyse 59

Configuration des paramètres des tâches d'analyse contre les virus 60

Consultation du rapport sur l'exécution des tâches d'analyse 63

LANCEMENT ET ARRET DES TACHES D'ANALYSE

Pour lancer la tâche d'analyse manuellement, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse contre les virus** qui s'ouvre, sélectionnez la tâche d'analyse que vous souhaitez lancer : **Analyse complète**, **Analyse rapide** ou **Analyse personnalisée**.
5. Si vous avez choisi la tâche **Analyse personnalisée**, une liste déroulante s'ouvre et vous permet de composer la zone d'analyse. Composez la zone d'analyse à l'aide de la liste (cf. section "Constitution de la zone d'analyse" à la page 59) ou déplacez le fichier ou le dossier dans la fenêtre.

La tâche d'analyse contre les virus est lancée.

Les informations relatives aux tâches d'analyse exécutées actuellement sont affichées dans la fenêtre **Analyse contre les virus** et dans la partie droite de la fenêtre principale de l'application, ainsi que dans la section **Tâches** de la fenêtre des rapports (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63). Les informations relatives aux tâches d'analyse exécutées sont également fournies dans la fenêtre **Analyse** et dans la section **Tâches** de la fenêtre des rapports.

Pour arrêter l'exécution de la tâche de recherche de virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse** qui s'ouvre, placez le curseur de la souris sur l'icône  en regard de la tâche d'analyse, puis cliquez sur le bouton  .
5. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur le bouton **Arrêter**.

L'analyse s'arrête.

CONSTITUTION DE LA ZONE D'ANALYSE

Les tâches **Analyse complète** et **Analyse rapide** incluses dans Kaspersky Endpoint Security possèdent déjà des zones d'analyse. Lors de l'exécution de la tâche Analyse complète, Kaspersky Endpoint Security analyse tous les fichiers de l'ensemble des disques internes de l'ordinateur, la mémoire et les objets à lancement automatique. Lors de l'exécution de la tâche Analyse express, Kaspersky Endpoint Security analyse la mémoire, les objets à lancement automatique et les dossiers, fichiers et bibliothèques du système.

Pour consulter ou modifier la zone d'analyse lors de l'Analyse complète et de l'Analyse express, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, dans la liste située à gauche, sélectionnez la tâche **Analyse complète** ou la tâche **Analyse rapide**.
4. Dans le groupe **Zone d'analyse** situé à droite, cliquez sur le bouton **Modifier**.

   Une fenêtre qui permet de créer une zone d'analyse s'ouvre.
5. Modifiez-la si nécessaire. Vous pouvez exécuter les opérations suivantes :
   - Ajouter un objet à la zone d'analyse.

     Faites glissez l'objet dans la fenêtre ou cliquez sur le bouton , puis sélectionnez dans la liste qui s'ouvre la variante la plus convenable (**Fichiers ou dossiers**, **Tous les disques**, etc).
   - Suspendre temporairement l'analyse d'un objet.

     Sélectionnez un objet et décochez la case à côté de cet objet. La tâche d'analyse ne sera pas exécutée pour cet objet tant que la case ne sera pas cochée à nouveau.
   - Supprimer l'objet (accessible uniquement pour les objets que vous avez ajoutés).

     Sélectionnez un objet et faites-le glisser depuis la fenêtre ou cliquez sur le bouton .
6. Cliquez sur le bouton **OK**.

Vous devez créer une zone d'analyse (fichiers, dossiers, disques, périphériques externe) pour l'exécution de la tâche **Analyse personnalisée**.

Pour définir la zone d'analyse de la tâche Analyse personnalisée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton .
3. La fenêtre **Analyse contre les virus** s'ouvre.
4. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche **Analyse personnalisée**.

   La liste déroulante de sélection de la zone d'analyse s'ouvre.
5. Dans la liste déroulante, choisissez l'option **Fichiers et dossiers** et désignez le fichier ou le dossier requis ou faites glisser sur la fenêtre les fichiers ou les dossiers pour lesquels vous souhaitez réaliser une analyse contre les programmes malveillants.

CONFIGURATION DES PARAMETRES DES TACHES D'ANALYSE CONTRE LES VIRUS

Vous pouvez configurer les paramètres suivants pour l'exécution des tâches d'analyse contre les virus :

- **Niveau de sécurité**

  Le *niveau de sécurité* désigne l'ensemble de paramètres qui définissent le rapport entre la minutie de l'analyse contre les virus et autres programmes dangereux pour l'ordinateur et la rapidité de celle-ci. Vous pouvez choisir un des trois niveaux prédéfinis de protection ou configurez les paramètres en fonction de vos préférences (cf. section "Sélection du niveau de sécurité" à la page 60).

- **Actions à réaliser sur les objets lors de l'analyse**

  Action que Kaspersky Endpoint Security exécute lors de la détection d'un objet infecté ou potentiellement infecté (cf. section "Sélection des actions à réaliser sur les objets lors de l'analyse" à la page 61).

- **Planification selon laquelle Kaspersky Endpoint Security lance automatiquement les tâches Analyse complète et Analyse rapide**

  Le lancement automatique d'une analyse contre les virus selon une planification permet de rechercher la présence éventuelle de virus et autres programmes dangereux sur l'ordinateur. Vous pouvez planifier le lancement des tâches Analyse rapide et Analyse complète (cf. section "Configuration de la planification du lancement de la tâche d'analyse contre les virus" à la page 62).

DANS CETTE SECTION

Sélection du niveau de sécurité....60

Sélection des actions à réaliser sur les objets lors de l'analyse....61

Configuration de la planification du lancement de la tâche d'analyse contre les virus 62

Restauration des paramètres d'analyse par défaut....62

SELECTION DU NIVEAU DE SECURITE

Chaque tâche d'analyse contre les virus se déroule selon un des niveaux de sécurité suivants :

- **Protection maximale** : niveau de sécurité qui correspond à l'analyse la plus complète de l'ordinateur ou d'un de ses disques, dossier ou fichier. Ce niveau de sécurité est recommandé si vous estimez que cet ordinateur est infecté.
- **Recommandé** : niveau de sécurité dont les paramètres sont recommandés par les experts de Kaspersky Lab.
- **Vitesse maximale** : niveau de sécurité qui permet de travailler avec les applications gourmandes en mémoire vive car le volume de fichiers analysés est réduit.

Par défaut, l'analyse contre les virus est exécutée selon le niveau de sécurité **Recommandé**. Vous pouvez augmenter ou réduire la minutie de l'analyse des objets en choisissant le niveau **Protection maximale** ou **Vitesse maximale** respectivement. Vous pouvez également modifier les paramètres du niveau de sécurité actuel. Dans ce cas, le nom du niveau de sécurité devient **Utilisateur**.

Pour modifier le niveau de sécurité de l'analyse contre les virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.

4. Déplacez le curseur dans le groupe **Niveau de sécurité**. En choisissant un niveau de sécurité, vous définissez le rapport entre la vitesse d'exécution et le volume d'objets à analyser : plus le nombre de fichiers soumis à l'analyse contre les virus sera réduit, plus la vitesse de l'analyse sera grande.

Afin de modifier les paramètres du niveau de sécurité en vigueur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.

4. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Préférences**.

   La fenêtre qui permet de modifier les paramètres du niveau de sécurité en vigueur s'ouvre.

5. Modifiez les paramètres du niveau de sécurité dans la fenêtre qui s'ouvre :

   - Dans le groupe **Types de fichier**, sélectionnez le type de fichiers qui seront repris dans l'analyse contre les virus de Kaspersky Endpoint Security.

   - Dans le groupe **Optimisation**, cochez ou décochez les cases et définissez les valeurs requises dans les champs afin de configurer les paramètres de performance de l'analyse et l'utilisation de la technologie iSwift.

   - Dans le groupe **Fichiers composés**, cochez ou décochez les cases en regard des types de fichiers composés qu'il faudra analyser.

   - Dans le groupe **Analyse heuristique**, cochez ou décochez la case **Utiliser l'analyse heuristique**. Si la case est cochée, déplacez le curseur afin de sélectionner le niveau d'analyse heuristique appliqué à l'analyse contre les virus.

6. Cliquez sur **OK** pour enregistrer les modifications des paramètres du niveau de sécurité.

SELECTION DES ACTIONS A REALISER SUR LES OBJETS LORS DE L'ANALYSE

Si Kaspersky Endpoint Security découvre un fichier infecté ou potentiellement infecté, il exécute l'action sélectionnée en fonction de l'état de l'objet.

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

- L'état *infecté* si un programme malveillant a été détecté dans le fichier.

- L'état *potentiellement infecté* si le fichier contient un objet dont le code contient un segment modifié de code d'un programme malveillant ou un objet dont le comportement évoque un tel programme.

Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés. Kaspersky Endpoint Security affiche par défaut une fenêtre de notification dans laquelle il faudra sélectionner l'action à réaliser sur l'objet détecté.

Pour sélectionner l'action exécutée par Kaspersky Endpoint Security sur les fichiers infectés ou potentiellement infectés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.

4. Dans le groupe **Action**, choisissez l'action de Kaspersky Endpoint Security sur l'objet malveillant détecté.

Avant de réparer ou de supprimer un fichier infecté, Kaspersky Endpoint Security enregistre une copie dans la sauvegarde (cf. section "Sauvegarde" à la page 73)afin de pouvoir restaurer le fichier original le cas échéant. Kaspersky Endpoint Security place les fichiers potentiellement infectés en quarantaine (cf. page 71). Il sera peut-être possible de réparer ces fichiers plus tard à l'aide des bases anti-virus mises à jour.

CONFIGURATION DE LA PLANIFICATION DU LANCEMENT DE LA TACHE D'ANALYSE CONTRE LES VIRUS

Toutes les tâches d'analyse intégrées peuvent être lancées manuellement (cf. section "Lancement et arrêt des tâches d'analyse" à la page 58). De plus, les tâches Analyse rapide et Analyse complète peuvent être lancées automatiquement par Kaspersky Endpoint Security selon une planification.

Pour configurer la planification du lancement des tâches Analyse rapide et Analyse complète, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.

4. Dans le groupe **Planification**, cochez la case dont le nom indique une planification de lancement de la tâche d'analyse contre les virus sélectionnée déjà définie. Si vous souhaitez modifier la planification du lancement de la tâche d'analyse contre les virus, cliquez sur le bouton **Planification**.

   La fenêtre qui permet de modifier la planification du lancement de la tâche d'analyse contre les virus s'ouvre.

5. Définissez la fréquence et l'heure du lancement de la tâche d'analyse contre les virus.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées à la planification du lancement des tâches d'analyse contre les virus.

RESTAURATION DES PARAMETRES D'ANALYSE PAR DEFAUT

Vous pouvez rétablir à tout moment les paramètres des tâches d'analyse par défaut. Ils sont recommandés par les experts de Kaspersky Lab et sont regroupés sous le niveau de sécurité **Recommandé**.

Pour restaurer les paramètres d'analyse par défaut, réalisez les opérations suivantes :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Analyse** de la fenêtre des paramètres de l'application, sélectionnez la tâche d'analyse dans la liste des tâches située à gauche.

4. Dans le groupe **Niveau de sécurité**, cliquez sur le bouton **Par défaut**.

   Les paramètres d'exécution de l'analyse contre les virus reprennent les valeurs recommandées. Le nom du niveau de sécurité devient **Recommandé**.

CONSULTATION DU RAPPORT SUR L'EXECUTION DES TACHES D'ANALYSE

Les informations relatives à l'exécution de chaque analyse en cours (en pourcentage) sont reprises dans la fenêtre **Analyse contre les virus** et dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22).

Kaspersky Endpoint Security propose également, dans la fenêtre des rapports, un rapport détaillé sur l'exécution des tâches d'analyse.

Pour consulter le rapport sur l'exécution des tâches d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la section **Tâches** de la fenêtre qui s'ouvre, choisissez **Analyse**.

Si des erreurs se sont produites suite à l'exécution de l'analyse, relancez-la. Si la nouvelle tentative d'exécution de l'analyse se solde également sur une erreur, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 129).

La partie droite de la fenêtre des rapports affiche les informations suivantes sur l'exécution de l'analyse par Kaspersky Endpoint Security :

- Toutes les tâches d'analyse en cours ou exécutées sont affichées avec le nom de la tâche, l'heure de début et de fin ainsi que l'état actuel de la tâche.
- Tous les objets détectés dans le cadre de la tâche sont affichés avec leur état. Les objets sont regroupés selon le nom de la tâche d'analyse. Vous pouvez développer une liste d'objet en cliquant sur l'icône ▸ située à côté du nom de la tâche d'analyse.

La partie inférieure de la fenêtre des rapports affiche, pour chaque objet découvert, le nom et le chemin d'accès au dossier dans lequel il se trouve, ainsi que l'état que Kaspersky Endpoint Security a attribué au fichier. Si l'application a pu définir exactement le programme malveillant qui a infecté le fichier, elle lui attribue l'état *infecté*. S'il est impossible de définir avec exactitude le type de programme malveillant, le fichier recevra le statut *potentiellement infecté*.

La partie inférieure de la fenêtre des rapports reprend également les informations sur l'exécution de la tâche d'analyse actuelle ou les statistiques de synthèse avec les résultats de la tâche d'analyse terminée. Les statistiques présentent des données sur le nombre d'objets analysés. L'heure de lancement de l'analyse et sa durée sont également affichés.

MISE A JOUR DE L'APPLICATION

La mise à jour en temps utiles des bases anti-virus de l'application est garante de la sécurité de votre ordinateur. L'Anti-Virus Fichiers (à la page 46), l'Anti-Virus Internet (à la page 50) et les tâches d'analyse (cf. section "Analyse" à la page 57) recherchent la présence éventuelle de virus et d'autres programmes qui constituent une menace et, le cas échéant, les neutralisent à l'aide des bases anti-virus. Les bases anti-virus sont enrichies chaque jour par les définitions des nouvelles menaces et les moyens de lutter contre celles-ci. Il est par conséquent vivement recommandé de les actualiser régulièrement.

Lors de la mise à jour, Kaspersky Endpoint Security télécharge les bases anti-virus et les mises à jour des modules de l'application depuis les serveurs de mises à jour de Kaspersky Lab et les installe sur votre ordinateur.

Les serveurs de mise à jour de Kaspersky Lab sont la principale source pour les mises à jour de Kaspersky Endpoint Security. Vous pouvez également utiliser les serveurs de Kaspersky Security Center en guise de source de mises à jour.

Pour réussir le téléchargement des mises à jour depuis les serveurs, la connexion de l'ordinateur à Internet est requise. Si la connexion à Internet s'opère via un serveur proxy, il faudra peut-être configurer les paramètres du réseau (cf. section "Configuration des paramètres de connexion au serveur proxy" à la page 70).

Le téléchargement des mises à jour des bases anti-virus s'opère selon l'un des modes suivants :

- **Automatiquement**. Kaspersky Endpoint Security recherche à intervalle régulier la présence d'un paquet de mises à jour sur les serveurs de Kaspersky Lab. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Endpoint Security les télécharge en arrière-plan et les installe sur l'ordinateur. Ce mode de mise à jour est utilisé par défaut.

- **Manuellement**. Vous lancez vous-même la procédure de mise à jour de Kaspersky Endpoint Security.

- **Selon la planification**. La mise à jour de Kaspersky Endpoint Security a lieu automatiquement conformément à la planification définie.

Par défaut, le téléchargement et l'installation des mises à jour des modules de Kaspersky Endpoint Security sur l'ordinateur se déroulent automatiquement.

Durant la mise à jour, les modules de l'application et des bases anti-virus présents sur l'ordinateur sont comparés aux modules et aux bases accessibles actuellement dans la source de la mise à jour. Si la dernière version des bases de l'application a été installée sur votre ordinateur, la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) indique que les bases sont à jour. Si les modules de l'application et les bases anti-virus diffèrent de deux proposés sur la source des mises à jour, l'ordinateur installe uniquement la partie manquante de la mise à jour. Les bases anti-virus ne sont pas copiées en entier, ce qui accélère la mise à jour et réduit le volume du trafic de réseau.

Avant de mettre à jour les bases anti-virus, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où il serait nécessaire de revenir à l'utilisation de la version précédente des bases. La possibilité de revenir à l'état antérieur à la mise à jour (cf. section "Annulation de la dernière mise à jour" à la page 65) est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte, qui amène Kaspersky Endpoint Security à bloquer une application qui ne présente aucun danger.

Si les bases de Kaspersky Endpoint Security sont endommagées, il est conseillé de lancer une mise à jour (cf. section "Procédure de mise à jour des bases de l'application" à la page 39) afin de télécharger et d'installer la version la plus récente des bases de l'application.

Parallèlement à la mise à jour, Kaspersky Endpoint Security peut copier les mises à jour récupérées dans une source locale (cf. section "Mise à jour depuis une source locale" à la page 65). Vous pouvez utiliser la copie locale des mises à jour récupérées pour mettre à jour les bases anti-virus de Kaspersky Endpoint Security et les modules sur les autres ordinateurs du réseau de l'organisation afin de réduire le trafic Internet.

DANS CETTE SECTION

Lancement de la mise à jour des bases de l'application 64

Annulation de la dernière mise à jour 65

Mise à jour depuis une source locale 65

Configuration de la mise à jour 66

Consultation du rapport sur l'exécution de la mise à jour 70

LANCEMENT DE LA MISE A JOUR DES BASES DE L'APPLICATION

La mise à jour en temps utiles de Kaspersky Endpoint Security permet de maintenir la protection de l'ordinateur au niveau requis.

Vous pouvez mettre à jour l'application à tout moment lors l'utilisation de Kaspersky Endpoint Security.

Pour lancer la mise à jour des bases de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Cliquez sur le bouton  .
3. La fenêtre **Mise à jour** s'ouvre.
4. Dans la fenêtre **Mise à jour** qui s'ouvre, cliquez sur **Mettre à jour**.

Les informations relatives à l'exécution de la tâche de mise à jour en cours (en pourcentage) sont reprises dans la partie inférieure de la fenêtre **Mise à jour**, ainsi que dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) et dans le Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35).

Les informations détaillées sur l'exécution de la mise à jour sont consignées dans le rapport sur l'exécution de la tâche de mise à jour (cf. section "Consultation du rapport sur l'exécution de la mise à jour" à la page 70).

ANNULATION DE LA DERNIERE MISE A JOUR

Avant de mettre à jour les bases anti-virus, Kaspersky Endpoint Security en crée une copie de sauvegarde au cas où il serait nécessaire de revenir à l'utilisation de la version précédente des bases. La possibilité de revenir à l'état antérieur à la mise à jour est utile, par exemple, si la nouvelle version des bases contient une signature incorrecte, qui amène Kaspersky Endpoint Security à bloquer une application qui ne présente aucun danger.

Si les bases de Kaspersky Endpoint Security sont endommagées, il est conseillé de lancer une mise à jour (cf. section "Procédure de mise à jour des bases de l'application" à la page 39) afin de télécharger et d'installer la version la plus récente des bases de l'application.

Pour revenir à l'état antérieur à la dernière mise à jour des bases anti-virus de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Retour à l'état antérieur**, cliquez sur le bouton **Revenir à l'état antérieur à la mise à jour**.

Les résultats de l'annulation de la dernière mise à jour sont présentés dans la fenêtre des rapports sur le fonctionnement de l'application (cf. section "Consultation du rapport sur l'exécution de la mise à jour" à la page 70).

MISE A JOUR DEPUIS UNE SOURCE LOCALE

Si plusieurs ordinateurs sont regroupés au sein d'un réseau local de l'organisation, il n'est pas nécessaire de télécharger la mise à jour de Kaspersky Endpoint Security sur chacun d'entre eux séparément, ce qui permet d'économiser le trafic Internet. Vous pouvez copier les mises à jour récupérées dans un dossier et mettre à jour les bases anti-virus de Kaspersky Endpoint Security et ses modules sur les autres ordinateurs localement, ce qui réduit le trafic Internet.

La récupération des mises à jour sera organisée de la manière suivante :

1. Un des ordinateurs du réseau reçoit le paquet de mises à jour de Kaspersky Endpoint Security depuis les serveurs de mise à jour de Kaspersky Lab ou depuis une autre source de mises à jour. Les mises à jour récupérées sont enregistrées dans un dossier partagé.

   Le dossier partagé doit être créé au préalable.

2. Les autres ordinateurs du réseau accèdent à ce dossier partagé qui fait office de source des mises à jour afin d'obtenir les mises à jour.

Pour activer la copie des mises à jour dans le dossier local, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Nouvelles versions**, cliquez sur le bouton **Préférences**.

   La fenêtre qui permet d'activer la copie des mises à jour dans un dossier local s'ouvre.
5. Sous l'onglet **Avancés**, cochez la case **Copier les fichiers de la mise à jour dans un dossier**, puis cliquez sur le bouton **Sélectionner**.

   Le Finder s'ouvre.
6. Dans le Finder, sélectionnez le dossier partagé dans lequel Kaspersky Endpoint Security enregistre les mises à jour récupérées.
7. Cliquez sur **Enregistrer** pour enregistrer les modifications des paramètres de la mise à jour.

CONFIGURATION DES PARAMETRES DE LA MISE A JOUR

Vous pouvez configurer les paramètres suivants de mise à jour de Kaspersky Endpoint Security :

- **Mise à jour des bases anti-virus**

  Permet de sélectionner le mode de lancement de la mise à jour : automatiquement (recommandé par les experts de Kaspersky Lab), manuellement ou selon une planification définie (cf. section "Configuration des paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security" à la page 68).

- **Nouvelles versions**

  Permet d'activer le téléchargement automatique et l'installation des mises à jour des modules de l'application sur l'ordinateur.

- **Sources des mises à jour**

  La source des mises à jour est une ressource qui contient les fichiers les plus récents de la base anti-virus et des modules de Kaspersky Endpoint Security. En guise de source des mises à jour, vous pouvez utiliser des serveurs HTTP, voire de répertoires locaux ou de réseau.

- **Proxy**

  Si la connexion Internet s'opère via un serveur proxy, vous pouvez configurer les paramètres de connexion au serveur proxy (cf. section "Configuration des paramètres de connexion au serveur proxy" à la page 70). Kaspersky Endpoint Security utilise ces paramètres pour la mise à jour des bases anti-virus et des modules de l'application.

- **Action après la mise à jour**

  Permet d'activer l'analyse automatique des fichiers en quarantaine après la fin de la mise à jour des bases anti-virus de l'application.

DANS CETTE SECTION

Sélection du mode de lancement de la mise à jour de Kaspersky Endpoint Security 67

Configuration des paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security 68

Désactivation du téléchargement automatique et de l'installation des mises à jour des modules de l'application sur l'ordinateur 68

Sélection de la source des mises à jour.....68

Configuration des paramètres de connexion au serveur proxy.....70

SELECTION DU MODE DE LANCEMENT DE LA MISE A JOUR DE KASPERSKY ENDPOINT SECURITY

Par défaut, le téléchargement des bases anti-virus et des modules de l'application depuis les serveurs de mises à jour de Kaspersky Lab s'opère automatiquement. Kaspersky Endpoint Security vérifie régulièrement la présence éventuelle d'un paquet de mise à jour sur la source de la mise à jour. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Endpoint Security les télécharge en arrière-plan et les installe sur l'ordinateur.

Vous pouvez sélectionner le mode de récupération du paquet de mises jour depuis les serveurs de Kaspersky Lab : automatiquement (recommandé par les experts de Kaspersky Lab), manuellement ou selon une planification définie (cf. section "Configuration des paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security" à la page 68).

Pour choisir le mode de lancement de la mise à jour de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton  .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Choisissez l'option qui vous convient dans le groupe **Mise à jour des bases anti-virus** :

   - Si vous souhaitez que le téléchargement et l'installation des bases anti-virus et des modules de l'application depuis les serveurs de mise à jour de Kaspersky Lab se déroulent automatiquement, choisissez l'option **Télécharger les mises à jour automatiquement**.
   - Si vous souhaitez lancer la mise à jour de l'application manuellement, choisissez l'option **Télécharger les mises à jour manuellement**.
   - Si vous souhaitez que la mise à jour de l'application soit lancée automatiquement selon une planification, choisissez l'option dont le nom reprend déjà la planification du lancement de la mise à jour. Vous pouvez modifier la planification du lancement de la mise à jour de l'application (cf. section "Configuration des paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security" à la page 68).

CONFIGURATION DES PARAMETRES DE LA PLANIFICATION DU LANCEMENT DE LA MISE A JOUR DE KASPERSKY ENDPOINT SECURITY

Pour configurer les paramètres de la planification du lancement de la mise à jour de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Mise à jour des bases anti-virus**, choisissez l'option dont le nom reprend la planification déjà définie pour le lancement de la mise à jour de l'application. Si vous souhaitez modifier la planification du lancement de la mise à jour de l'application, cliquez sur le bouton **Planification**.

   La fenêtre qui permet de configurer la planification du lancement de la mise à jour s'ouvre.
5. Définissez la fréquence et l'heure du lancement de la mise à jour de l'application.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications apportées à la planification du lancement de la mise à jour de l'application.

DESACTIVATION DU TELECHARGEMENT AUTOMATIQUE ET DE L'INSTALLATION DES MISES A JOUR DES MODULES DE L'APPLICATION SUR L'ORDINATEUR

Pour désactiver le téléchargement automatique et l'installation des mises à jour de l'application sur l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Nouvelles versions**, décochez la case **Mettre à jour les modules de l'application**.

S'il s'avère au moment de la mise à jour que la source contient non seulement les mises à jour des bases antivirus, mais également les mises à jour des modules de l'application, Kaspersky Endpoint Security récupère les mises à jour des modules de l'application et les installe après le redémarrage de l'ordinateur. Ces mises à jour des modules de l'application ne seront pas installées tant que l'ordinateur n'aura pas redémarré. Si une nouvelle mise à jour de l'application est publiée sur les serveurs de Kaspersky Lab avant le redémarrage de l'ordinateur et l'installation des mises à jour des modules de l'application récupérées antérieurement, Kaspersky Endpoint Security actualisera uniquement les bases antivirus.

SELECTION DE LA SOURCE DES MISES A JOUR

La source des mises à jour est une ressource qui contient les mises à jour des bases anti-virus et des modules de Kaspersky Endpoint Security. Il peut s'agir de serveurs HTTP, voire de répertoires locaux ou de réseau.

Les serveurs de mise à jour de Kaspersky Lab sont la principale source pour les mises à jour de Kaspersky Endpoint Security. Vous pouvez également utiliser les serveurs de Kaspersky Security Center en guise de source de mises à jour.

Pour choisir la source de mises à jour de Kaspersky Endpoint Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Nouvelles versions**, cliquez sur le bouton **Préférences**.

   La fenêtre qui permet de sélectionner les sources des mises à jour s'ouvre.
5. Sous l'onglet **Sources de la mise à jour**, cochez les cases en regard du nom des sources des mises à jour que vous souhaitez utiliser.

   Par défaut, les sources des mises à jour contiennent uniquement les serveurs de mises à jour de Kaspersky Lab et les serveurs de Kaspersky Security Center. En exécutant la mise à jour, Kaspersky Endpoint Security s'adresse à cette liste, sélectionne la première adresse du serveur de la liste et tente de télécharger les mises à jour depuis cette adresse. Si l'adresse sélectionnée ne répond pas, l'application choisit le serveur suivant et tente de télécharger à nouveau les bases antivirus. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que toutes les sources disponibles n'ont pas été sollicitées. La prochaine fois qu'il faudra récupérer les mises à jour, l'application s'adressera, en premier lieu, au serveur depuis lequel les mises à jour ont bien été obtenues la fois précédente.

   Vous pouvez exécuter les opérations suivantes :

   - Ajouter une nouvelle source de mises à jour dans la liste.

     Cliquez sur le bouton + et sélectionnez dans la liste déroulante l'option qui vous convient le mieux :

     - Si vous souhaitez ajouter un serveur local ou réseau en guise de source des mises à jour, choisissez l'option **Ajouter au dossier**. Dans la fenêtre du Finder qui s'ouvre, sélectionnez le dossier requis.
     - Si vous souhaitez ajouter une ressource Internet en guise de source des mises à jour, choisissez l'option **Ajouter l'adresse Internet**. Dans la fenêtre qui s'ouvre, saisissez l'adresse du serveur dans le champ **Adresse Internet de la source des mises à jour**.
   - Modifier une source de mises à jour.

     Double-cliquez pour sélectionner la source des mises à jour dans la liste et introduire les modifications.

     Les serveurs de mises à jour de Kaspersky Lab et les serveurs de Kaspersky Security Center sont des sources de mise à jour qui ne peuvent être ni modifiées, ni supprimées.
   - Désactiver temporairement l'obtention des mises à jour depuis une source.

     Sélectionnez une source de mises à jour dans la liste et décochez la case à côté de cette règle. La mise à jour de Kaspersky Endpoint Security depuis cette source ne sera pas exécutée jusqu'à ce que la case ne soit pas cochée de nouveau.
   - Supprimer la source des mises à jour (disponible uniquement pour les sources de mise à jour ajoutées par les utilisateurs).

     Sélectionnez une source de mises à jour dans la liste et cliquez sur le bouton −.
6. Cliquez sur **Enregistrer** pour enregistrer les modifications des paramètres de la mise à jour.

CONFIGURATION DES PARAMETRES DE CONNEXION AU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, vous pouvez configurer les paramètres de connexion à ce dernier. Kaspersky Endpoint Security utilise ces paramètres pour la mise à jour des bases anti-virus et le téléchargement des mises à jour des modules de l'application.

Pour configurer les paramètres de connexion au serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Choisissez l'onglet **Mise à jour**.
4. Dans le groupe **Proxy**, cochez la case **Utiliser le serveur proxy**, puis cliquez sur **Préférences**.

   La fenêtre qui permet de configurer les paramètres de connexion au serveur proxy s'ouvre.
5. Configurez les paramètres de connexion au serveur proxy.
6. Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications des paramètres de connexion au serveur proxy.

CONSULTATION DU RAPPORT SUR L'EXECUTION DE LA MISE A JOUR

Les brèves statistiques sur le fonctionnement actuel de la mise à jour (date d'édition des bases anti-virus, données sur l'actualité des bases utilisées) sont accessibles dans le Centre de protection via le bouton **En savoir plus** dans la partie droite de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) et dans la fenêtre **Mise à jour**.

Les informations relatives à la dernière mise à jour sont absentes si la mise à jour de Kaspersky Endpoint Security n'a pas encore été réalisée.

Les informations relatives à l'exécution de la tâche de mise à jour en cours (en pourcentage) sont reprises dans la fenêtre **Mise à jour**, ainsi que dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page 22) et dans le Centre de protection (cf. section "Utilisation du Centre de protection" à la page 35).

Kaspersky Endpoint Security propose également un rapport détaillé sur l'exécution des tâches de mise à jour dans la fenêtre des rapports.

Pour consulter le rapport sur l'exécution des tâches de mise à jour procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la section **Tâches** de la fenêtre qui s'ouvre, choisissez **Mise à jour**.

Si la tâche de mise à jour échoue, il faut vérifier les paramètres de connexion au serveur proxy (cf. section "Configuration des paramètres de connexion au serveur proxy" à la page 70) et tenter à nouveau la mise à jour. Si vous ne parvenez pas à résoudre vous-même le problème, contactez le Support Technique de Kaspersky Lab (cf. section "Contacter le Support technique" à la page 129).

La partie droite de la fenêtre des rapports affiche les informations suivantes sur l'exécution des mises à jour par Kaspersky Endpoint Security :

- Toutes les tâches de mise à jour en cours ou exécutées sont affichées avec l'heure de début et de fin, la taille des fichiers téléchargés et installés et la vitesse à laquelle le transfert de données a eu lieu.

- Toutes les opérations exécutées durant la mise à jour avec l'indication des noms des objets actualisés, des chemins d'accès aux dossiers où ces objets sont conservés et de l'heure d'appel vers ces objets. Les opérations sont regroupées par heure de lancement de la mise à jour. Pour développer la liste des opérations, cliquez sur l'icône ▸ située à côté de l'heure de lancement de la mise à jour.

RAPPORTS ET STOCKAGES

Kaspersky Endpoint Security crée une copie des fichiers infectés dans la sauvegarde avant de les réparer ou de les supprimer et il met en quarantaine les fichiers potentiellement infectés qu'il a détectés. Kaspersky Endpoint Security génère également un rapport sur le fonctionnement de chaque module de la protection.

DANS CETTE SECTION

Quarantaine 71

Sauvegarde 73

Consultation des rapports 74

Exportation des rapports 75

Activation de la consignation des événements à caractère informatif 75

Configuration de la durée de conservation des fichiers en quarantaine et dans la sauvegarde 76

QUARANTAINE

La *Quarantaine* est un dossier dans lequel Kaspersky Endpoint Security place les objets potentiellement infectés qu'elle a détectés. Les objets en quarantaine sont enregistrés sous forme chiffrée pour éviter qu'ils puissent agir sur l'ordinateur.

Un *objet potentiellement infecté* est un objet dont le code contient un segment modifié de code d'un programme dangereux connu ou un objet dont le comportement évoque un tel programme.

L'état *potentiellement infecté* peut être attribué à un fichier dans les cas suivants :

- Le code de l'objet analysé est semblable à celui d'une application malveillante connue, mais a été partiellement modifié.

  Les bases anti-virus de Kaspersky Endpoint Security contiennent des informations sur ces menaces qui ont été étudiées à ce jour par les experts de Kaspersky Lab. Si les bases ne contiennent pas encore les informations relatives à une modification d'une menace, alors Kaspersky Endpoint Security classe l'objet infecté par cette modification dans les objets potentiellement infectés et indique à quelle menace ressemble cette infection.

- Le code de l'objet infecté rappelle par sa structure celui d'un programme malveillant, mais les bases de Kaspersky Endpoint Security ne recensent rien de similaire.

Un fichier potentiellement infecté peut être détecté et placé en quarantaine par l'Anti-Virus Fichiers (cf. section "Anti-Virus Fichier" à la page 46) ou lors de l'exécution de tâche d'analyse (cf. section "Analyse" à la page 57). Vous pouvez également placer un fichier en quarantaine manuellement (cf. section "Que faire si vous soupçonnez l'infection d'un fichier par un virus" à la page 41).

AFFICHAGE DE LA QUARANTAINE

Pour consulter le contenu de la quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**.

La partie droite de la fenêtre affichera le contenu de la quarantaine.

ACTIONS SUR LES FICHIERS POTENTIELLEMENT INFECTES

Vous pouvez réaliser les opérations suivantes sur les fichiers potentiellement infectés :

- Placer manuellement des fichiers en quarantaine si vous pensez que le fichier est infecté par un virus ou un autre programme qui constitue une menace, alors qu'aucun programme malveillant n'a été détecté par Kaspersky Endpoint Security (cf. section "Que faire si vous soupçonnez l'infection d'un fichier par un virus" à la page 41).
- Analyser tous les fichiers potentiellement infectés en quarantaine à l'aide de la version installée des bases antivirus (cf. section "Que faire si l'application a placé le fichier en quarantaine ?" à la page 40).

  Vous pouvez activer l'analyse automatique des fichiers potentiellement infectés en quarantaine après chaque mise à jour des bases antivirus (cf. section "Activation de l'analyse automatique du contenu de la quarantaine après la mise à jour des bases antivirus" à la page 72).
- Restaurer les fichiers dans le dossier indiqué ou dans le dossier où ils se trouvaient avant d'être placés en quarantaine (cf. section "Que faire si l'application a placé le fichier en quarantaine ?" à la page 40).
- Supprimer les fichiers potentiellement infectés de la quarantaine (cf. section "Que faire si l'application a placé le fichier en quarantaine ?" à la page 40).

  Vous pouvez également configurer la suppression automatique des fichiers les plus anciens de la quarantaine (cf. section "Configuration de la durée de conservation des fichiers en quarantaine et dans la sauvegarde" à la page 76) à l'issue du nombre de jours défini.

ACTIVATION DE L'ANALYSE AUTOMATIQUE DU CONTENU DE LA QUARANTAINE APRES LA MISE A JOUR DES BASES ANTIVIRUS

Chaque mise à jour de la base anti-virus contient des nouveaux enregistrements qui permettent de protéger l'ordinateur contre les nouveaux virus et autres programmes qui présentent un danger. Les experts de Kaspersky Lab conseillent d'analyser à nouveau les fichiers placés en quarantaine (cf. page 71) après chaque mise à jour des bases anti-virus.

Kaspersky Endpoint Security n'analyse pas le contenu de la quarantaine directement après la mise à jour des bases si la section **Quarantaine** de la fenêtre des rapports de Kaspersky Endpoint Security est ouverte à ce moment.

Pour activer l'analyse automatique du contenu de la quarantaine après la mise à jour de la base anti-virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Choisissez l'onglet **Mise à jour**.

4. Dans le groupe **Action après la mise à jour**, cochez la case **Analyser la quarantaine**.

SAUVEGARDE

Il n'est pas toujours possible de préserver l'intégrité des fichiers infectés lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de restaurer le fichier original depuis la sauvegarde.

Copie de sauvegarde : la copie d'un fichier dangereux créée lors de la première réparation ou suppression de ce fichier et conservée dans la sauvegarde.

La *Sauvegarde* est un stockage spécial qui contient les copies de sauvegarde des fichiers supprimés ou modifiés lors de la réparation. La fonction principale de la sauvegarde est de permettre la restauration du fichier original à n'importe quel moment. Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger à l'ordinateur.

CONSULTATION DU CONTENU DE LA SAUVEGARDE

Vous pouvez consulter le contenu de la Sauvegarde dans la section **Sauvegarde** de la fenêtre des rapports de l'application.

Pour consulter le contenu de la Sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports de l'application, choisissez **Sauvegarde**.

La partie droite de la fenêtre affichera le contenu de la Sauvegarde.

ACTIONS SUR LES COPIES DE SAUVEGARDE DES FICHIERS

Vous pouvez restaurer et supprimer les copies de sauvegarde des fichiers de la Sauvegarde.

Pour restaurer une copie de sauvegarde d'un fichier de la Sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports de l'application, choisissez **Sauvegarde**.

   La partie droite de la fenêtre affichera le contenu de la Sauvegarde.

4. Dans la liste des copies de sauvegarde, sélectionnez les fichiers que vous souhaitez restaurer, puis cliquez sur le bouton **Restaurer**.

   La fenêtre dans laquelle vous devez saisir le nom du fichier et le dossier dans lequel il sera restauré s'ouvre. Le nom et l'emplacement d'origine du fichier sont proposés par défaut.

5. Indiquez le nom du fichier ou du dossier dans lequel le fichier va être restauré.

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

L'application restaure le fichier dans l'emplacement indiqué avec le même nom.

Il est conseillé de réaliser une analyse contre les virus et autres programmes dangereux pour la sécurité de l'ordinateur directement après la restauration. Il sera possible de le réparer avec les bases anti-virus les plus récentes tout en préservant son intégrité.

Il n'est pas recommandé, sans urgence, de restaurer les copies de sauvegarde des fichiers. Cela pourrait en effet entraîner l'infection de votre ordinateur.

Pour supprimer les copies de sauvegarde des fichiers du dossier de sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports de l'application, choisissez **Sauvegarde**.

   La partie droite de la fenêtre affichera le contenu de la Sauvegarde.

4. Sélectionnez les fichiers que vous souhaitez supprimer dans la liste des copies de sauvegarde :

   - Si vous souhaitez supprimer une ou plusieurs copies de sauvegarde de fichiers, sélectionnez-les, puis cliquez sur le bouton **Supprimer**.

   - Si vous souhaitez supprimer toutes les copies de sauvegarde des fichiers, cliquez sur le bouton **Tout supprimer**.

CONSULTATION DES RAPPORTS

Vous pouvez consulter le rapport de fonctionnement de Kaspersky Endpoint Security qui répertorie l'ensemble des objets détectés. Vous pouvez de même consulter les rapports sur le fonctionnement des composants et des fonctions suivantes de l'application : Anti-Virus Fichiers (cf. section "Consultation du rapport de fonctionnement de l'Anti-Virus Fichiers" à la page 49), Anti-Virus Internet (cf. section "Consultation du rapport de fonctionnement de l'Anti-Virus Internet" à la page 52), protection contre les attaques réseau (cf. section "Consultation du rapport relatif à la prévention des intrusions" à la page 56), analyse contre les virus (cf. section "Consultation du rapport sur l'exécution des tâches d'analyse" à la page 63) et mise à jour (cf. section "Consultation du rapport sur l'exécution de la mise à jour" à la page 70).

Pour ouvrir la fenêtre des rapports, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).

2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.

La fenêtre des rapports contient les rubriques suivantes :

- **Rapports**. Contient les informations sur tous les objets et fichiers détectés et placés dans la quarantaine ou conservés dans la sauvegarde. La section **Rapports** contient les sous-sections suivantes :

  - **Objets détectés**. Liste de tous les fichiers infectés ou potentiellement infectés découverts par l'Anti-Virus Fichiers et l'analyse ainsi que des objets dangereux du trafic Internet détectés par l'Anti-Virus Internet.

  - **Quarantaine**. Liste des fichiers mis en quarantaine.

  - **Dossier de sauvegarde**. Liste des fichiers placés dans la Sauvegarde.

- **Tâches.** Contient des rapports sur le fonctionnement des modules et des fonctions de Kaspersky Endpoint Security. La section **Tâches** contient les sous-sections suivantes :
  - **Mise à jour**. Rapport sur l'exécution des tâches de mise à jour.
  - **Analyse**. Rapport sur l'exécution des tâches d'analyse.
  - **Anti-Virus Fichiers**. Rapport de fonctionnement de l'Anti-Virus Fichiers.
  - **Anti-Virus Internet**. Rapport de fonctionnement de l'Anti-Virus Internet.
  - **Protection contre les attaques réseau**. Rapport relatif à la protection contre les attaques réseau.

EXPORTATION DES RAPPORTS

Kaspersky Endpoint Security peut enregistrer le rapport sur son fonctionnement dans un fichier texte. Cette possibilité peut être utile si l'Anti-Virus Fichiers, l'Anti-Virus Internet, l'analyse ou la mise à jour a produit une erreur que vous ne parvenez pas à corriger vous-même et qui requiert l'intervention du Support Technique de Kaspersky Lab (cf. "Contacter le Support technique" à la page 129). Dans ce cas, il faut envoyer le rapport au format texte au Support Technique pour que nos spécialistes puissent étudier le problème en détail et de le résoudre le plus vite possible.

Pour exporter le rapport sur le fonctionnement d'un module de Kaspersky Endpoint Security ou sur l'exécution d'une tâche dans un fichier texte, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des rapports de Kaspersky Endpoint Security s'ouvre.
3. Dans partie gauche de la fenêtre des rapports, sous la section **Tâches**, sélectionnez le rapport souhaité.
4. Dans la partie inférieure de la fenêtre des rapports, cliquez sur le bouton **Exporter**.
5. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier et le dossier dans lesquels le rapport doit être enregistré et cliquez sur le bouton **Enregistrer**.

ACTIVATION DE LA CONSIGNATION DES EVENEMENTS A CARACTERE INFORMATIF

Vous pouvez autoriser la consignation dans le rapport des événements informatifs (cf. section "Présentation des types d'événement" à la page 24).

Pour activer la consignation des événements à caractère informatif, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Rapports** de la fenêtre des paramètres de l'application, dans le groupe **Rapports**, cochez la case **Consigner les événements non critiques**.

CONFIGURATION DE LA DUREE DE CONSERVATION DES FICHIERS EN QUARANTAINE ET DANS LA SAUVEGARDE

Par défaut, la durée de conservation des fichiers dans la quarantaine et dans la sauvegarde est de 30 jours ; au terme de cette période les fichiers sont supprimés. Vous pouvez modifier la durée maximale de conservation des fichiers en quarantaine ou dans la sauvegarde ou ne pas imposer de limite.

Pour configurer la durée de conservation des fichiers en quarantaine et dans la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Rapports** de la fenêtre des paramètres de l'application, dans le groupe **Quarantaine et sauvegarde**, cochez la case **Supprimer les objets après** et indiquez la période à l'issue de laquelle les fichiers en quarantaine seront automatiquement supprimés.

PARTICIPATION AU KASPERSKY SECURITY NETWORK

Afin d'améliorer l'efficacité de la protection de votre ordinateur, Kaspersky Endpoint Security utilise les données obtenues auprès d'utilisateurs issus du monde entier. Le réseau Kaspersky Security Network permet d'analyser 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 nouvelles 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 d'obtenir 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 vous donne accès aux données relatives à la réputation des applications et des sites Internet.

La participation au Kaspersky Security Network signifie que les statistiques obtenues pendant l'utilisation de Kaspersky Endpoint Security sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

Aucune donnée personnelle n'est collectée, traitée et conservée.

La participation au Kaspersky Security Network est volontaire. Vous prenez cette décision pendant l'installation de Kaspersky Endpoint Security, mais vous pouvez la changer à tout moment.

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

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **KSN** de la fenêtre des paramètres de l'application, dans le groupe **Général** cliquez sur le bouton **Lire le texte complet du contrat** pour prendre connaissance de la Déclaration de Kaspersky Security Network.

4. Si vous êtes d'accord avec tous les points des Conditions, veuillez cocher la case **Je confirme ma participation au Kaspersky Security Network**.

5. Si vous souhaitez que les données obtenues via Kaspersky Security Network, soient utilisées pour analyser les fichiers et les classer, cochez la case **Utiliser pour l'analyse et le classement des fichiers**.

6. Si vous souhaitez que les données obtenues via Kaspersky Security Network, soient utilisées pour analyser les adresses Internet malveillantes, cochez la case **Utiliser pour vérifier les adresses Internet**.

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Endpoint Security à l'aide de la ligne de commande.

Après l'installation de la mise à jour des modules de Kaspersky Endpoint Security, la version du client de l'application dans la ligne de commande peut différer de la version installée.

La syntaxe de la ligne de commande est la suivante :

```
kav <commande> <paramètres>
```

Vous pouvez envoyer les <commandes> suivantes :

- help – aide sur la syntaxe de la commande, affichage d'une liste de commandes ;
- scan – analyse des objets à la recherche de programmes malveillants ;
- update – lancement de la mise à jour de l'application ;
- rollback – retour à l'état antérieur à la dernière mise à jour de Kaspersky Endpoint Security (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- start – lancement du composant ou de la tâche ;
- stop – arrêt du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- status – apparition à l'écran de l'état actuel du composant ou de la tâche ;
- statistics – apparition à l'écran des statistiques de fonctionnement du composant ou de la tâche ;
- export – exportation des paramètres du composant ou de la tâche ;
- import – importation des paramètres du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- addkey – activation de l'application à l'aide du fichier clé (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- exit – quitte l'application (l'exécution de cette instruction requiert les privilèges d'administrateur).

Chaque commande possède sa propre sélection de paramètres.

DANS CETTE SECTION

Consultation de l'aide....79

Recherche de virus....79

Mise à jour de l'application....81

Annulation de la dernière mise à jour....82

Lancement/arrêt d'un composant ou d'une tâche....82

Etat et statistiques du fonctionnement du composant ou de la tâche....83

Exportation des paramètres de protection....83

Importation des paramètres de protection....84

Activation de l'application....84

Arrêt de l'application....84

Codes de retour de la ligne de commande....84

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
kav -? | help
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
kav <commande> -?
kav help <commande>
```

RECHERCHE DE VIRUS

La ligne de commande pour le lancement de la recherche d'éventuels virus dans un secteur quelconque ressemble à ceci :

```
kav scan <zone d'analyse> <action> <types de fichiers> <exclusions> <paramètres du
rapport> <paramètres complémentaires>
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande (cf. section "Lancement/arrêt du fonctionnement du composant ou de la tâche" à la page 82). Dans ce cas, la tâche est réalisée selon les paramètres définis dans l'interface de Kaspersky Endpoint Security.

Description des paramètres

<zone d'analyse> : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace :

- <files> : liste des chemins d'accès aux fichiers et/ou dossiers à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques :
  - si le nom de l'objet ou le chemin d'accès contient un espace ou un caractère spécial ($, &, @, etc.), il doit être repris entre guillemets ou le caractère doit être précédé d'une barre oblique inverse ;
  - lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
- -all : analyse complète de l'ordinateur ;
- -remdrives : tous les disques amovibles ;
- -fixdrives : tous les disques durs ;
- -netdrives : tous les disques réseau ;

- -quarantine : quarantaine ;
- -@:<filelist.lst> : chemin d'accès au fichier contenant une liste d'objets et de dossiers à soumettre à l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. Seuls les chemins absolus au fichier sont admis.

Si la zone d'analyse n'est pas définie, Kaspersky Endpoint Security lance la tâche Analyse personnalisée avec les paramètres définis dans l'interface de l'application.

<action> : le paramètre définit les actions à réaliser sur les objets malveillants détectés lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur -i8. Les valeurs suivantes sont possibles :

- -i0 : ne réaliser aucune action sur l'objet, conserver uniquement les informations le concernant dans le rapport ;
- -i1 : réparer les objets infectés, si la réparation est impossible, les ignorer ;
- -i2 : réparer les objets infectés, si la réparation est impossible, les supprimer ; ne pas supprimer les objets infectés des conteneurs, sauf les conteneurs avec un en-tête exécutable (archives sfx) ;
- -i3 : réparer les objets infectés, si la réparation est impossible, les supprimer ; supprimer complètement les conteneurs s'il est impossible de supprimer les fichiers infectés qu'ils contiennent ;
- -i4 : supprimer les objets infectés ; supprimer complètement les conteneurs s'il est impossible de supprimer les fichiers infectés qu'ils contiennent ;
- -i8 : confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté (cette action est utilisée par défaut) ;
- -i9 : confirmer l'action auprès de l'utilisateur à la fin de l'analyse.

<types de fichiers> : définit les types de fichiers qui seront soumis à l'analyse antivirus. Par défaut, si le paramètre n'est pas défini, seuls seront analysés les objets pouvant être infectés en fonction du contenu. Les valeurs suivantes sont possibles :

- -fe : analyser les applications et les documents (selon l'extension) ;
- -fi : analyser les applications et les documents (selon le contenu) ;
- -fa : analyser tous les fichiers.

<exclusions> : ce paramètre définit les objets qui sont exclus de l'analyse. Il est possible d'utiliser plusieurs paramètres de la liste suivante, à condition de les séparer par un espace :

- -e:a : ne pas analyser les archives ;
- -e:b : ne pas analyser les bases de messagerie ;
- -e:m : ne pas analyser les messages électroniques au format texte ;
- -e:<mask> : ne pas analyser les objets en fonction du masque (cf. section "Masques dans les chemins d'accès aux fichiers et aux dossiers" à la page 137) ;
- -e:<seconds> : ignorer les objets dont l'analyse dure plus que la valeur définie en secondes ;
- -es:<size> : ignorer les objets dont la taille dépasse la valeur définie en mégaoctets.

<paramètres du rapport> : ce paramètre définit le format du rapport de l'analyse anti-virus. Les chemins relatifs et absolus au fichier pour l'enregistrement du rapport sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

- -r:<fichier du rapport> : consigner uniquement les événements importants dans le fichier indiqué ;
- -ra:<fichier du rapport> : consigner tous les événements dans le rapport.

<paramètres complémentaires> : paramètres qui définissent l'utilisation des technologies de l'analyse antivirus et l'utilisation du fichier de configuration :

- -iSwift=<on|off> : activer / désactiver l'utilisation de la technologie iSwift ;
- -c:<fichier de configuration> : ce paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les valeurs définies dans l'interface utilisateur de l'application sont utilisées en plus des valeurs déjà indiquées dans la ligne de commande.

Exemple :

Lancer l'analyse des dossiers ~/Documents, /Applications et du fichier my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Analyser les objets dont la liste est reprise dans le fichier objects2scan.txt. Utiliser le fichier de configuration scan_settings.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Exemple de fichier de configuration :

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

MISE A JOUR DE L'APPLICATION

La commande de mise à jour de l'application possède la syntaxe suivante :

```
kav update <source_de_la_mise_à_jour> -app=<on|off> <paramètres_de_rapport>
<paramètres_complémentaires>
```

Description des paramètres

<source_des_mises_à_jour> : serveur HTTP, répertoire réseau ou local utilisé pour le téléchargement des mises à jour. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.

-app=<on|off> : active/désactive la mise à jour des modules de l'application.

<paramètres du rapport> : ce paramètre définit le format du rapport de l'analyse anti-virus. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

- -r:<fichier du rapport> : consigner uniquement les événements importants dans le fichier indiqué ;
- -ra:<fichier du rapport> : consigner tous les événements dans le rapport.

<paramètres complémentaires> : paramètre qui définit l'utilisation du fichier de configuration des paramètres.

-c:<fichier de configuration> : ce paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour la mise à jour. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.

Exemple :

Actualiser les bases de l'application depuis la source par défaut et consigner tous les événements dans le rapport :

```
kav update -ra:avbases_upd.txt
```

Mettre à jour les modules de Kaspersky Endpoint Security en utilisant les paramètres du fichier de configuration updateapp.ini :

```
kav update -app=on -c:updateapp.ini
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
kav rollback <paramètres_du_rapport>
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<paramètres du rapport> : le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

- -r:<fichier du rapport> : consigner uniquement les événements importants dans le fichier indiqué ;
- -ra:<fichier du rapport> : consigner tous les événements dans le rapport.

Exemple :

kav rollback -ra:rollback.txt

LANCEMENT/ARRET D'UN COMPOSANT OU D'UNE TACHE

La commande pour le lancement d'un composant ou d'une tâche possède la syntaxe suivante :

```
kav start <nom de la tâche ou du composant> <paramètres du rapport>
```

Commande pour l'arrêt d'un composant ou d'une tâche possède la syntaxe suivante :

```
kav stop <nom de la tâche ou du composant>
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<nom de la tâche ou du composant> : il faut utiliser une des valeurs suivantes :

- fm ou file_monitoring : Anti-Virus Fichiers ;
- wm ou web_monitoring : Anti-Virus Internet ;
- full ou scan_my_computer : tâche d'analyse complète de l'ordinateur ;
- scan_objects : analyse de la zone indiquée ;
- quick ou scan_critical_areas : tâche d'analyse rapide de l'ordinateur ;
- updater : tâche de mise à jour ;
- rollback : tâche d'annulation de la mise à jour ;
- <nom de la tâche> : tâche définie par l'utilisateur.

<paramètres du rapport> : ce paramètre permet d'enregistrer le rapport sur l'exécution de la tâche ou le fonctionnement du composant dans le fichier indiqué. Vous pouvez saisir un chemin d'accès absolu ou relatif au fichier du rapport. Si le paramètre n'est pas défini, Kaspersky Endpoint Security affiche les résultats du fonctionnement du composant ou de l'exécution de la tâche à l'écran, conformément aux paramètres définis dans l'interface utilisateur graphique de l'application.

Vous pouvez désigner les paramètres suivants pour le rapport :

- -r:<fichier du rapport> : Kaspersky Endpoint Security consigne uniquement les événements importants dans le fichier indiqué ;
- -ra:<fichier du rapport> : Kaspersky Endpoint Security consigne tous les événements dans le fichier indiqué.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface utilisateur graphique du logiciel.

Exemple :

Pour activer l'Anti-Virus Fichiers, saisissez dans la ligne de commande :

```
kav start fm
```

Pour arrêter la tâche d'analyse complète, saisissez dans la ligne de commande :

```
kav stop scan_my_computer
```

ETAT ET STATISTIQUES DU FONCTIONNEMENT DU COMPOSANT OU DE LA TACHE

Syntaxe de la commande status :

```
kav status <nom de la tâche ou du composant>
```

Syntaxe de la commande statistics :

```
kav statistics <nom de la tâche ou du composant>
```

Description des paramètres

Le paramètre <nom de la tâche ou du composant> désigne une des valeurs reprises pour la commande start / stop (cf. section "Lancement/arrêt d'un composant ou d'une tâche" à la page 82).

Si la commande status est lancée sans définir la valeur du paramètre <nom de la tâche ou du composant>, l'application affichera l'état actuel de toutes ses tâches et composants à l'écran. La valeur du paramètre <nom de la tâche ou du composant> de la commande statistics doit être obligatoirement définie.

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav export <nom de la tâche ou du composant> <fichier d'exportation>
```

Description des paramètres

Le paramètre <nom de la tâche ou du composant> désigne une des valeurs reprises pour la commande start / stop (cf. section "Lancement/arrêt d'un composant ou d'une tâche" à la page 82).

<fichier d'exportation> : chemin d'accès au fichier dans lequel les paramètres de l'application sont exportés. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple :

```
kav export fm settings.txt – format texte
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav import <fichier d'importation>
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<fichier d'importation> : chemin d'accès au fichier contenant les paramètres de l'application à importer. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple :

kav import settings.dat

ACTIVATION DE L'APPLICATION

Kaspersky Endpoint Security peut être activé à l'aide d'un fichier clé.

Syntaxe de la commande :

```
kav addkey <fichier clé>
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<fichier clé> : fichier clé de l'application avec l'extension .key.

Exemple :

```
kav addkey 1AA111A1.key
```

ARRET DE L'APPLICATION

Syntaxe de la commande :

```
kav exit
```

L'exécution de cette commande requiert les privilèges d'administrateur.

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches reprennent les codes généraux et les codes spécifiques à un type de tâche en particulier.

Syntaxe de la commande de réception du code de retour :

```
echo $?
```

Codes de retour généraux :

- 0 – opération réussie ;
- 1 – valeur de paramètre invalide ;
- 2 – erreur inconnue ;
- 3 – erreur d'exécution de la tâche ;
- 4 – annulation de l'exécution de la tâche.

Codes de retour des tâches d'analyse antivirus :

- 101 – tous les objets malveillants ont été traités ;
- 102 – des objets malveillants ont été détectés.

ADMINISTRATION A DISTANCE VIA KASPERSKY SECURITY CENTER

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

L'application Kaspersky Security Center permet de résoudre de manière centralisée les principales tâches d'administration et de maintenance de la protection du réseau de l'organisation. Vous trouverez de plus amples informations sur l'application Kaspersky Security Center dans le *Manuel de l'administrateur de Kaspersky Security Center*

Vous pouvez également administrer Kaspersky Endpoint Security via l'interface utilisateur graphique de l'application (cf. section "Interface de l'application" à la page 21) et la ligne de commande (cf. section "Utilisation de l'application au départ de la ligne de commande" à la page 78).

DANS CETTE SECTION

Schéma de déploiement type de Kaspersky Endpoint Security 86

Installation du plug-in d'administration de Kaspersky Endpoint Security 87

Préparatifs pour l'installation de Kaspersky Endpoint Security 87

Gestion de l'Agent d'administration via la ligne de commande 90

Installation et suppression de Kaspersky Endpoint Security 92

Lancement et arrêt de l'application 100

Administration des stratégies 101

Administration des tâches 110

SCHEMA DE DEPLOIEMENT TYPE DE KASPERSKY ENDPOINT SECURITY

- *Pour déployer Kaspersky Endpoint Security sur le réseau de l'organisation, procédez comme suit :*

1. Déployez le *Serveur d'administration* sur le réseau.

   Il s'agit d'un composant de l'application Kaspersky Security Center qui remplit le rôle de conservation centralisée des informations relatives aux applications de Kaspersky Lab installées sur le réseau et qui permet de les administrer.

2. Installez la *Console d'administration* sur le poste de travail de l'administrateur de Kaspersky Security Center.

   Cette Console d'administration est un composant de l'application Kaspersky Security Center qui constitue l'interface utilisateur des services d'administration du Serveur d'administration et de l'Agent d'administration.

3. Installez le *plug-in d'administration de Kaspersky Endpoint Security* (cf. section "*Installation du plug-in d'administration Kaspersky Endpoint Security*" à la page 87) sur le poste de travail de l'administrateur de Kaspersky Security Center

   Le plug-in d'administration de Kaspersky Endpoint Security est un composant spécial qui offre une interface pour l'administration du fonctionnement de l'application de Kaspersky Lab via la Console d'administration. Chaque application possède son propre plug-in d'administration. Le plug-in d'administration est fourni avec toutes les applications de Kaspersky Lab qui peuvent être administrées à l'aide de Kaspersky Security Center.

4. Installez l'Agent d'administration sur les Mac distants d'une des manières suivantes :
   - localement (cf. section "Installation locale de l'Agent d'administration" à la page 88) ;
   - à distance via le protocole SSH (cf. section "Installation de l'Agent d'administration à l'aide du protocole SSH" à la page 89).
5. Installez Kaspersky Endpoint Security sur les Mac distants à l'aide d'une des méthodes suivantes :
   - localement (cf. section "Installation standard de Kaspersky Endpoint Security" à la page 17).
   - à distance via le protocole SSH (cf. section "Installation de l'application à l'aide du protocole SSH" à la page 93).
   - à distance, via Kaspersky Security Center (cf. section "Installation de l'application via Kaspersky Security Center" à la page 94).

Si des logiciels antivirus sont déjà installés sur les ordinateurs distants, il faudra les supprimer avant d'installer Kaspersky Endpoint Security.

Vous trouverez de plus amples informations sur le déploiement du Serveur d'administration et sur l'installation de la Console d'administration dans le *Manuel de déploiement de Kaspersky Security Center*.

INSTALLATION DU PLUG-IN D'ADMINISTRATION DE KASPERSKY ENDPOINT SECURITY

Pour installer le plug-in d'administration de Kaspersky Endpoint Security sur le poste de travail de l'administrateur, procédez comme suit :

1. Décompactez l'archive qui contient les fichiers de la distribution de Kaspersky Endpoint Security.
2. Ouvrez le dossier qui contient les fichiers de la distribution de Kaspersky Endpoint Security.
3. Dans la fenêtre où se trouve le contenu de la distribution, ouvrez le dossier **Security Center Console Plugin**.
4. Ouvrez le dossier contenant la version de l'application dans la langue qui vous convient.
5. Lancez le fichier exécutable klcfginst.exe.

Une fois l'installation du plug-in d'administration de Kaspersky Endpoint Security terminée, celui-ci est ajouté à la liste des plug-in d'administration des applications.

Avant d'installer le plug-in d'administration de Kaspersky Endpoint Security, il faut quitter la Console d'administration sur le poste de travail de l'administrateur de Kaspersky Security Center.

PREPARATIFS POUR L'INSTALLATION DE KASPERSKY ENDPOINT SECURITY

Cette section fournit des informations sur les modes d'installation de l'Agent d'administration sur un ordinateur distant.

Pour installer Kaspersky Endpoint Security sur un ordinateur distant via Kaspersky Security Center, il convient d'installer l'Agent d'administration sur l'ordinateur distant.

DANS CETTE SECTION

Installation locale de l'Agent d'administration 88

Installation de l'Agent d'administration à l'aide du protocole SSH 89

INSTALLATION LOCALE DE L'AGENT D'ADMINISTRATION

Pour installer l'Agent d'administration localement sur l'ordinateur de l'utilisateur, procédez comme suit :

1. Ouvrez le contenu de la distribution de l'Agent d'administration sur l'ordinateur de l'utilisateur.
2. Depuis la fenêtre affichant le contenu de la distribution ou depuis le fichier dmg, lancez l'installation de l'application d'un double-clic sur l'icône **Kaspersky Network Agent**.
3. Confirmez le lancement de l'installation de l'application dans la boîte de dialogue.
4. Dans la fenêtre **Introduction**, cliquez sur le bouton **Continuer**.
5. Dans la fenêtre **Informations**, lisez les renseignements relatifs à l'application qui va être installée.

   Assurez-vous que l'ordinateur distant répond à la configuration matérielle et logicielle requise. Pour imprimer ces informations, cliquez sur **Imprimer**. Pour exporter ces informations dans un fichier texte, cliquez sur **Enregistrer**. Pour poursuivre l'installation, cliquez sur **Poursuivre**.
6. Dans la fenêtre **Contrat de licence**, lisez le texte du contrat de licence sur l'utilisation de l'Agent d'administration, qui a été conclu entre vous et Kaspersky Lab. Ce texte est disponible en plusieurs langue. Pour imprimer le Contrat de licence, cliquez sur **Imprimer**. Pour exporter le Contrat de licence dans un fichier texte, cliquez sur **Enregistrer**.

   Si vous acceptez toutes les dispositions du Contrat de licence, cliquez sur **Poursuivre**. La boîte de dialogue de confirmation de l'acceptation des dispositions du Contrat de licence s'ouvre. Vous pouvez exécuter les opérations suivantes :

   - poursuivre l'installation de l'Agent d'administration en appuyant sur **J'accepte** ;
   - revenir au texte du Contrat de licence en cliquant sur **Lire le Contrat de licence** ;
   - interrompre l'installation de l'application en cliquant sur **Je refuse**.
7. Dans le champ **Serveur** de la fenêtre **Configuration**, saisissez l'adresse IP ou le nom DNS du serveur sur lequel Kaspersky Security Center est installé. Saisissez le numéro du port pour les connexions non sécurisées avec le serveur dans le champ **Port** et le numéro du port dédié aux connexions au serveur via SSL dans le champ **Port SSL**.

   Si vous ne souhaitez pas utiliser le protocole SSL pour établir la connexion avec le serveur, décochez la case **Utiliser SSL**. Pour poursuivre l'installation, cliquez sur **Poursuivre**.
8. Dans la fenêtre **Type d'installation**, analysez les informations relatives au disque sur lequel l'application va être installée.

   Pour installer l'application selon les paramètres standard proposés, cliquez sur **Installer** et saisissez le mot de passe d'administrateur.

   Patientez pendant que le programme d'installation de l'Agent d'administration installe les composants de l'application.
9. Cliquez sur le bouton **Terminer** pour quitter le programme d'installation.

INSTALLATION DE L'AGENT D'ADMINISTRATION A L'AIDE DU PROTOCOLE SSH

Avant d'installer l'Agent d'administration sur un ordinateur distant via le protocole SSH, assurez-vous que les conditions suivantes sont remplies :

- Le Serveur d'administration de Kaspersky Security Center est déployé sur le réseau de l'organisation.
- La Console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Security Center.
- Le paquet d'installation de l'Agent d'administration a été créé et il se trouve dans le dossier partagé du Serveur d'administration.

Vous trouverez de plus amples informations sur les paquets d'installation dans le *Manuel de l'administrateur de Kaspersky Security Center*.

Pour installer l'Agent d'administration sur un ordinateur distant via le protocole SSH, procédez comme suit :

1. Activez le service **Accès à distance** sur le Mac.
2. Lancez le client SSH sur le poste de travail de l'administrateur.
3. Connectez-vous au Mac distant.
4. Connectez le dossier partagé du Serveur d'administration en guide de disque réseau sur l'ordinateur distant. Pour se faire, saisissez les commandes suivantes dans le terminal du client SSH :

   ```
   mkdir /Volumes/KLSHARE
   ```

   ```
   mount_smbfs //<compte utilisateur d'administrateur>:<mot de passe>@<adresse IP du serveur d'administration>/KLSHARE /Volumes/KLSHARE
   ```

   Description des paramètres :

   - <compte utilisateur d'administrateur> : nom d'utilisateur de l'administrateur du Serveur d'administration ;
   - <mot de passe> : mot de passe de l'administrateur du Serveur d'administration ;
   - <Adresse IP du serveur d'administration> : adresse IP du serveur sur lequel Kaspersky Security Center est installé.

5. Lancez le script d'installation. Pour se faire, saisissez les commandes suivantes dans le terminal du client SSH :

   ```
   cd /Volumes/KLSHARE/Packages/<klnagent_package_folder>
   ```

   où <klnagent_package_folder> représente le dossier qui contient le paquet d'installation de l'Agent d'administration.

   ```
   sudo ./install.sh -r <serveur> [-s <action>] [-p <numéro de port>] [-l <numéro du port SSL>]
   ```

   Description des paramètres :

   - <action> : paramètre qui définit l'utilisation du chiffrement pour la connexion entre l'Agent d'administration et le Serveur d'administration. Si la valeur est 0, la connexion ne sera pas sécurisée. Si la valeur est 1, la connexion utilise le protocole SSL (valeur par défaut ;
   - <serveur> : adresse IP ou nom DNS du serveur sur lequel Kaspersky Security Center est installé ;
   - <numéro du port> : numéro du port via lequel la connexion non sécurisée au Serveur d'administration est établie. Il s'agit par défaut du port 14000 ;
   - **<numéro de port SSL>** : numéro du port via lequel la connexion sécurisée au Serveur d'administration via le protocole SSL est établie. Il s'agit par défaut du port 13000.

L'exécution de cette commande requiert les privilèges d'administrateur.

6. Ejectez le disque réseau de l'ordinateur distant. Saisissez pour ce faire la commande suivante dans le terminal du client SSH :

   ```
   umount /Volumes/KLSHARE
   ```

7. Vérifiez le fonctionnement de l'Agent d'administration sur l'ordinateur distant. Pour se faire, saisissez les commandes suivantes dans le terminal du client SSH :

   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```

   Si l'essai réussit, l'Agent d'administration fonctionne normalement.

GESTION DE L'AGENT D'ADMINISTRATION VIA LA LIGNE DE COMMANDE

Cette section fournit des informations sur la gestion de l'Agent d'administration à l'aide de la ligne de commande sur l'ordinateur de l'utilisateur.

Vous pouvez arrêter l'Agent d'administration et le relancer.

Vous pouvez également connecter un ordinateur distant au Serveur d'administration manuellement à l'aide de l'utilitaire klmover et vérifier la connexion entre l'ordinateur distant et le Serveur d'administration via l'utilitaire klnagchk.

DANS CETTE SECTION

Lancer/arrêt de l'Agent d'administration sur l'ordinateur distant.....90

Connexion manuelle de l'ordinateur distant au Serveur d'administration. Utilitaire klmover 91

Vérification manuelle de la connexion de l'ordinateur distant au Serveur d'administration Utilitaire klnagchk 92

LANCER/ARRET DE L'AGENT D'ADMINISTRATION SUR L'ORDINATEUR DISTANT

Vous pouvez utiliser la ligne de commande pour arrêter l'Agent d'administration sur l'ordinateur distant et pour le relancer.

- *Pour arrêter l'Agent d'administration,*

  lancez l'utilitaire launchctl sur l'ordinateur distant en saisissant la commande unload sur la ligne de commande.

Syntaxe de la commande

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

- *Pour lancer l'Agent d'administration,*

  lancez l'utilitaire launchctl sur l'ordinateur distant en saisissant la commande load sur la ligne de commande.

Syntaxe de la commande

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

L'arrêt et le lancement de l'Agent d'administration requièrent des privilèges d'administrateur.

CONNEXION MANUELLE DE L'ORDINATEUR DISTANT AU SERVEUR D'ADMINISTRATION. UTILITAIRE KLMOVER

Pour connecter l'ordinateur distant au Serveur d'administration,

lancez l'utilitaire klmover, qui fait partie de la distribution de l'Agent d'administration, via la ligne de commande sur l'ordinateur distant.

Après l'installation de l'Agent d'administration, cet utilitaire se trouve dans le dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries et il peut exécuter les opérations suivantes lorsqu'il est exécuté via la ligne de commande, quels que soient les paramètres utilisés :

- connexion de l'Agent d'administration au Serveur d'administration selon les paramètres indiqués ;
- consignation des résultats de l'exécution de l'opération dans le fichier indiqué ou affichage de ceux-ci à l'écran.

Avant de lancer l'utilitaire, accédez au dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntaxe de l'utilitaire :

```
sudo ./klmover [-logfile <nom du fichier>] [-address <adresse du serveur>] [-pn <numéro du port>] [-ps <numéro du port SSL>] [-nossl] [-cert <chemin du fichier de certificat>] [-silent] [-dupfix]
```

L'exécution de l'utilitaire requiert les privilèges d'administrateur.

Description des paramètres :

-logfile <nom du fichier> : les résultats de l'exécution de l'utilitaire sont consignés dans le fichier indiqué ; si le paramètre n'a pas été défini, les résultats et les messages d'erreur sont affichés à l'écran.

-address <adresse du serveur> : adresse du Serveur d'administration en vue de la connexion ; l'adresse peut être l'adresse IP ou le nom DNS du serveur.

-pn <numéro du port> : numéro du port utilisé pour établir la connexion non sécurisée au Serveur d'administration. Par défaut, il s'agit du port 14000.

-ps <numéro de port SSL> : numéro du port via lequel la connexion sécurisée au Serveur d'administration via le protocole SSL est établie. Par défaut, il s'agit du port 13000.

-nossl : utilisation d'une connexion non sécurisée au Serveur d'administration ; si la valeur n'est pas définie, la connexion de l'Agent d'administration au serveur sera réalisée via le protocole sécurisé SSL.

-cert <chemin d'accès au fichier> : utilise le fichier de certificat indiqué en vue de l'authentification sur un nouveau Serveur d'administration. Si le paramètre n'est pas défini, l'Agent d'administration recevra le certificat lors de la première connexion au Serveur d'administration.

-silent : exécution de l'utilitaire en mode silencieux.

-dupfix : ce paramètre est utilisé si l'installation de l'Agent d'administration a été réalisée sur les ordinateurs non pas selon les méthodes suggérées dans le Manuel de l'administrateur, mais, par exemple via une restauration depuis une image de disque doté de l'agent d'administration. Si l'authentification automatique de l'Agent d'administration entraîne le dédoublement des icônes de l'ordinateur d'origine et des autres ordinateurs dans la Console d'administration, vous pouvez connecter à nouveau les ordinateurs en double.

Il est conseillé d'attribuer une valeur à tous les paramètres si vous souhaitez lancer l'utilitaire.

Exemple :

```
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001
```

L'ordinateur distant connecté au Serveur d'administration via l'Agent d'administration est un *poste client*.

VERIFICATION MANUELLE DE LA CONNEXION DE L'ORDINATEUR DISTANT AU SERVEUR D'ADMINISTRATION UTILITAIRE KLNAGCHK

Pour vérifier la connexion de l'ordinateur distant avec le Serveur d'administration,

lancez l'utilitaire klnagchk, qui fait partie de la distribution de l'Agent d'administration, via la ligne de commande sur l'ordinateur distant.

Lors de l'installation de l'Agent d'administration, cet utilitaire se trouve dans le dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries. L'utilitaire réalise les opérations suivantes lors du lancement via la ligne de commande en fonction des paramètres utilisés :

- affichage à l'écran ou consignation dans le fichier indiqué des valeurs des paramètres de connexion de l'Agent d'administration installé sur l'ordinateur distant au Serveur d'administration ;
- consignation des statistiques de fonctionnement de l'Agent d'administration dans le fichier indiqué (depuis le dernier lancement de ce composant) et des résultats de l'exécution de l'utilitaire, ou affichage des informations à l'écran ;
- tentative d'établissement de la connexion entre l'Agent d'administration et le Serveur d'administration ;
- en cas d'échec de la connexion, envoi d'un paquet ICMP afin de vérifier l'état de l'ordinateur sur lequel est installé le Serveur d'administration.

Avant de lancer l'utilitaire, accédez au dossier /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Syntaxe de l'utilitaire :

```
sudo ./klnagchk [-logfile <nom du fichier>] [-sp] [-savecert <chemin au fichier de certificat>] [-restart]
```

L'exécution de l'utilitaire requiert les privilèges d'administrateur.

Description des paramètres

-logfile <nom du fichier> : les valeurs des paramètres de connexion de l'Agent d'administration au Serveur d'administration ainsi que les résultats de l'exécution de l'utilitaire sont consignés dans le fichier de rapport indiqué ; si le paramètre n'es pas défini, les paramètres de connexion au serveur, les résultats et les messages d'erreur sont affichés à l'écran.

-sp : affiche à l'écran le mot de passe pour l'authentification de l'utilisateur sur le serveur proxy ou le consigne dans le fichier du rapport ; ce paramètre est utilisé si la connexion au serveur d'administration s'opère via un serveur proxy. Par défaut, il n'est pas utilisé.

-savecert <nom du fichier> : enregistrement du certificat pour l'authentification sur le Serveur d'administration dans le fichier indiqué.

-restart : redémarrage de l'Agent d'administration après l'arrêt de l'utilitaire.

Exemple :

```
sudo ./klnagchk -logfile klnagchk.log -sp
```

INSTALLATION ET SUPPRESSION DE KASPERSKY ENDPOINT SECURITY

Cette section fournit des informations sur les modes d'installation et de désinstallation à distance de Kaspersky Endpoint Security sur le poste client.

Vous pouvez également installer ou supprimer Kaspersky Endpoint Security localement (cf. page 16).

DANS CETTE SECTION

Installation de l'application à l'aide du protocole SSH 93

Installation de l'application via Kaspersky Security Center 94

Suppression de l'application via Kaspersky Security Center 97

INSTALLATION DE L'APPLICATION A L'AIDE DU PROTOCOLE SSH

Avant d'installer Kaspersky Endpoint Security sur l'ordinateur distant, assurez-vous que les conditions suivantes sont remplies :

- Le Serveur d'administration de Kaspersky Security Center est déployé sur le réseau de l'organisation.
- La Console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Security Center.
- Le paquet d'installation pour Kaspersky Endpoint Security a été créé et se trouve dans le dossier partagé du Serveur d'administration.
- Le fichier clé de Kaspersky Endpoint Security se trouve dans le dossier partagé du Serveur d'administration (préférable).

Pour installer Kaspersky Endpoint Security sur un ordinateur distant via le protocole SSH, procédez comme suit :

1. Activez le service **Accès à distance** sur le Mac.
2. Lancez le client SSH sur le poste de travail de l'administrateur.
3. Etablissez la connexion avec le Mac distant.
4. Connectez le dossier partagé du Serveur d'administration en guide de disque réseau sur l'ordinateur distant. Pour se faire, saisissez les commandes suivantes dans le terminal du client SSH :

   ```
   mkdir /Volumes/KLSHARE
   ```

   ```
   mount_smbfs //<compte utilisateur d'administrateur>:<mot de passe>@<adresse IP du serveur d'administration>/KLSHARE /Volumes/KLSHARE
   ```

   Description des paramètres :

   - <compte utilisateur d'administrateur> : nom d'utilisateur de l'administrateur du Serveur d'administration ;
   - <mot de passe> : mot de passe de l'administrateur du Serveur d'administration ;
   - <Adresse IP du serveur d'administration> : adresse IP du serveur sur lequel Kaspersky Security Center est installé.

5. Lancez le script d'installation. Pour se faire, saisissez les commandes suivantes dans le terminal du client SSH :

   ```
   cd /Volumes/KLSHARE/Packages/<kes_package_folder>
   ```

   ```
   sudo ./install.sh
   ```

   où <kes_package_folder> désigne le dossier dans lequel se trouve le paquet d'installation de Kaspersky Endpoint Security.

   L'exécution de cette commande requiert les privilèges d'administrateur.

6. Ejectez le disque réseau de l'ordinateur distant. Saisissez pour ce faire la commande suivante dans le terminal du client SSH :

   ```
   umount /Volumes/KLSHARE
   ```

INSTALLATION DE L'APPLICATION VIA KASPERSKY SECURITY CENTER

Avant d'installer Kaspersky Endpoint Security sur le poste client, assurez-vous que les conditions suivantes sont remplies :

- Le Serveur d'administration de Kaspersky Security Center est déployé sur le réseau de l'organisation.
- La Console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Security Center.
- L'Agent d'administration est installé sur le Mac.
- Le paquet d'installation pour Kaspersky Endpoint Security a été créé et se trouve dans le dossier partagé du Serveur d'administration.
- Le fichier clé de Kaspersky Endpoint Security se trouve dans le dossier partagé du Serveur d'administration (préférable).
- Le Mac a été ajouté au groupe **Ordinateurs gérés** du Serveur d'administration (selon les préférences).

Vous trouverez de plus amples informations sur les groupes du Serveur d'administration dans le *Manuel de l'administrateur de Kaspersky Security Center*.

L'installation de Kaspersky Endpoint Security sur un poste client via Kaspersky Security Center s'opère à l'aide de la création et de l'exécution d'une tâche d'installation à distance de l'application.

Pour créer une tâche d'installation à distance de Kaspersky Endpoint Security sur le poste client via Kaspersky Security Center, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration – <Nom du serveur>**.
3. Choisissez le dossier **Tâches pour des sélections d'ordinateurs**.
4. Dans l'espace de travail, lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les étapes de l'Assistant de création de tâche afin de créer la tâche d'installation à distance de Kaspersky Endpoint Security.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation Windows® que vous utilisez.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 95

Etape 2. Sélection du type de tâche 95

Etape 3. Création du paquet d'installation 95

Etape 4. Installation d'applications complémentaires 96

Etape 5. Configuration des paramètres d'installation 96

Etape 6. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 97

Etape 7. Sélection des postes client 97

Etape 8. Planification du lancement de la tâche 97

Etape 9. Fin de la création de la tâche 97

ETAPE 1. DEFINITION DU NOM DE LA TACHE

1. Saisissez le nom de la tâche créée dans le champ **Nom** de la fenêtre **Définition du nom de la tâche**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 2. SELECTION DU TYPE DE TACHE

1. Dans la fenêtre **Sélection du type de tâche**, développez le nœud **Serveur d'administration Kaspersky Security Center**.
2. Choisissez la tâche **Installation à distance de l'application**.
3. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 3. CREATION DU PAQUET D'INSTALLATION

Si un paquet d'installation aux paramètres voulus a déjà été créé pour Kaspersky Endpoint Security, choisissez-le dans la liste de la partie supérieure de la fenêtre **Sélection du paquet d'installation** et passez à l'étape 13.

Si le paquet d'installation requis n'a pas encore été créé, réalisez les opérations suivantes dans la fenêtre **Sélection du paquet d'installation** :

1. Cliquez sur le bouton **Nouveau**.

   L'Assistant de création de paquet d'installation s'ouvre.

2. Dans la fenêtre **Sélectionnez le type de paquet d'installation**, cliquez sur le bouton **Créer un paquet d'installation pour une application de Kaspersky Lab**.

   La fenêtre **Indiquez le nom du nouveau paquet** s'ouvre.

3. Dans le champ **Nom** de la fenêtre **Indiquez le nom du nouveau paquet**, saisissez le nom du nouveau paquet d'installation, puis cliquez sur **Suivant**.

   La fenêtre **Sélection de la distribution de l'application à installer** s'ouvre.

4. Dans la fenêtre **Sélection de la distribution de l'application à installer**, cliquez sur le bouton **Sélectionner**.

   La fenêtre de sélection du fichier pour la création du paquet d'installation s'ouvre.

5. Ouvrez le dossier contenant la distribution de Kaspersky Endpoint Security et choisissez kesmac.kud.

   La fenêtre **Sélection de la distribution de l'application à installer** affiche le nom et la version de l'application dont l'installation à distance peut être réalisée via le fichier ajouté.

6. Si vous souhaitez copier la mise à jour de l'application depuis le stockage de Kaspersky Security Center dans le paquet d'installation, cochez la case **Copier la mise à jour depuis le stockage dans le paquet d'installation** de la fenêtre **Sélection de la distribution de l'application à installer**.

7. Dans la fenêtre **Sélection de la distribution de l'application à installer**, cliquez sur le bouton **Suivant**.

   La fenêtre **Contrat de licence** s'ouvre.

8. Dans la fenêtre **Contra de licence**, cochez la case **J'accepte les conditions du contrat de licence**, puis appuyez sur le bouton **Suivant**.

   Le téléchargement du paquet sur le Serveur d'administration démarre. La fenêtre **Type d'installation** s'ouvre à la fin du téléchargement.

9. Réalisez les opérations suivantes dans la fenêtre **Type d'installation** :

   - Dans le groupe **Paquets d'installation**, décochez les cases en regard des modules que vous souhaitez ignorer lors de l'installation sur le poste client.

     Si vous décidez de ne pas installer le composant **Interface utilisateur graphique**, l'utilisateur du poste client ne pourra pas activer Kaspersky Endpoint Security et utiliser l'application via l'interface graphique locale, ni configurer les paramètres de fonctionnement et d'utilisation de Kaspersky Security Network via cette même interface.

   - Si vous souhaitez participer à Kaspersky Security Network, cochez, dans le groupe **Paramètres d'utilisation de Kaspersky Security Network**, la case **J'accepte les conditions de participation à Kaspersky Security Network**.

   - Si vous souhaitez lire l'intégralité de la Déclaration de Kaspersky Security Network, cliquez sur **Déclaration de KSN**.

     Sachez qu'à tout moment de votre utilisation de Kaspersky Endpoint Security vous pouvez décider de rejoindre le Kaspersky Security Network ou vous en retirer.

10. Dans la fenêtre **Type d'installation** qui s'ouvre, cliquez sur le bouton **Suivant**.

    Le paquet d'installation pour Kaspersky Endpoint Security avec les paramètres indiqués sera créé.

11. Dans la dernière fenêtre de l'Assistant, cliquez sur le bouton **Terminer** pour quitter l'Assistant de création de paquet d'installation et revenir à l'Assistant de création d'une tâche d'installation à distance de l'application.

12. Sélectionnez le paquet d'installation créé dans la fenêtre **Sélection du paquet d'installation**.

13. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 4. INSTALLATION D'APPLICATIONS COMPLEMENTAIRES

1. Dans la fenêtre **Avancé**, cochez la case **Installer l'Agent d'administration avec cette application** s'il faut installer l'Agent d'administration sur le poste client.

2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 5. CONFIGURATION DES PARAMETRES D'INSTALLATION

1. Dans la fenêtre **Paramètres**, configurez les paramètres de l'installation à distance de l'application.

2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 6. DEFINITION DU MODE DE SELECTION DES POSTES CLIENTS POUR LESQUELS LA TACHE VA ETRE CREEE

Dans la fenêtre **Définition de la méthode de sélection des postes client pour lesquels la tâche va être créée**, sélectionnez la méthode à l'aide de laquelle vous désirez désigner les postes client :

- Si vous souhaitez choisir parmi les ordinateurs détectés sur le réseau par le Serveur d'administration, sélectionnez l'option **Sélectionner les ordinateurs détectés sur le réseau par le Serveur d'administration**.
- Si vous souhaitez indiquer l'adresse IP des ordinateurs manuellement ou importer ces adresses depuis un fichier, choisissez l'option **Définir les adresses des ordinateurs manuellement ou les importer depuis une liste**.
- Si vous souhaitez créer une tâche pour une sélection d'ordinateurs selon un critère prédéfini, choisissez l'option **Ordinateurs de la sélection définie**.

ETAPE 7. SELECTION DES POSTES CLIENT

1. Dans la fenêtre **Sélection des postes client**, sélectionnez les postes clients ou indiquez les adresses IP des ordinateurs sur lesquels vous souhaitez installer l'application.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 8. PLANIFICATION DU LANCEMENT DE LA TACHE

1. Dans la liste déroulante **Lancement planifié** de la fenêtre **Planification du lancement de la tâche**, sélectionnez le mode de lancement.
2. Le cas échéant, configurez les conditions de lancement automatique de la tâche selon une planification (par exemple, la date et l'heure de lancement de la tâche).
3. Si vous souhaitez autoriser l'exécution des tâches que l'application n'a pas pu lancer selon la planification (parce que, par exemple, l'ordinateur était éteint à l'heure planifiée), cochez la case **Lancer les tâches ignorées**.

   Kaspersky Endpoint Security exécutera la tâche dès que l'élément qui empêche son exécution aura été éliminé.
4. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 9. FIN DE LA CREATION DE LA TACHE

1. Si vous souhaitez lancer la tâche une fois que l'Assistant a terminé, cochez la case **Lancer la tâche après la fin de l'Assistant**.
2. Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

   La tâche créée apparaît dans l'espace de travail du dossier **Tâches pour des sélections d'ordinateur**.

SUPPRESSION DE L'APPLICATION VIA KASPERSKY SECURITY CENTER

La suppression de Kaspersky Endpoint Security du poste client expose celui-ci à un grave risque d'infection.

Avant de supprimer Kaspersky Endpoint Security du poste client via Kaspersky Security Center, assurez-vous que les conditions suivantes sont remplies :

- Le Serveur d'administration de Kaspersky Security Center est déployé sur le réseau de l'organisation.
- La Console d'administration est installée sur le poste de travail de l'administrateur de Kaspersky Security Center.
- L'Agent d'administration est installé sur le poste client.

Pour supprimer Kaspersky Endpoint Security du poste client via Kaspersky Security Center, vous devez créer et lancer une tâche de suppression à distance.

Pour créer une tâche de suppression à distance de Kaspersky Endpoint Security du poste client, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration – <Nom du serveur>**.
3. Choisissez le dossier **Tâches pour des sélections d'ordinateurs**.
4. Dans l'espace de travail, lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les étapes de l'Assistant de création de tâche afin de créer une tâche de suppression à distance de Kaspersky Endpoint Security du poste client.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation que vous utilisez.

DANS CETTE SECTION

Etape 1. Définition du nom de la tâche 98
Etape 2. Sélection du type de tâche. Suppression à distance de l'application 99
Etape 3. Sélection de l'application à supprimer 99
Etape 4. Sélection des paramètres de suppression 99
Etape 5. Sélection de l'option de redémarrage du système d'exploitation 99
Etape 6. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 99
Etape 7. Sélection des postes client 99
Etape 8. Sélection du compte utilisateur pour le lancement de la tâche 100
Etape 9. Planification du lancement de la tâche 100
Etape 10. Fin de la création de la tâche 100

ETAPE 1. DEFINITION DU NOM DE LA TACHE

1. Saisissez le nom de la tâche créée dans le champ **Nom** de la fenêtre **Définition du nom de la tâche**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 2. SELECTION DU TYPE DE TACHE. SUPPRESSION A DISTANCE DE L'APPLICATION

1. Dans la fenêtre **Sélection du type de tâche**, développez le nœud **Serveur d'administration Kaspersky Security Center**.
2. Développez le dossier **Avancés**.
3. Choisissez la tâche **Suppression à distance de l'application**.
4. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 3. SELECTION DE L'APPLICATION A SUPPRIMER

Dans la fenêtre **Sélection de l'application à supprimer**, choisissez l'option **Supprimer l'application prise en charge par Kaspersky Security Center**.

ETAPE 4. SELECTION DES PARAMETRES DE SUPPRESSION

1. Dans la liste déroulante **Application à supprimer** de la fenêtre **Paramètre**, choisissez l'option **Kaspersky Endpoint Security 10 for Mac**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 5. SELECTION DE L'OPTION DE REDEMARRAGE DU SYSTEME D'EXPLOITATION

1. Dans la fenêtre **Sélection de l'option de redémarrage du système d'exploitation**, choisissez l'option **Ne pas redémarrer l'ordinateur**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 6. DEFINITION DU MODE DE SELECTION DES POSTES CLIENTS POUR LESQUELS LA TACHE VA ETRE CREEE

Dans la fenêtre **Définition de la méthode de sélection des postes client pour lesquels la tâche va être créée**, sélectionnez la méthode à l'aide de laquelle vous désirez désigner les postes client :

- Si vous souhaitez choisir parmi les ordinateurs détectés sur le réseau par le Serveur d'administration, sélectionnez l'option **Sélectionner les ordinateurs détectés sur le réseau par le Serveur d'administration**.
- Si vous souhaitez indiquer l'adresse IP des ordinateurs manuellement ou importer ces adresses depuis un fichier, choisissez l'option **Définir les adresses des ordinateurs manuellement ou les importer depuis une liste**.

ETAPE 7. SELECTION DES POSTES CLIENT

1. Dans la fenêtre **Sélection des postes client**, désignez les postes client sur lesquels il faut supprimer Kaspersky Endpoint Security.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 8. SELECTION DU COMPTE UTILISATEUR POUR LE LANCEMENT DE LA TACHE

Toutes les tâches de Kaspersky Security Center sur les ordinateurs tournant sous le système d'exploitation OS X sont lancées avec les privilèges de l'utilisateur root. Vous devez ignorer cette étape.

Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 9. PLANIFICATION DU LANCEMENT DE LA TACHE

1. Dans la liste déroulante **Lancement planifié** de la fenêtre **Planification du lancement de la tâche**, sélectionnez le mode de lancement.
2. Le cas échéant, configurez les conditions de lancement de la tâche (par exemple, la date et l'heure de lancement de la tâche).
3. Si vous souhaitez autoriser l'exécution des tâches que l'application n'a pas pu lancer selon la planification (parce que, par exemple, l'ordinateur était éteint à l'heure planifiée), cochez la case **Lancer les tâches ignorées**.

   Kaspersky Endpoint Security exécutera la tâche dès que l'élément qui empêche son exécution aura été éliminé.
4. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 10. FIN DE LA CREATION DE LA TACHE

1. Si vous souhaitez lancer la tâche une fois que l'Assistant a terminé, cochez la case **Lancer la tâche après la fin de l'Assistant**.
2. Dans la fenêtre **Fin de la création de la tâche**, cliquez sur le bouton **Terminer**.

   La tâche créée apparaît dans l'espace de travail du dossier **Tâches pour des sélections d'ordinateur**.

LANCEMENT ET ARRET DE L'APPLICATION

Pour arrêter ou lancer Kaspersky Endpoint Security, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.

   Choisissez l'onglet **Ordinateurs**.
5. Sélectionnez l'ordinateur requis dans la liste des postes client.
6. Ouvrez la fenêtre **Propriétés : <nom de l'ordinateur>** d'une des méthodes suivantes :
   - double-clic sur le nom du poste client ;
   - clic droit pour ouvrir le menu contextuel du poste client et sélection de l'option **Propriétés** ;
   - lien **Propriétés de l'ordinateur** dans le groupe d'administration de l'objet sélectionné.

7. Choisissez la section **Applications**.

8. Dans la liste **Applications de Kaspersky Lab installées sur le poste client**, ouvrez le menu contextuel de l'option **Kaspersky Endpoint Security 10 for Mac** d'un clic droit, puis réalisez une des opérations suivantes :

   - Si vous souhaitez lancer l'application, choisissez l'option **Lancer**.
   - Si vous souhaitez arrêter l'application, choisissez l'option **Arrêter**.

Une fois que Kaspersky Endpoint Security aura été arrêté, le poste client continuera à fonctionner sans protection et il sera exposé au risque d'infection.

ADMINISTRATION DES STRATEGIES

Cette section explique la création et la configuration des stratégies pour Kaspersky Endpoint Security.

Une stratégie détermine des paramètres de fonctionnement de l'application et d'accès à la configuration de l'application installée sur les ordinateurs du groupe d'administration. Il faut créer une stratégie pour chaque application. Vous pouvez créer un nombre infini de stratégies différentes pour les applications installées sur les ordinateurs de chaque groupe d'administration. Toutefois, au sein de chacun de ces groupes, une seule stratégie peut être appliquée simultanément à chaque programme.

Lors de la création et de la configuration d'une stratégie, vous pouvez interdire ou autoriser la modification de chaque groupe de paramètres dans les stratégies des sous-groupes à l'aide des boutons  et  .

Les stratégies peuvent être soumises aux opérations suivantes :

- création d'une stratégie ;
- configuration des paramètres d'une stratégie ;
- copie et transfert d'une stratégie d'un groupe vers un autre et suppression d'une stratégie à l'aide du menu contextuel ;
- modification de l'état d'une stratégie ;
- importation d'une stratégie depuis un fichier ;
- exportation d'une stratégie dans un fichier.

Vous trouverez de plus amples informations sur les stratégies de Kaspersky Security Center dans le *Manuel de l'administrateur de Kaspersky Security Center*.

DANS CETTE SECTION

Création d'une stratégie 102

Configuration des paramètres d'une stratégie 106

Modification de l'état d'une stratégie 108

Importation d'une stratégie depuis un fichier 109

Ouverture de la liste des stratégies 109

Exportation d'une stratégie dans un fichier 109

CREATION D'UNE STRATEGIE

Cette section explique et décrit les étapes de l'Assistant de création d'une stratégie.

Pour créer une stratégie, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
6. Dans l'espace de travail, lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une stratégie**.
7. Suivez les étapes de l'Assistant de création d'une stratégie afin de créer une stratégie.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation que vous utilisez.

DANS CETTE SECTION

Etape 1. Saisie des données générales sur la stratégie 103

Etape 2. Sélection de l'application 103

Etape 3. Configuration de la protection 103

Etape 4. Configuration des paramètres de l'Anti-Virus Fichiers 103

Etape 5. Configuration des paramètres de l'Anti-Virus Internet 104

Etape 6. Configuration de la protection contre les attaques réseau 104

Etape 7. Configuration de la mise à jour 104

Etape 8. Configuration des paramètres d'utilisation de KSN 104

Etape 9. Configuration de l'interaction avec l'utilisateur 105

Etape 10. Configuration de l'interaction avec le réseau 105

Etape 11. Configuration des paramètres des rapports, de la quarantaine et de la sauvegarde 105

Etape 12. Sélection de l'état de la stratégie 105

Etape 13. Fin de la création de la stratégie 105

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA STRATEGIE

1. Renseignez le nom de la stratégie créée dans le champ **Nom** de la fenêtre **Définition du nom de la stratégie de groupe pour l'application**. Le nom ne peut pas contenir les caractères " * < : > ? \ / .
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 2. SELECTION DE L'APPLICATION

1. Sélectionnez **Kaspersky Endpoint Security 10 for Mac** dans la liste **Nom de l'application** de la fenêtre **Sélection de l'application pour la création d'une stratégie de groupe**.
2. Cochez la case **Utiliser les paramètres d'une stratégie existante pour la version antérieure de l'application** si vous souhaitez importer les paramètres d'une stratégie existante pour Endpoint Security 8.0 dans la nouvelle stratégie.
3. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 3. CONFIGURATION DE LA PROTECTION

1. Le cas échéant, réalisez les opérations suivantes dans la fenêtre **Protection** :
   - Configurez les paramètres de la protection du système d'exploitation du poste client.
   - Configurez la zone de confiance.
   - Sélectionnez les catégories des objets à détecter.
   - Configurez le mode de lancement des tâches lorsque l'ordinateur est alimenté par une batterie.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

VOIR EGALEMENT

Consultation et modification des paramètres de la tâche de l'Anti-Virus Fichiers 126

ETAPE 4. CONFIGURATION DES PARAMETRES DE L'ANTI-VIRUS FICHIERS

1. Le cas échéant, réalisez les opérations suivantes dans la fenêtre **Anti-Virus Fichiers** :
   - Activez ou désactivez l'Anti-Virus Fichiers.

     Par défaut, l'Anti-Virus Fichiers est activé.
   - Sélectionnez le niveau de sécurité.

     Le niveau de sécurité utilisé par défaut est le niveau recommandé par les experts de Kaspersky Lab.
   - Sélectionnez l'action à réaliser en cas de détection d'un objet malveillant.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 5. CONFIGURATION DES PARAMETRES DE L'ANTI-VIRUS INTERNET

1. Le cas échéant, réalisez les opérations suivantes dans la fenêtre **Anti-Virus Internet** :
   - Activez ou désactivez l'Anti-Virus Internet.

     L'Anti-Virus Internet est activé par défaut.
   - Sélectionnez le niveau de sécurité.

     Le niveau de sécurité utilisé par défaut est le niveau recommandé par les experts de Kaspersky Lab.
   - Sélectionnez l'action à réaliser en cas de détection d'un objet malveillant dans le trafic Internet.
   - Activez ou désactivez l'analyse des données reçues sur l'ordinateur ou transmises depuis celui-ci via le protocole HTTPS.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 6. CONFIGURATION DE LA PROTECTION CONTRE LES ATTAQUES RESEAU

1. Le cas échéant, réalisez les opérations suivantes dans la fenêtre **Protection contre les attaques réseau** :
   - Activez ou désactivez la protection contre les attaques réseau.

     La protection contre les attaques de réseau est activée par défaut.
   - Configurez les paramètres de la protection contre les attaques réseau.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 7. CONFIGURATION DE LA MISE A JOUR

1. Le cas échéant, configurez les paramètres selon lesquels vous souhaitez exécuter les tâches de mise à jour de l'application dans la fenêtre **Mise à jour**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

VOIR EGALEMENT

Consultation et modification des paramètres de la tâche de mise à jour.....124

ETAPE 8. CONFIGURATION DES PARAMETRES D'UTILISATION DE KSN

1. Le cas échéant, configurez les paramètres d'utilisation de Kaspersky Security Network et les paramètres du proxy KSN Dans la fenêtre **KSN**.

   La participation au Kaspersky Security Network signifie que les statistiques obtenues pendant l'utilisation de Kaspersky Endpoint Security sur votre ordinateur sont envoyées automatiquement à Kaspersky Lab.

   Aucune donnée personnelle n'est collectée, traitée et conservée.
2. Si vous souhaitez lire l'intégralité de la Déclaration de KSN, cliquez sur **Déclaration de Kaspersky Security Network**.
3. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

VOIR EGALEMENT

Etape 9. Configuration de l'interaction avec l'utilisateur 105

ETAPE 9. CONFIGURATION DE L'INTERACTION AVEC L'UTILISATEUR

1. Le cas échéant, configurez l'interaction entre Kaspersky Endpoint Security 10 for Mac et l'utilisateur du poste client dans la fenêtre **Interaction avec l'utilisateur**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 10. CONFIGURATION DE L'INTERACTION AVEC LE RESEAU

1. Le cas échéant, configurez les paramètres de la connexion au serveur proxy dans la fenêtre **Réseau**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 11. CONFIGURATION DES PARAMETRES DES RAPPORTS, DE LA QUARANTAINE ET DE LA SAUVEGARDE

1. Le cas échéant, réalisez les opérations suivantes dans la fenêtre **Rapports** :
   - Configurez les paramètres de constitution et de conservation des rapports.
   - Configurez la durée de conservation des fichiers en quarantaine et dans la sauvegarde.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 12. SELECTION DE L'ETAT DE LA STRATEGIE

1. Dans la fenêtre **Création d'une stratégie de groupe pour l'application**, sélectionnez l'état qui sera attribué à la stratégie après sa création. Vous pouvez attribuer un des états suivants à une stratégie :
   - *stratégie active* : la stratégie est appliquée au groupe d'administration sélectionné ;
   - *stratégie inactive* : la stratégie n'est pas appliquée ;
   - *stratégie pour utilisateurs autonomes* : la stratégie est appliquée au groupe d'administration sélectionné lorsqu'il n'est plus connecté au réseau de l'organisation.

   Plusieurs stratégies peuvent être créées dans un groupe d'administration pour une application mais il ne peut y avoir qu'une seule politique active.

   Vous trouverez de plus amples informations sur les états des stratégies dans le *Manuel de l'administrateur de Kaspersky Security Center*.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant de création d'une stratégie.

ETAPE 13. FIN DE LA CREATION DE LA STRATEGIE

La dernière fenêtre de l'Assistant vous informe sur la réussite de la création de la stratégie. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

La stratégie créée apparaît sous l'onglet **Stratégies** de l'espace de travail du groupe d'administration correspondant.

Vous pouvez modifier les paramètres de la stratégie créée. Vous pouvez également interdire ou autoriser la modification de chaque groupe de paramètres au départ du poste client à l'aide des boutons et . Le bouton en regard d'un groupe de paramètres signifie que l'utilisateur du poste client ne peut pas modifier ces paramètres sur son ordinateur. Le bouton en regard d'un groupe de paramètres signifie que l'utilisateur du poste client peut modifier ces paramètres sur son ordinateur.

La stratégie est appliquée aux postes clients après la première synchronisation des postes client avec le Serveur d'administration.

CONFIGURATION DES PARAMETRES D'UNE STRATEGIE

Vous pouvez modifier une stratégie créée dans Kaspersky Security Center, ainsi qu'interdire la modification de ses paramètres dans les stratégies des sous-groupes et dans les paramètres des tâches. Les paramètres de la stratégie peuvent être modifiés sous l'onglet **Configuration**.

Les paramètres de stratégie pour Kaspersky Endpoint Security incluent les paramètres de l'application et les paramètres des tâches (cf. section "Consultation des paramètres d'une tâche" à la page 117).

Pour consulter et configurer les paramètres d'une stratégie, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
6. D'un clic droit, ouvrez le menu contextuel de la stratégie contenant les paramètres que vous souhaitez configurer puis, sélectionnez **Propriétés**.
7. Configurez les paramètres requis de la stratégie dans la fenêtre **Propriétés : <nom de la stratégie>** :
   - Le cas échéant, configurez les paramètres de protection suivant dans la section **Protection** :
     - Activez ou désactivez la protection en temps réel du poste client.
     - Activez ou désactivez Kaspersky Endpoint Security au démarrage du poste client.
     - Configurez les paramètres de la zone de confiance.
     - Sélectionnez les catégories des objets à détecter.
     - Activez ou désactivez le lancement automatique des tâches programmées quand l'ordinateur est alimenté par la batterie.
   - Le cas échéant, configurez les paramètres suivants dans la section **Anti-Virus Fichiers** :
     - Activez ou désactivez l'Anti-Virus Fichiers.
     - Sélectionnez un des niveaux de sécurité prédéfinis ou configurez manuellement les paramètres de sécurité.
     - Sélectionnez les types de fichiers que l'Anti-Virus Fichiers analyse.
     - Configurez les performances de l'analyse antivirus.

- Sélectionnez les types de fichiers composés que l'Anti-Virus Fichiers analyse.
- Définissez la zone de protection.
- Sélectionnez le mode d'analyse antivirus.
- Activez ou désactivez la suspension de la tâche programmée.
- Activez ou désactivez l'analyse heuristique.
- Sélectionnez l'action que l'Anti-Virus Fichiers exécute en cas de détection d'un fichier infecté.

- Le cas échéant, configurez les paramètres suivants dans la section **Anti-Virus Internet** :
  - Activez ou désactivez l'Anti-Virus Internet.
  - Sélectionnez un des niveaux de sécurité prédéfinis ou configurez manuellement les paramètres de sécurité.
  - Activez ou désactivez l'analyse des adresses Internet selon la base des adresses Internet malveillantes.
  - Configurez les paramètres de l'anti-phishing.
  - Composez la liste des adresses de confiance dont le trafic ne sera pas analysé par l'Anti-Virus Internet.
  - Choisissez l'action que l'application exécutera en cas de détection d'un objet malveillant.
  - Activez ou désactivez l'analyse des données reçues sur l'ordinateur ou transmises depuis celui-ci via le protocole HTTPS.
- Dans la section **Protection contre les attaques réseaux**, configurez les paramètres suivants, le cas échéant :
  - Activez ou désactivez la protection contre les attaques réseau.
  - Configurez les paramètres de la protection contre les attaques réseau.
  - Indiquez les adresses IP des ordinateurs dont l'activité réseau ne sera pas bloquée.
- Le cas échéant, configurez les paramètres suivants dans la section **Mise à jour** :
  - Activez ou désactivez la mise à jour des modules de l'application.
  - Activez ou désactivez la copie des fichiers de mise à jour dans le dossier.
  - Indiquez le dossier dans lequel Kaspersky Endpoint Security va copier les fichiers de la mise à jour.
  - Désignez les sources des mises à jour.
  - Sélectionnez l'action à réaliser après la mise à jour des bases.
- Le cas échéant, configurez les paramètres suivants dans la section **KSN** :
  - Activez ou désactivez l'utilisation de KSN.
  - Activez ou désactivez l'utilisation de KSN pour analyser et classer les fichiers.
  - Activez ou désactivez l'utilisation de KSN pour analyser les adresses Internet.
  - Configurez les paramètres d'utilisation du proxy KSN.

- Le cas échéant, configurez les paramètres suivants dans la section **Interaction avec l'utilisateur** :
  - Activez ou désactivez les notifications sur les événements.
  - Sélectionnez la méthode utilisée par Kaspersky Endpoint Security pour prévenir les utilisateurs sur les événements survenus.
  - Activez ou désactivez l'affichage de l'icône de Kaspersky Endpoint Security dans la barre de menus.
  - Activez ou désactivez l'affichage de l'option **Quitter** dans le menu contextuel de l'icône de Kaspersky Endpoint Security sur le poste client.
  - Choisissez la langue d'affichage des événements dans Kaspersky Security Center.
  - Définissez des restrictions sur les possibilités d'administration de Kaspersky Endpoint Security pour l'utilisateur du poste client.
- Le cas échéant, configurez les paramètres suivants dans la section **Réseau** :
  - Sélectionnez le mode d'utilisation du serveur proxy.
  - Indiquez l'adresse du serveur proxy.
  - Activez ou désactivez l'adresse du serveur proxy pour les adresses locales.
  - Indiquez le nom d'utilisateur et le mot de passe pour l'authentification sur le serveur proxy.
- Le cas échéant, configurez les paramètres suivants dans la section **Rapports** :
  - Activez ou désactivez la consignation des événements non critiques dans le rapport.
  - Activez ou désactivez la suppression des événements à l'issue de la période définie.
  - Définissez la durée de conservation des événements.
  - Activez ou désactivez la suppression des objets en quarantaine et dans la sauvegarde à l'issue de la période définie.
  - Définissez la durée de conservation des fichiers en quarantaine et dans la sauvegarde.

8. Cliquez sur **OK** pour enregistrer les modifications introduites et fermer la fenêtre des propriétés de la stratégie.

MODIFICATION DE L'ETAT D'UNE STRATEGIE

Vous pouvez modifier l'état d'une stratégie existante.

Pour modifier l'état d'une stratégie, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
6. D'un clic droit, ouvrez le menu contextuel de la stratégie contenant les paramètres que vous souhaitez modifier puis, sélectionnez **Propriétés**.

7. Dans la fenêtre **Propriétés : <nom de la stratégie>** qui s'ouvre, choisissez le groupe **Général**.
8. Dans le groupe **Etat de la stratégie**, sélectionnez une des valeurs possibles :
   - **Stratégie active**. La stratégie s'applique au groupe d'administration sélectionné.
   - **Stratégie pour les utilisateurs nomades**. La stratégie est appliquée au groupe d'administration sélectionné lorsqu'il n'est plus connecté au réseau de l'organisation.
   - **Stratégie inactive**. La stratégie n'est pas appliquée.
9. Cliquez sur le bouton **OK** pour enregistrer les modifications et fermer la fenêtre **Propriétés :<nom de la stratégie>**.

IMPORTATION D'UNE STRATEGIE DEPUIS UN FICHIER

Vous pouvez importer une stratégie existante depuis un fichier au format KLP.

Pour importer une stratégie depuis un fichier, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
6. Ouvrez la fenêtre de sélection de fichiers d'une des méthodes suivantes :
   - Cliquez sur le lien **Importer la stratégie depuis un fichier**.
   - Cliquez-droit pour ouvrir le menu contextuel de l'espace de travail et choisissez l'option **Importer**.
7. Sélectionnez le fichier contenant la stratégie.

La stratégie importée apparaît dans la liste des stratégies de l'espace de travail.

OUVERTURE DE LA LISTE DES STRATEGIES

Pour ouvrir la liste des stratégies créées pour Kaspersky Endpoint Security, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.

EXPORTATION D'UNE STRATEGIE DANS UN FICHIER

Vous pouvez exporter une stratégie existante pour Kaspersky Endpoint Security dans un fichier au format KPL.

Pour exporter une stratégie existante, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, ouvrez l'onglet **Stratégies**.
6. Cliquez-droit pour ouvrir le menu contextuel de la stratégie et choisissez l'option **Exporter**.

   La fenêtre d'enregistrement du fichier s'ouvre.
7. Indiquez le nom du fichier.
8. Enregistrez le fichier dans le dossier sélectionné.

ADMINISTRATION DES TACHES

Cette section explique comment créer et configurer des tâches pour Kaspersky Endpoint Security sur le poste client ou sur un groupe de postes client.

Une *tâche* est un ensemble d'actions exécutées par Kaspersky Endpoint Security sur le poste client selon des paramètres définis. Vous pouvez lancer une tâche manuellement ou la planifier.

Lors de l'installation sur le poste client, Kaspersky Endpoint Security crée un ensemble de tâches prédéfinies. Il s'agit de tâches de protection, d'analyse contre les virus, de mise à jour et d'annulation de la mise à jour.

Vous pouvez administrer le lancement des tâches système et en configurer les paramètres. Il est toutefois impossible de les supprimer.

Vous pouvez créer également des tâches selon vos propres paramètres, par exemple, une tâche d'analyse contre les virus, une tâche de mise à jour de l'application, une tâche d'ajout du fichier clé.

Vous pouvez réaliser les opérations suivantes sur les tâches personnalisées :

- configuration des paramètres de la tâche ;
- suivi de l'exécution de la tâche ;
- copie et transfert d'une tâche d'un groupe vers un autre ;
- suppression d'une tâche ;
- importation et exportation d'une tâche.

Vous trouverez de plus amples informations sur les tâches dans le *Manuel de l'administrateur de Kaspersky Security Center*.

DANS CETTE SECTION

Création d'une tâche 111

Lancement et arrêt manuels des tâches 117

Consultation des paramètres d'une tâche 117

Consultation de la liste des tâches pour les ordinateurs qui appartiennent au groupe d'administration 118

Consultation de la liste des tâches pour les ordinateurs en dehors du groupe d'administration 118

Consultation de la liste des tâches locales 119

Consultation et modification des paramètres de la tâche d'Analyse rapide 119

Consultation et modification des paramètres de la tâche d'Analyse complète 120

Consultation et modification des paramètres de la tâche de l'Anti-Virus Internet 121

Consultation et modification des paramètres de la tâche d'ajout d'une clé 122

Consultation et modification des paramètres de la tâche de protection contre les attaques réseau 123

Consultation et modification des paramètres de la tâche de mise à jour 124

Consultation et modification des paramètres de la tâche d'analyse définie par l'utilisateur 125

Consultation et modification des paramètres de la tâche de l'Anti-Virus Fichiers 126

CREATION D'UNE TACHE

Cette section explique et décrit les étapes de l'Assistant de création d'une tâche.

Dans le cadre de l'utilisation de Kaspersky Endpoint Security via Kaspersky Security Center, vous pouvez créer les types de tâche suivants :

- des tâches locales pour un poste client distinct ;
- des tâches des postes client du groupe d'administration ;
- des tâches pour des sélections de postes client en dehors du groupe d'administration.

DANS CETTE SECTION

Création d'une tâche locale pour un poste client distinct 112

Création d'une tâche pour des postes client du groupe d'administration 113

Création d'une tâche pour des postes client en dehors du groupe d'administration 113

Etape 1. Saisie des données générales sur la tâche 114

Etape 2. Sélection de l'application et du type de tâche 114

Etape 3. Configuration des paramètres du type de tâche sélectionné 114

Etape 4. Définition du mode de sélection des postes clients pour lesquels la tâche va être créée 116

Etape 5. Sélection des postes client 116

Etape 6. Paramètres de planification 116

Etape 7. Fin de la création de la tâche 117

CREATION D'UNE TACHE LOCALE POUR UN POSTE CLIENT DISTINCT

Afin de créer une tâche locale pour un ordinateur client particulier, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, sélectionnez l'onglet **Ordinateurs**.
6. Sélectionnez l'ordinateur requis dans la liste des postes client.
7. Ouvrez la fenêtre **Propriétés : <nom de l'ordinateur>** d'une des méthodes suivantes :
   - double-clic sur le nom du poste client ;
   - clic droit pour ouvrir le menu contextuel du poste client et sélection de l'option **Propriétés** ;
   - lien **Propriétés de l'ordinateur** dans le groupe d'administration de l'objet sélectionné.
8. Dans la fenêtre **Propriétés: <nom de l'ordinateur>** qui s'ouvre, sélectionnez la section **Tâches**.

   La liste des tâches prédéfinies et des tâches définies par l'utilisateur pour ce poste client apparaît dans l'espace de travail à droite.
9. Dans la partie inférieure de l'espace de travail, cliquez sur le bouton **Ajouter**.

   L'Assistant de création de tâche démarre.
10. Suivez les étapes de l'Assistant de création de tâche afin de créer une tâche locale pour un poste client distinct.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation que vous utilisez.

VOIR EGALEMENT

Création d'une tâche pour des postes client du groupe d'administration 113

Création d'une tâche pour des postes client en dehors du groupe d'administration 113

CREATION D'UNE TACHE POUR DES POSTES CLIENT DU GROUPE D'ADMINISTRATION

Pour consulter créer une tâche pour des postes client appartenant à un groupe d'administration, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, sélectionnez l'onglet **Tâches**.
6. Dans l'espace de travail, lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche**.
7. Suivez les étapes de l'Assistant de création d'une tâche afin de créer une tâche pour les postes client du groupe d'administration.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation que vous utilisez.

Vous trouverez de plus amples informations sur les particularité de la création de tâches de groupe dans le *Manuel de l'administrateur de Kaspersky Security Center*.

VOIR EGALEMENT

Création d'une tâche locale pour un poste client distinct.....112

Création d'une tâche pour des postes client en dehors du groupe d'administration.....113

CREATION D'UNE TACHE POUR DES POSTES CLIENT EN DEHORS DU GROUPE D'ADMINISTRATION

Pour créer une tâche pour des sélections de postes client en dehors du groupe d'administration, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Choisissez le dossier **Tâches pour des sélections d'ordinateurs**.
4. Dans l'espace de travail, lancez l'Assistant de création de tâche en cliquant sur le lien **Créer une tâche**.
5. Suivez les étapes de l'Assistant de création d'une tâche afin de créer une tâche pour les postes client en dehors du groupe d'administration.

Pour passer à l'étape suivante de l'Assistant, cliquez sur **Suivant**. Pour revenir à l'étape antérieure de l'Assistant, cliquez sur  . Pour interrompre le fonctionnement de l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

L'aspect du bouton peut varier en fonction de la version du système d'exploitation que vous utilisez.

Pour obtenir de plus amples informations sur les particularités de la création de tâches pour des sélections de postes client en dehors du groupe d'administration dans le *Manuel de l'administrateur de Kaspersky Security Center*.

VOIR EGALEMENT

Création d'une tâche locale pour un poste client distinct.....112

Création d'une tâche pour des postes client du groupe d'administration.....113

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA TACHE

1. Saisissez le nom de la tâche créée dans le champ **Nom** de la fenêtre **Définition du nom de la tâche**.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 2. SELECTION DE L'APPLICATION ET DU TYPE DE TACHE

1. Dans la fenêtre **Sélection du type de tâche**, développez le nœud **Kaspersky Endpoint Security 10 for Mac**.
2. Sélectionnez le type de tâche à créer :
   - Si vous souhaitez créer une tâche d'ajout de clé, choisissez **Ajouter une clé**.
   - Si vous souhaitez créer une tâche de mise à jour, choisissez **Mise à jour**.
   - Si vous souhaitez créer une tâche d'annulation de la mise à jour, choisissez **Retour à l'état antérieur**.
   - Si vous souhaitez créer une tâche d'analyse contre les virus, choisissez **Analyse contre les virus**.
3. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 3. CONFIGURATION DES PARAMETRES DU TYPE DE TACHE SELECTIONNE

Le contenu de la fenêtre de configuration de la tâche varie en fonction du type de tâche choisi à l'étape antérieure. Cette fenêtre n'apparaît pas pour la tâche de retour à l'état antérieur à la mise à jour.

Activation de l'application

Réalisez les opérations suivantes dans la fenêtre **Activation de l'application** :

1. Sélectionnez le code d'activation ou ajouter un fichier clé.
2. Si vous souhaitez ajouter la clé désignée en tant que clé de réserve, cochez la case **Ajouter en tant qu'une clé de réserve**.

   La clé de licence de réserve deviendra la clé active à l'échéance de la validité de la clé active actuelle.

Les informations relatives à la clé indiquée (clé, type et date de fin de validité) s'affichent dans la fenêtre **Activation de l'application**.

Mise à jour

Par défaut, Kaspersky Endpoint Security met à jour les bases et les modules de l'application et utilise en guise de sources des mises à jour le Serveur d'administration Kaspersky Endpoint Security et les serveurs de mise à jour de Kaspersky Lab.

Le cas échéant, modifiez les paramètres de la tâche de mise à jour dans la fenêtre **Mise à jour** :

1. Si vous souhaitez désactiver la mise à jour des modules de l'application, décochez la case **Mettre à jour les modules de l'application**.
2. Si vous souhaitez que Kaspersky Endpoint Security copie les fichiers de mise à jour récupérés dans le dossier que vous indiquerez, cochez la case **Copier les fichiers de mise à jour dans un dossier** et indiquez le chemin d'accès au dossier.
3. Si vous souhaitez modifier les sources de la mise à jour, procédez comme suit :
   a. Cliquez sur le bouton **Paramètres**.

      La fenêtre **Paramètres : Mise à jour** s'ouvre.

   b. Cochez les cases en regard du nom des sources des mises à jour que vous souhaitez utiliser.

   c. Si vous souhaitez désigner une autre source de mises à jour, cliquez sur le bouton **Ajouter**.

      La fenêtre **Sources des mises à jour** s'ouvre.

   d. Indiquez l'adresse Internet de la source des mises à jour ou le chemin d'accès au dossier local ou de réseau qui remplit la fonction de source des mises à jour.

   e. Cliquez sur **OK** pour enregistrer les modifications introduites et fermer la fenêtre **Paramètres : Mise à jour**.

Analyse

Kaspersky Endpoint Security utilise par défaut le niveau de sécurité **Recommandé**, confirme l'action à réaliser sur un objet infecté ou potentiellement infecté à l'issue de l'analyse et analyse les objets suivants :

- Tous les disques amovibles ;
- Tous les disques durs ;
- Tous les disques réseau.

Le cas échéant, vous pouvez modifier les paramètres de l'analyse dans la fenêtre **Analyse contre les virus** :

1. Sélectionnez un des niveaux de sécurité prédéfinis ou configurez manuellement les paramètres du niveau de sécurité.
2. Indiquez l'action que Kaspersky Endpoint Security exécutera en cas de détection d'un objet infecté ou potentiellement infecté.

   Dans les tâches pour les postes client appartenant au groupe d'administration et dans les tâches pour les sélections de postes client en dehors des groupes d'administration, les options **Confirmer à la fin de l'analyse** et **Confirmer pendant l'analyse** ne sont pas disponibles.

3. Délimitez la portée de l'analyse.

Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 4. DEFINITION DU MODE DE SELECTION DES POSTES CLIENTS POUR LESQUELS LA TACHE VA ETRE CREEE

Si vous créez une tâche pour un poste client particulier ou pour des clients d'un groupe d'administration, cette étape n'apparaît pas.

Dans la fenêtre **Définition de la méthode de sélection des postes client pour lesquels la tâche va être créée**, sélectionnez la méthode à l'aide de laquelle vous désirez désigner les postes client :

- Si vous souhaitez choisir parmi les ordinateurs détectés sur le réseau par le Serveur d'administration, sélectionnez l'option **Sélectionner les ordinateurs détectés sur le réseau par le Serveur d'administration**.
- Si vous souhaitez indiquer l'adresse IP des ordinateurs manuellement ou importer ces adresses depuis un fichier, choisissez l'option **Définir les adresses des ordinateurs manuellement ou les importer depuis une liste**.

ETAPE 5. SELECTION DES POSTES CLIENT

Si vous créez une tâche pour un poste client particulier ou pour des clients d'un groupe d'administration, cette étape n'apparaît pas.

1. Dans la fenêtre **Sélection des postes client**, sélectionnez les postes clients ou indiquez les adresses IP des ordinateurs auxquels vous souhaitez appliquer la tâche.
2. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 6. PARAMETRES DE PLANIFICATION

1. Dans la liste déroulante **Lancement planifié** de la fenêtre **Planification du lancement de la tâche**, sélectionnez le mode de lancement de la tâche.
2. Le cas échéant, configurez les conditions de lancement de la tâche (par exemple, la date et l'heure de lancement de la tâche).
3. Si vous souhaitez autoriser l'exécution des tâches que l'application n'a pas pu lancer selon la planification (par exemple, l'ordinateur était éteint à l'heure planifiée), cochez la case **Lancer les tâches ignorées**.

   Kaspersky Endpoint Security exécutera la tâche dès que l'élément qui empêche son exécution aura été éliminé.
4. Si vous souhaitez que l'application Kaspersky Security Center définisse automatiquement l'intervalle entre les lancements d'une tâche sur différents ordinateurs, cochez la case **Déterminer automatiquement l'intervalle pour la distribution du lancement de la tâche**.

   Cette fonction permet de réduire la charge sur le Serveur d'administration Kaspersky Security Center.
5. Si vous souhaitez indiquer manuellement l'intervalle entre les lancements d'une tâche sur différents ordinateurs, cochez la case **Répartir le lance de la tâche de manière aléatoire dans l'intervalle (min)** et indiquez le nombre de minutes.

   Cette fonction permet de réduire la charge sur le Serveur d'administration Kaspersky Security Center.
6. Cliquez sur le bouton **Suivant** pour passer à l'étape suivante de l'Assistant.

ETAPE 7. FIN DE LA CREATION DE LA TACHE

Exécutez les actions suivantes dans la fenêtre **Fin de la création de la tâche** :

1. Si vous souhaitez lancer la tâche une fois que l'Assistant a terminé, cochez la case **Lancer la tâche après la fin de l'Assistant**.

2. Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

LANCEMENT ET ARRET MANUELS DES TACHES

Le lancement d'une tâche sur le poste client est possible uniquement si l'Agent d'administration est lancé. En cas d'arrêt de l'Agent d'administration, l'exécution de toutes les tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide des commandes du menu contextuel) ou depuis la fenêtre des propriétés de la tâche.

Pour lancer ou arrêter une tâche manuellement, procédez comme suit :

1. Ouvrez la liste dans laquelle se trouve la tâche :

   - Si vous souhaitez lancer ou arrêter une tâche locale, ouvrez la liste des tâches locales (cf. section "Consultation de la liste des tâches locales" à la page 119).

   - Si vous souhaitez lancer ou arrêter une tâche pour des ordinateurs d'un groupe d'administration, ouvrez la liste des tâches pour les ordinateurs du groupe d'administration (cf. section "Consultation de la liste des tâches pour les ordinateurs qui appartiennent au groupe d'administration" à la page 118).

   - Si vous souhaitez lancer ou arrêter une tâche pour des ordinateurs en dehors d'un groupe d'administration, ouvrez la liste des tâches pour les ordinateurs en dehors du groupe d'administration (cf. section "Consultation de la liste des tâches pour les ordinateurs en dehors au groupe d'administration" à la page 118).

2. Sélectionnez la tâche que vous souhaitez lancer ou arrêter.

3. Lancez ou arrêtez la tâche d'une des manières suivantes :

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche, puis sélectionnez l'option **Lancer** ou **Arrêter**.

   - Dans l'espace de travail, cliquez sur le bouton **Lancer** ou **Arrêter**.

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Lancer** ou **Arrêter**.

CONSULTATION DES PARAMETRES D'UNE TACHE

Pour consulter les paramètres d'une tâche locale, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client distinct (cf. section "Consultation de la liste des tâches locales" à la page 119).

2. Sélectionnez la tâche dans la liste et ouvrez les propriétés de la tâche d'une des manières suivantes :

   - Cliquez deux fois sur le nom de la tâche.

   - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.

   - Cliquez sur le bouton **Propriétés**.

- *Pour consulter les paramètres d'une tâche pour les postes client appartenant au groupe d'administration, procédez comme suit :*

  1. Ouvrez la liste des tâches pour les ordinateurs du groupe d'administration (cf. section "Consultation de la liste des tâches pour les ordinateurs qui appartiennent au groupe d'administration" à la page 118).
  2. Sélectionnez la tâche et ouvrez les propriétés de la tâche d'une des manières suivantes :
     - Cliquez deux fois sur le nom de la tâche.
     - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.
     - Cliquez sur le lien **Modifier les paramètres** dans l'espace de travail.

- *Pour consulter les paramètres d'une tâche pour des sélections de postes client en dehors du groupe d'administration, procédez comme suit :*

  1. Ouvrez la liste des tâches pour les sélections de postes client en dehors des groupes d'administration (cf. section "Consultation de la liste des tâches pour les sélections d'ordinateurs en dehors du groupe d'administration" à la page 118).
  2. Sélectionnez la tâche et ouvrez les propriétés de la tâche d'une des manières suivantes :
     - Cliquez deux fois sur le nom de la tâche.
     - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.
     - Cliquez sur le lien **Modifier les paramètres** dans l'espace de travail.

  Pour obtenir de plus amples informations sur les particularités de la création de tâches pour des sélections postes client dans le *Manuel de l'administrateur de Kaspersky Security Center*.

CONSULTATION DE LA LISTE DES TACHES POUR LES ORDINATEURS QUI APPARTIENNENT AU GROUPE D'ADMINISTRATION

- *Pour consulter la liste des tâches pour les postes client appartenant au groupe d'administration, procédez comme suit :*

  1. Lancez la Console d'administration Kaspersky Security Center.
  2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
  3. Développez le dossier **Ordinateurs gérés**.
  4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
  5. Dans la zone de travail, sélectionnez l'onglet **Tâches**.

  La liste des tâches pour les ordinateurs du groupe d'administration apparaît dans l'espace de travail.

CONSULTATION DE LA LISTE DES TACHES POUR LES ORDINATEURS EN DEHORS DU GROUPE D'ADMINISTRATION

- *Pour consulter la liste des tâches pour des sélections de postes client en dehors du groupe d'administration, procédez comme suit :*

  1. Lancez la Console d'administration Kaspersky Security Center.
  2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
  3. Choisissez le dossier **Tâches pour des sélections d'ordinateurs**.

  La liste des tâches pour les sélections de postes client en dehors du groupe d'administration apparaît dans l'espace de travail.

CONSULTATION DE LA LISTE DES TACHES LOCALES

Pour consulter la liste des tâches locales créées pour un poste client, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Dans la zone de travail, sélectionnez l'onglet **Ordinateurs**.
6. Sélectionnez l'ordinateur requis dans la liste des postes client.
7. Ouvrez la fenêtre **Propriétés : <nom de l'ordinateur>** d'une des méthodes suivantes :
   - double-clic sur le nom du poste client ;
   - clic droit pour ouvrir le menu contextuel du poste client et sélection de l'option **Propriétés** ;
   - lien **Propriétés de l'ordinateur** dans le groupe d'administration de l'objet sélectionné.
8. Dans la fenêtre **Propriétés: <nom de l'ordinateur>** qui s'ouvre, sélectionnez la section **Tâches**.

   La liste des tâches prédéfinies et des tâches définies par l'utilisateur pour ce poste client apparaît dans l'espace de travail à droite.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE D'ANALYSE RAPIDE

Pour consulter et modifier les paramètres de la tâche d'analyse rapide, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client (cf. section "Consultation de la liste des tâches locales" à la page 119).
2. Ouvrez les propriétés de la tâche Analyse rapide d'une des méthodes suivantes :
   - Cliquez deux fois sur le nom de la tâche.
   - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés**.
3. Sélectionnez la section **Analyse contre les virus**.
4. Le cas échéant, dans la section **Analyse**de l'espace de travail, configurez les paramètres suivants :
   - Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis, utilisez le curseur du groupe **Niveau de sécurité**.
   - Si vous souhaitez configurer les paramètres de sécurité manuellement, cliquez sur le bouton **Paramètres** et procédez comme suit :
     a. Dans le groupe **Types de fichiers** de l'onglet **Général**, sélectionnez les types de fichiers que Kaspersky Endpoint Security contrôlera.
     b. Configurez les performances de l'analyse dans le groupe **Optimisation** sous l'onglet **Général**.

c. Sous l'onglet **Général**, dans le groupe **Fichiers composés**, sélectionnez les types de fichier composé que Kaspersky Endpoint Security analysera.

d. Sous l'onglet **Avancé**, dans le groupe **Paramètres complémentaires**, configurez l'utilisation de la technologie iSwift, la reprise des tâches arrêtées et la consignation des informations relatives aux objets malveillants détectés dans les statistiques de l'application.

e. Sous l'onglet **Avancé**, dans le groupe **Analyse heuristique**, configurez les paramètres de l'utilisation de l'analyse heuristique et sélectionnez le niveau de protection utilisé par l'analyse heuristique.

- Le groupe **Action** permet de sélectionner l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un fichier infecté ou potentiellement infecté.

- Si vous souhaitez définir une zone d'analyse, réalisez les opérations suivantes dans le groupe **Zone d'analyse** :

a. Cliquez sur le bouton **Paramètres**.

La fenêtre **Zone d'analyse** s'ouvre.

a. Si vous souhaitez que Kaspersky Endpoint Security analyse les objets dans la liste par défaut, cochez la case en regard de l'objet souhaité.

b. Si vous souhaitez que Kaspersky Endpoint Security analyse d'autres fichiers ou dossiers, cliquez sur le bouton **Ajouter** et désignez le fichier, le dossier ou le masque de nom de fichier ou de dossier.

5. Enregistrez les modifications introduites d'une des méthodes suivantes :

- Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : Analyse rapide** après l'enregistrement des modifications introduites.

- Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Analyse rapide** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE D'ANALYSE COMPLETE

Pour consulter et modifier les paramètres de la tâche d'analyse complète, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client (cf. section "Consultation de la liste des tâches locales" à la page 119).

2. Ouvrez les propriétés de la tâche Analyse complète d'une des méthodes suivantes :

- Cliquez deux fois sur le nom de la tâche.

- Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.

- Cliquez sur le bouton **Propriétés**.

3. Sélectionnez la section **Analyse contre les virus**.

4. Le cas échéant, dans la section **Analyse**de l'espace de travail, configurez les paramètres suivants :

- Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis, utilisez le curseur du groupe **Niveau de sécurité**.

- Si vous souhaitez configurer les paramètres de sécurité manuellement, cliquez sur le bouton **Paramètres** et procédez comme suit :

a. Dans le groupe **Types de fichiers** de l'onglet **Général**, sélectionnez les types de fichiers que Kaspersky Endpoint Security contrôlera.

b. Configurez les performances de l'analyse dans le groupe **Optimisation** sous l'onglet **Général**.

c. Sous l'onglet **Général**, dans le groupe **Fichiers composés**, sélectionnez les types de fichier composé que Kaspersky Endpoint Security analysera.

d. Sous l'onglet **Avancé**, dans le groupe **Paramètres complémentaires**, configurez l'utilisation de la technologie iSwift, la reprise des tâches arrêtées et la consignation des informations relatives aux objets malveillants détectés dans les statistiques de l'application.

e. Sous l'onglet **Avancé**, dans le groupe **Analyse heuristique**, configurez les paramètres de l'utilisation de l'analyse heuristique et sélectionnez le niveau de protection utilisé par l'analyse heuristique.

- Le groupe **Action** permet de sélectionner l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un fichier infecté ou potentiellement infecté.

- Si vous souhaitez définir une zone d'analyse, réalisez les opérations suivantes dans le groupe **Zone d'analyse** :

a. Cliquez sur le bouton **Paramètres**.

La fenêtre **Zone d'analyse** s'ouvre.

a. Si vous souhaitez que Kaspersky Endpoint Security analyse les objets dans la liste par défaut, cochez la case en regard de l'objet souhaité.

b. Si vous souhaitez que Kaspersky Endpoint Security analyse d'autres fichiers ou dossiers, cliquez sur le bouton **Ajouter** et désignez le fichier, le dossier ou le masque de nom de fichier ou de dossier.

5. Enregistrez les modifications introduites d'une des méthodes suivantes :

- Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : Analyse complète** après l'enregistrement des modifications introduites.

- Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Analyse complète** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE DE L'ANTI-VIRUS INTERNET

Pour consulter et modifier les paramètres d'une tâche de l'Anti-Virus Internet, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client (cf. section "Consultation de la liste des tâches locales" à la page 119).

2. Sélectionnez la tâche **Anti-Virus Internet** dans la liste des tâches locales et ouvrez ses propriétés d'une des méthodes suivantes :

- Cliquez deux fois sur le nom de la tâche.

- Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.

- Cliquez sur le bouton **Propriétés**.

3. Sélectionnez la section **Anti-Virus Internet**.

4. Le cas échéant, dans la section **Anti-Virus Internet** de l'espace de travail, configurez les paramètres suivants :

- Activez ou désactivez l'Anti-Virus Internet sur le poste client.

- Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis, utilisez le curseur du groupe **Niveau de sécurité**.

- Si vous souhaitez configurer les paramètres de sécurité manuellement, cliquez sur le bouton **Paramètres** et procédez comme suit :

  a. Activez ou désactivez l'analyse des adresses Internet selon la base des adresses Internet malveillantes dans le groupe **Mode d'analyse**.

  b. Activez ou désactivez l'analyse des adresses Internet selon la base des adresses Internet de phishing dans le groupe **Paramètres d'Anti-Phishing**.

  c. Dans le groupe **Anti-Phishing**, activez ou désactivez l'analyse heuristique pour détecter les liens de phishing.

5. Dans le groupe **En cas de détection d'un objet malveillant**, sélectionnez l'action qui sera exécutée par l'Anti-Virus Internet en cas de détection d'un objet dangereux dans le trafic Internet.

6. Enregistrez les modifications introduites d'une des méthodes suivantes :

   - Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : Anti-Virus Internet** après l'enregistrement des modifications introduites.

   - Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Anti-Virus Internet** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE D'AJOUT D'UNE CLE

Vous pouvez consulter et modifier les paramètres de la tâche d'ajout d'une clé dans les types de tâche suivants :

- tâches locales sur des postes client particuliers ;

- tâches pour des ordinateurs d'un groupe d'administration ;

- tâches pour des ordinateurs en dehors d'un groupe d'administration.

Pour consulter et modifier les paramètres d'une tâche d'ajout d'une clé, procédez comme suit :

1. Ouvrez la fenêtre des paramètres de la tâche d'ajout d'une clé (cf. section "Consultation des paramètres d'une tâche" à la page 117).

2. Choisissez la section **Activation de l'application**.

3. Le cas échéant, ajoutez une autre clé d'une des méthodes suivantes :

   - Si vous souhaitez sélectionner un code d'activation de la liste des codes d'activation ajoutés au référentiel de Kaspersky Security Center, procédez comme suit :

     a. Choisissez l'option **Code d'activation**.

     b. Cliquez sur le bouton **Sélectionner**.

        La fenêtre **Codes d'activation ajoutés au stockage Kaspersky Security Center** s'ouvre.

     c. Sélectionnez le code d'activation.

     d. Cliquez sur le bouton **OK**.

   - Si vous souhaitez ajouter un fichier clé, procédez comme suit :

     a. Choisissez l'option **Fichier clé**.

b. Cliquez sur le bouton **Ajouter**.

La fenêtre de sélection du fichier s'ouvre.

c. Sélectionnez le fichier clé.

d. Cliquez sur le bouton **Ouvrir**.

La clé actuelle est supprimée lors de l'ajout d'une autre clé..

4. Si vous souhaitez ajouter la clé désignée en tant que clé de réserve, cochez la case **Ajouter en tant qu'une clé de réserve**.

   La clé de réserve deviendra la clé active à l'échéance de la validité de la clé active actuelle.

5. Enregistrez les modifications introduites d'une des méthodes suivantes :

   - Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.
   - Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE DE PROTECTION CONTRE LES ATTAQUES RESEAU

Pour consulter et modifier les paramètres de la tâche de protection contre les attaques réseau, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client (cf. section "Consultation de la liste des tâches locales" à la page 119).
2. Dans la liste des tâches locales, sélectionnez la tâche **Protection contre les attaques réseau** et ouvrez les propriétés d'une des méthodes suivantes :

   - Cliquez deux fois sur le nom de la tâche.
   - Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.
   - Cliquez sur le bouton **Propriétés**.

3. Sélectionnez la section **Prévention des intrusions**.
4. Le cas échéant, dans la section **Protection contre les attaques réseau** de l'espace de travail, configurez les paramètres suivants :

   - Activez ou désactivez la protection contre les attaques réseau sur le poste client.
   - Dans le groupe **Paramètres de la protection contre les attaques réseau**, cochez ou décochez la case **Ajouter les ordinateurs attaquants à la liste des ordinateurs bloqués pendant <valeur> min** et indiquez la valeur.
   - Vous pouvez également indiquer les adresses IP des ordinateurs dont l'activité réseau ne sera pas bloquée. Pour ce faire, exécutez les actions suivantes :

     - Cliquez sur le bouton **Exclusions**.

       La fenêtre **Exclusions** s'ouvre.

- Cliquez sur le bouton **Ajouter**.

  La fenêtre **Adresse IP** s'ouvre.

- Indiquez l'adresse IP de l'ordinateur dont l'activité réseau ne sera pas bloquée.

5. Enregistrez les modifications introduites d'une des méthodes suivantes :

   - Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : Protection contre les attaques réseau** après l'enregistrement des modifications introduites.

   - Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Protection contre les attaques réseau** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE DE MISE A JOUR

Vous pouvez consulter et modifier les paramètres de la tâche de mise à jour dans les types de tâche suivants :

- tâches locales sur des postes client particuliers ;
- tâches pour des ordinateurs d'un groupe d'administration ;
- tâches pour des ordinateurs en dehors d'un groupe d'administration.

Pour consulter et modifier les paramètres de la tâche de mise à jour, procédez comme suit :

1. Ouvrez la fenêtre des paramètres de la tâche de mise à jour (cf. section "Consultation des paramètres d'une tâche" à la page 117).
2. Choisissez la section **Mise à jour**.
3. Si vous souhaitez que Kaspersky Endpoint Security mette à jour les modules de l'application en même temps que les bases de l'application, cochez la case **Mettre à jour les modules de l'application**.
4. Si vous souhaitez que Kaspersky Endpoint Security copie les fichiers de mise à jour dans un dossier local ou réseau, cochez la case **Copier les fichiers de mise à jour dans un dossier** et indiquez le chemin d'accès au dossier.
5. Si vous souhaitez sélectionner la source de la mise à jour, procédez comme suit :

   a. Cliquez sur le bouton **Paramètres**.

      La fenêtre **Paramètres : Mise à jour** s'ouvre.

   b. Indiquez la source des mises à jour d'une des méthodes suivantes :

      - Si vous souhaitez que l'application télécharge la mise à jour depuis le Serveur d'administration, cochez la case **Kaspersky Security Center**.

      - Si vous souhaitez que l'application télécharge les mises à jour depuis les serveurs de Kaspersky Lab, cochez la case **Serveurs de mises à jour de Kaspersky Lab**.

      - Si vous souhaitez indiquer une autre source de mises à jour, cliquez sur le bouton **Ajouter** et dans la fenêtre qui s'ouvre, saisissez le chemin d'accès à cette source de mise à jour.

      Par défaut, Kaspersky Endpoint Security récupère les mises à jour sur le Serveur d'administration et sur les serveurs de mises à jour de Kaspersky Lab.

6. Enregistrez les modifications introduites d'une des méthodes suivantes :

   - Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.

   - Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE D'ANALYSE DEFINIE PAR L'UTILISATEUR

Vous pouvez configurer les paramètres de la tâche d'analyse contre les virus dans les types de tâche suivants :

- tâches locales pour des postes client particulier du groupe d'administration ;
- tâches pour des sélections de postes client en dehors du groupe d'administration ;
- tâches pour des postes client.

Pour consulter et modifier les paramètres d'une tâche d'analyse contre les virus, procédez comme suit :

1. Ouvrez la fenêtre des paramètres de la tâche d'analyse (cf. section "Consultation des paramètres d'une tâche" à la page 117).
2. Sélectionnez la section **Analyse contre les virus**.
3. Si vous souhaitez modifier le niveau de sécurité auquel Kaspersky Endpoint Security exécute la tâche d'analyse contre les virus, réalisez une des opérations suivantes dans le groupe **Niveau de sécurité** :

   - Sélectionnez le niveau de sécurité prédéfini en déplaçant le curseur le long de l'échelle.

     Vous avez le choix entre les options suivantes :

     - **Protection maximale**. Kaspersky Endpoint Security exerce un contrôle total sur les fichiers ouverts, enregistrés et modifiés.
     - **Recommandé**. Kaspersky Endpoint Security contrôle les fichiers selon les paramètres recommandés par les experts de Kaspersky Lab.

       Ce niveau de sécurité est sélectionné par défaut.

     - **Vitesse maximale**. Kaspersky Endpoint Security contrôle une sélection minime de fichiers. Vous pouvez choisir ce niveau de sécurité si vous souhaitez pouvoir travailler sans contraintes avec d'autres applications gourmandes en mémoire vive.

   - Configurez manuellement les paramètres de sécurité :

     a. Cliquez sur le bouton **Paramètres**.

        La fenêtre **Paramètres : Analyse contre les virus** s'ouvre.

     b. Dans le groupe **Types de fichiers** de l'onglet **Général**, sélectionnez le type de fichiers que Kaspersky Endpoint Security contrôlera dans le cadre de l'analyse conte les virus.

     c. Configurez les performances de l'analyse dans le groupe **Optimisation** sous l'onglet **Général**.

     d. Sous l'onglet **Général**, dans le groupe **Fichiers composés**, sélectionnez les types de fichier composé que Kaspersky Endpoint Security soumettra à l'analyse.

     e. Sous l'onglet **Avancé**, dans le groupe **Paramètres complémentaires**, configurez l'utilisation de la technologie iSwift, la reprise des tâches arrêtées et la consignation des informations relatives aux objets malveillants détectés dans les statistiques de l'application.

f. Sous l'onglet **Avancé**, dans le groupe **Analyse heuristique**, configurez les paramètres de l'utilisation de l'analyse heuristique et sélectionnez le niveau de protection utilisé par l'analyse heuristique lors de l'exécution de la tâche d'analyse contre les virus.

g. Cliquez sur **OK** pour enregistrer les modifications introduites et fermer la fenêtre **Paramètres : Analyse**.

Le niveau de sécurité devient **Personnalisé**.

- Si vous souhaitez rétablir les paramètres par défaut, cliquez sur le bouton **Par défaut**.

Le nom du niveau de sécurité devient **Recommandé**.

4. Le groupe **Action** permet de sélectionner, le cas échéant, l'action que Kaspersky Endpoint Security exécutera en cas de découverte d'un fichier infecté ou potentiellement infecté.

Dans les tâches pour les postes client appartenant au groupe d'administration et dans les tâches pour les sélections de postes client en dehors des groupes d'administration, les options **Confirmer à la fin de l'analyse** et **Confirmer pendant l'analyse** ne sont pas disponibles.

5. Si vous souhaitez définir une zone d'analyse, réalisez les opérations suivantes dans le groupe **Zone d'analyse** :

a. Cliquez sur le bouton **Paramètres**.

La fenêtre **Zone d'analyse** s'ouvre.

b. Si vous souhaitez que Kaspersky Endpoint Security analyse la mémoire vive, cochez la case **Mémoire vive**.

c. Si vous souhaitez que Kaspersky Endpoint Security analyse les objets de démarrage, cochez la case **Objets de démarrage**.

d. Si vous souhaitez que Kaspersky Endpoint Security analyse tous les disques internes, cochez la case **Tous les disques internes**.

e. Si vous souhaitez que Kaspersky Endpoint Security analyse d'autres fichiers ou dossiers, cliquez sur le bouton **Ajouter** et désignez le fichier, le dossier ou le masque de nom de fichier ou de dossier.

6. Enregistrez les modifications introduites d'une des méthodes suivantes :

- Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.

- Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : <nom de la tâche>** après l'enregistrement des modifications introduites.

CONSULTATION ET MODIFICATION DES PARAMETRES DE LA TACHE DE L'ANTI-VIRUS FICHIERS

Pour consulter et modifier les paramètres d'une tâche de l'Anti-Virus Fichiers, procédez comme suit :

1. Ouvrez la liste des tâches locales pour un poste client (cf. section "Consultation de la liste des tâches locales" à la page 119).

2. Dans la liste des tâches locales, choisissez **Anti-Virus Fichiers** et ouvrez ses propriétés d'une des manières suivantes :

- Cliquez deux fois sur le nom de la tâche.

- Cliquez-droit pour ouvrir le menu contextuel de la tâche et choisissez l'option **Propriétés**.

- Cliquez sur le bouton **Propriétés**.

3. Sélectionnez la section **Anti-Virus Fichiers**.

4. Le cas échéant, dans la section **Anti-Virus Fichiers**de l'espace de travail, configurez les paramètres suivants :

   - Activez ou désactivez l'Anti-Virus Fichiers sur le poste client.

   - Si vous souhaitez utiliser un des niveaux de sécurité prédéfinis, utilisez le curseur du groupe **Niveau de sécurité**.

   - Si vous souhaitez configurer les paramètres de sécurité manuellement, cliquez sur le bouton **Paramètres** et procédez comme suit :

     a. Dans le groupe **Types de fichiers** de l'onglet **Général**, sélectionnez les types de fichiers que Kaspersky Endpoint Security contrôlera à l'ouverture, pendant l'exécution et à l'enregistrement.

     b. Sous l'onglet **Général**, dans le groupe **Optimisation**, configurez les performances de l'analyse et sélectionnez la technologie de l'analyse.

     c. Sous l'onglet **Général**; dans le groupe **Fichiers composés**, sélectionnez les fichiers composants dans lesquels il faudra rechercher les objets indiqués et introduisez les restrictions sur l'analyse des objets de grande taille.

     d. Sous l'onglet **Zone de protection**, désignez les fichiers ou les dossiers que l'Anti-Virus Fichiers va contrôler.

        L'analyse de tous les objets situés sur les disques durs, les disques amovibles et les disques réseau connectés au poste client est activée par défaut. Vous pouvez ajouter un objet à analyser, modifier un objet dans la liste, suspendre temporairement la protection d'un objet dans la liste ou le supprimer de la liste.

     e. Sous l'onglet **Avancé**, dans le groupe **Mode d'analyse**, sélectionnez le mode de fonctionnement de l'Anti-Virus Fichiers.

     f. Sous l'onglet **Avancé**, dans le groupe **Suspension des tâches**, activez ou désactivez la suspension planifiée de l'Anti-Virus Fichiers et configurez les paramètres de suspension automatique des tâches planifiées.

     g. Sous l'onglet **Avancé**, dans le groupe **Analyse heuristique**, configurez l'utilisation de l'analyse heuristique par l'Anti-Virus Fichiers.

   - Dans le groupe **En cas de détection d'un objet malveillant**, sélectionnez l'action qui sera exécutée par l'Anti-Virus Fichiers en cas de détection d'un objet infecté ou potentiellement infecté.

5. Enregistrez les modifications introduites d'une des méthodes suivantes :

   - Cliquez sur le bouton **Appliquer** pour rester dans la fenêtre **Propriétés : Anti-Virus Fichiers** après l'enregistrement des modifications introduites.

   - Cliquez sur le bouton **OK** pour fermer la fenêtre **Propriétés : Anti-Virus Fichiers** après l'enregistrement des modifications introduites.

COMPOSITION DU RAPPORT SUR LES OBJETS QUE L'APPLICATION A DETECTE SUR LE POSTE CLIENT

Pour composer le rapport sur les objets détectés sur le poste client, procédez comme suit :

1. Lancez la Console d'administration Kaspersky Security Center.
2. Développez le nœud **Serveur d'administration - <Nom du serveur>**.
3. Développez le dossier **Ordinateurs gérés**.
4. Dans le dossier **Ordinateurs gérés**, choisissez le groupe d'administration auquel appartient le poste client.
5. Choisissez l'onglet **Ordinateurs**.
6. Sélectionnez l'ordinateur requis dans la liste des postes client.
7. Ouvrez la fenêtre **Propriétés : <nom de l'ordinateur>** d'une des méthodes suivantes :
   - double-clic sur le nom du poste client ;
   - clic droit pour ouvrir le menu contextuel du poste client et sélection de l'option **Propriétés** ;
   - lien **Propriétés de l'ordinateur** dans le groupe d'administration de l'objet sélectionné.
8. Choisissez la section **Protection**.
9. Dans l'espace de travail, créez le rapport en cliquant sur le lien **Consulter le rapport sur les virus découverts**.

Le rapport s'affiche dans une fenêtre du navigateur.

Vous trouverez des informations sur les autres méthodes de composition d'un rapport sur les objets que l'application a détecté sur le poste client dans le *Manuel de l'administrateur de Kaspersky Security Center*.

CONTACTER LE SUPPORT TECHNIQUE

Cette section décrit les modes de support technique et les conditions nécessaires pour bénéficier du Support technique.

DANS CETTE SECTION

Présentation du Support Technique 129

Support technique par téléphone 129

Support technique via Kaspersky CompanyAccount 130

Utilisation du fichier de traçage 130

Création d'un fichier de traçage 130

Collecte d'informations pour le Support Technique 131

PRESENTATION DU SUPPORT TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des autres sources d'informations relatives à l'application (cf. section "Sources d'information sur l'application "à la page 11), contactez le Support Technique de Kaspersky Lab. Les experts du Support technique répondront à toutes vos questions concernant l'installation et l'utilisation de l'application.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence commerciale pour l'application. Le Support n'est pas proposé aux utilisateurs d'une version d'essai.

Avant de contacter le Support Technique, veuillez prendre connaissance des règles d'octroi de l'assistance technique (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du Support Technique par un des moyens suivants :

- Téléphoner au Support Technique de Kaspersky Lab.
- Envoyer une requête au Support Technique de Kaspersky Lab via le service en ligne Kaspersky CompanyAccount.

SUPPORT TECHNIQUE PAR TELEPHONE

Dans la majorité des régions, les experts du support technique de Kaspersky Lab sont joignables par téléphone. Vous pouvez trouver des informations sur les modes d'obtention de l'assistance technique dans votre région et les coordonnées du Support Technique sur le site Internet du Support Technique de Kaspersky Lab" (http://support.kaspersky.com/b2b).

Avant de contacter le Service de Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique (http://support.kaspersky.com/fr/support/rules). Ces règles précisent les heures auxquelles vous pouvez contacter le Support Technique de Kaspersky Lab ainsi que les données à fournir à l'expert pour qu'il puisse vous venir en aide.

SUPPORT TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) est un service Internet destiné aux organisations qui utilisent les applications de Kaspersky Lab. Le service Kaspersky CompanyAccount permet aux utilisateurs d'interagir avec les experts de Kaspersky Lab par le biais de requêtes électroniques. Le service Internet Kaspersky CompanyAccount permet de suivre le traitement des requêtes envoyées aux experts de Kaspersky Lab et de conserver l'historique de celles-ci.

Vous pouvez inscrire tous les employés de votre entreprise au sein d'un seul compte Kaspersky CompanyAccount. Un compte permet de gérer de manière centralisée les requêtes électroniques des employés inscrits chez Kaspersky Lab ainsi que de gérer les autorisations de ces employés au sein du Kaspersky CompanyAccount.

Le service en ligne de Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais
- Russe
- Français
- Japonais

Vous pouvez également obtenir de plus amples informations sur le Kaspersky CompanyAccount sur le site Internet du Support technique (http://support.kaspersky.com/fr/faq/companyaccount_help).

UTILISATION DU FICHIER DE TRACE

Après avoir communiqué votre problème aux experts du Support Technique de Kaspersky Lab, ces derniers peuvent vous demander de créer un rapport contenant les informations sur le fonctionnement de Kaspersky Endpoint Security et de leur envoyer ce document. Les experts du Support Technique de Kaspersky Lab peuvent également vous demander de créer *un fichier de traçage*. Le fichier de traçage permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

CREATION D'UN FICHIER DE TRAÇAGE

Pour créer un fichier de traçage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (à la page 22).
2. Dans le panneau de navigation de la partie supérieure de la fenêtre principale de l'application, cliquez sur le bouton .

   La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Rapports** de la fenêtre des paramètres de l'application, dans le groupe **Traçage**, cochez la case **Activer le traçage**.

4. Relancez Kaspersky Endpoint Security pour lancer le processus de traçage.

Utilisez le traçage uniquement sous la direction d'un spécialiste du Support Technique de Kaspersky Lab.

Les fichiers de traçage peuvent occuper beaucoup d'espace sur le disque. Après avoir terminé le travail avec les fichiers de traçage, il est recommandé de désactiver leur création en décochant la case **Activer le traçage** sous l'onglet **Rapports** de la fenêtre des paramètres de l'application. Il est ensuite nécessaire de relancer Kaspersky Endpoint Security.

COLLECTE D'INFORMATIONS POUR LE SUPPORT TECHNIQUE

Pour une assistance plus efficace en cas de questions sur l'utilisation de l'application, les experts du Support Technique peuvent vous demander (pour la réparation) de modifier les paramètres de l'application pendant les diagnostics. Pour ce faire, l'exécution des actions suivantes peut être requise :

- Activer la fonctionnalité de remise à zéro des informations diagnostiques élargies.
- Exécuter une configuration plus fine des modules distincts de l'application, qui n'est pas disponibles via les outils standards de l'interface d'utilisateur.
- Modifier les paramètres d'envoi des informations diagnostiques récoltées.

Toutes les informations requises à la réalisation des actions citées et la composition des données récoltées aux fins de débogages seront précisées par les opérateurs du Support Technique. Les informations diagnostiques élargies récoltées sont enregistrées sur l'ordinateur de l'utilisateur. Les données récoltées ne sont pas envoyées automatiquement à Kaspersky Lab.

ANNEXES

Cette section contient des renseignements qui viennent compléter le contenu principal du document.

DANS CETTE SECTION

Liste des objets analysés en fonction de l'extension 132

Masques dans les chemins d'accès aux fichiers et aux dossiers 137

LISTE DES OBJETS ANALYSES EN FONCTION DE L'EXTENSION

Si dans le cadre de la configuration de l'analyse contre les virus (cf. section "Sélection du niveau de sécurité" à la page 60) vous aviez choisi l'option **Analyser les applications et les documents (selon l'extension)**, alors Kaspersky Endpoint Security recherche la présence éventuelle de virus dans les objets sans extensions et dans les objets portant une des extensions reprises ci-dessous :

Formats généraux

- txt ;
- csv ;
- htm ;
- html.

Fichiers multimédia (audio/vidéo)

- flv ;
- f4v ;
- avi ;
- 3gp ;
- 3g2 ;
- 3gp2 ;
- 3p2 ;
- divx ;
- mp4 ;
- mkv ;
- mov ;
- qt ;
- asf ;

- wmv ;
- rm ;
- rmvb ;
- vob ;
- dat ;
- mpg ;
- mpeg ;
- bik ;
- fcs ;
- mp3 ;
- mpeg3 ;
- flac ;
- ape ;
- ogg ;
- aac ;
- m4a ;
- wma ;
- ac3 ;
- wav ;
- mka ;
- rm ;
- ra ;
- ravb ;
- mid ;
- midi ;
- cda.

Images

- jpg ;
- jpe ;
- jpeg ;
- jff ;
- gif ;

- png ;
- bmp ;
- tif ;
- tiff ;
- emf ;
- wmf ;
- eps ;
- psd ;
- cdr ;
- swf.

Fichiers exécutables et système

- exe ;
- dll ;
- scr ;
- ocx ;
- com ;
- sys ;
- class ;
- o ;
- so ;
- elf ;
- prx ;
- vb ;
- vbs ;
- js ;
- bat ;
- cmd ;
- msi ;
- deb ;
- rpm ;

- sh ;
- pl ;
- dylib.

Documents et modèles

- doc ;
- dot ;
- docx ;
- dotx ;
- docm ;
- dotm ;
- xsl ;
- xls ;
- xlsx ;
- xltx ;
- xlsm ;
- xltm ;
- xlam ;
- xlsb ;
- ppt ;
- pot ;
- pps ;
- pptx ;
- potx ;
- pptm ;
- potm ;
- ppsx ;
- ppsm ;
- rtf ;
- pdf ;
- msg ;

- eml ;
- vsd ;
- vss ;
- vst ;
- vdx ;
- vsx ;
- vtx ;
- xps ;
- oxps ;
- one ;
- onepkg ;
- xsn ;
- odt ;
- ods ;
- odp ;
- sxw ;
- pub ;
- mdb ;
- accdb ;
- accde ;
- accdr ;
- accdc ;
- chm ;
- mht.

Fichiers compactés

- zip ;
- 7z* ;
- 7-z ;
- rar ;
- iso ;

- cab ;
- jar ;
- bz ;
- bz2 ;
- tbz ;
- tbz2 ;
- gz ;
- tgz ;
- arj ;
- dmg ;
- smi ;
- img ;
- xar.

Le format réel du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

MASQUES DANS LES CHEMINS D'ACCES AUX FICHIERS ET AUX DOSSIERS

Vous pouvez utiliser la tilde (~) dans la définition de la zone de protection, de la zone d'analyse et de la zone de confiance.

Le caractère ~ dans le chemin d'accès à un fichier ou à un dossier remplace /Users/<nom de l'utilisateur>. Par exemple, le chemin d'accès ~/Desktop indique que la zone de protection contient le dossier Desktop de tous les utilisateurs pour les ordinateurs desquels vous créez une zone de protection.

GLOSSAIRE

A

ACTIVATION DE L'APPLICATION

L'application devient entièrement fonctionnelle. L'activation est exécutée par l'utilisateur pendant ou après l'installation de l'application. Pour activer l'application, l'utilisateur doit posséder le code d'activation ou le fichier clé.

ADMINISTRATEUR KASPERSKY SECURITY CENTER

Personne qui gère le fonctionnement de l'application via le système d'administration centralisée à distance Kaspersky Security Center.

AGENT D'ADMINISTRATION

Composant de l'application Kaspersky Security Center qui coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (un poste de travail ou un serveur). Ce composant est unique pour toutes les applications pour Windows développées par la société. Il existe des versions de l'Agent d'administration pour les versions des logiciels de Kaspersky Lab pour Novell®, Unix™ et Mac.

ANALYSEUR HEURISTIQUE

La technologie de détection des menaces dont les informations ne sont pas inscrites dans les bases de Kaspersky Lab. L'analyseur heuristique permet de découvrir les objets dont le comportement dans le système d'exploitation évoque celui d'une menace. Les objets détectés à l'aide de l'analyseur heuristique sont reconnus comme des objets potentiellement infectés. Par exemple, l'objet contenant les suites des commandes propres aux objets infectés (ouverture des fichiers, enregistrement dans le fichier) peut être reconnu comme l'objet potentiellement infecté.

ARCHIVE

Un ou plusieurs fichiers regroupés dans un même fichier compressé. La compression et la décompression des données requièrent une application spéciale appelée un compacteur.

B

BASE ANTIVIRUS

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les Bases antivirus sont composées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

BLOCAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté ou modifié.

C

CLE ACTIVE

La clé utilisée au moment actuel pour faire fonctionner l'application.

CLE DE RESERVE

La clé qui confirme le droit d'utilisation de l'application mais qui n'est pas utilisée actuellement.

CLIENT DU SERVEUR D'ADMINISTRATION (POSTE CLIENT)

Ordinateur, serveur ou poste de travail sur lequel sont installés l'Agent d'administration et les applications de Kaspersky Lab gérées.

E

ETAT DE LA PROTECTION

Etat actuel de la protection qui définit le niveau de protection de l'ordinateur.

EXCLUSION

Exclusion : objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un dossier ou un programme), des processus ou des objets selon un nom conforme à la classification de l'Encyclopédie des virus. Chaque tâche peut avoir ses propres exclusions.

F

FAUX-POSITIFS

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

G

GROUPE D'ADMINISTRATION

Sélection d'ordinateurs regroupés selon les fonctions exécutées et les applications de Kaspersky Lab installées. Les ordinateurs sont regroupés pour en faciliter la gestion au sein d'un ensemble. Un groupe peut contenir d'autres groupes. Pour chacune des applications installées dans un groupe, il est possible de créer des stratégies de groupe et des tâches de groupe.

M

MASQUE DE FICHIERS

Représentation du nom d'un fichier à l'aide de caractères génériques. Les principaux caractères génériques utilisés dans les masques sont * et ? (où * représente n'importe quelle série de caractères et ?, n'importe quel caractère unique).

MISE A JOUR

La fonction de l'application de Kaspersky Lab qui permet de maintenir la protection de l'ordinateur dans l'état actuel. Pendant la mise à jour, l'application copie les mises à jour des bases et des modules de l'application à partir des serveurs de mises à jour de Kaspersky Lab sur l'ordinateur et les installe et les applique automatiquement.

N

NIVEAU RECOMMANDE

Niveau de sécurité qui repose sur les paramètres de fonctionnement de l'application recommandés par les experts de Kaspersky Lab et qui garantissent la protection optimale de l'ordinateur. Ce niveau est sélectionné par défaut.

O

OBJET INFECTE

Objet dont un segment de code correspond parfaitement à un segment de code d'un programme dangereux connu. Les experts de Kaspersky Lab ne conseillent pas de travailler avec tels objets.

OBJET OLE

Objet associé à un autre fichier ou intégré à un fichier à l'aide de la technologie Object Linking and Embedding (OLE). Un tableau créé dans Microsoft Office Excel® et intégré dans un document Microsoft Office Word est un objet OLE.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient un segment modifié de code d'un programme dangereux connu ou objet dont le comportement évoque un tel programme.

P

PAQUET DE MISE A JOUR

Paquet de fichiers pour la mise à jour des modules de l'application. L'application de Kaspersky Lab copie les paquets de mise à jour depuis les serveurs de mises à jour de Kaspersky Lab, puis les installe et les applique automatiquement.

PORT RESEAU

Paramètre des protocoles TCP et UDP qui détermine la destination des paquets de données au format IP transmis à l'hôte via le réseau et qui permet à différentes applications, exécutées sur un hôte, de recevoir les données indépendamment les unes des autres. Chaque application traite les données reçues via le port défini (on dit parfois que l'application "écoute" ce numéro de port).

En général, il existe pour certains protocoles réseau répandus des numéros de port standard (par exemple, les serveurs Web reçoivent normalement les données via le protocole HTTP sur le port TCP 80), même si dans l'absolu, une application peut utiliser n'importe quel protocole sur n'importe quel port. Un numéro de port peut être compris entre 1 et 65535.

PROTECTION

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTECTION MAXIMALE

Niveau de sécurité de l'ordinateur qui correspond à la protection la plus complète que peut offrir l'application. A ce niveau, la recherche d'éventuels virus porte sur tous les fichiers de l'ordinateur, les disques amovibles et les disques réseau, si ceux-ci sont connectés à l'ordinateur.

Q

QUARANTAINE

Dossier dans lequel l'application de Kaspersky Lab place les objets potentiellement infectés qu'elle a détectés. Les objets en quarantaine sont enregistrés sous forme chiffrée pour éviter qu'ils puissent agir sur l'ordinateur.

R

REPARATION D'OBJETS

Le mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Il n'est pas possible de réparer tous les objets infectés.

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

S

SAUVEGARDE

Dossier spécial prévu pour conserver les copies de sauvegarde des objets créés avant leur réparation ou leur suppression.

SERVEUR D'ADMINISTRATION

Composant de l'application Kaspersky Security Center qui remplit la fonction d'enregistrement centralisé des informations sur les applications Kaspersky Lab installées sur le réseau local de la société, et d'un outil efficace de gestion de ces applications.

SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Serveurs HTTP de Kaspersky Lab sur lesquels les applications de Kaspersky Lab récupèrent les mises à jour des bases et des modules de l'application.

STRATEGIE

Une stratégie détermine des paramètres de fonctionnement de l'application et d'accès à la configuration de l'application installée sur les ordinateurs du groupe d'administration. Il faut créer une stratégie pour chaque application. Vous pouvez créer un nombre infini de stratégies différentes pour les applications installées sur les ordinateurs de chaque groupe d'administration. Toutefois, au sein de chacun de ces groupes, une seule stratégie peut être appliquée simultanément à chaque programme.

STRATEGIE DE GROUPE

Cf. Stratégie

T

TACHE DE GROUPE

Tâche déterminée pour un groupe d'administration et exécutée sur tous les postes client qui appartiennent à ce groupe d'administration.

TACHE POUR UNE SELECTION D'ORDINATEURS

Tâche définie pour une sélection de postes client tirés de divers groupes d'administration et exécutée sur ceux-ci.

AO KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les 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 qualifiés.

PRODUITS. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des applications antivirus pour ordinateurs de bureau et ordinateurs portables, ainsi que des applications pour la protection des tablettes, des smartphones et autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases anti-virus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (E-U), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie des virus :	http://www.securelist.com/fr/
Laboratoire d'étude des virus :	http://newvirus.kaspersky.com/fr/ (pour l'analyse des fichiers et des sites Internet suspects)
Forum Internet de Kaspersky Lab :	http://forum.kaspersky.com/index.php?showforum=129

INFORMATIONS SUR LE CODE TIERS

Les informations relatives au code tiers sont reprises dans le fichier legal_notices.txt qui se trouve dans le dossier d'installation de l'application.

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Finder, Mac, OS X et Safari sont des marques commerciales d'Apple Inc., déposées aux Etats-Unis et dans d'autres pays.

Google Chrome est une marque de Google Inc.

Excel, Microsoft et Windows sont des marques de commerce de Microsoft Corporation, déposées aux Etats-Unis et dans d'autres pays.

Firefox est une marque déposée de Mozilla Foundation.

Novel est une marque de Novell Inc. déposée aux Etats-Unis et dans d'autres pays.

VMware Fusion est une marque de VMware, Inc. ou une marque déposées de VMware, Inc. aux Etats-Unis ou dans d'autres juridictions.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays, utilisée sous licence par X/Open Company Limited.

INDEX

A

Actions sur les objets 72
Activation de l'application 29
  version d'évaluation 30
Activation de l'application à l'aide du code d'activation 30
Agent d'administration
  installation 88, 89
Analyse 37, 38
  lancement planifié 62
  niveau de sécurité 60
  restauration des paramètres par défaut 62
AO Kaspersky Lab 142

B

Bases 65, 66
  mise à jour automatique 68
  mise à jour manuellement 68
Bases de l'application 39

C

Centre de protection 33, 35
Configuration matérielle et logicielle 15

D

Déploiement 86

F

Fenêtre principale de l'application 22

I

Installation
  à distance 92
  personnalisée 18
Installation à distance 92
Installation personnalisée 18

L

Lancement
  application 32
  tâche de recherche de virus 37, 38
Lancement de la tâche de mise à jour 39
Licence 26
  achat 29
  code d'activation 28
  Contrat de licence 26
  information 28
  renouveler 29

M

Mise à jour
  analyse des fichiers en quarantaine 72
  annulation de la dernière mise à jour 65

lancement programmé 68
objet de la mise à jour 68
source des mises à jour 68
Mise à jour de l'application 39

N

Niveau de sécurité
analyse 60
Notifications 24, 43

P

Plug-in d'administration
installation 87
Protection 34, 35

Q

Quarantaine 42

R

Rapports 42
Restauration de l'objet 42, 72

S

Sauvegarde 73
Script AVZ 130
Source des mises à jour 65, 68
Stockages
sauvegarde 73
Stratégie 101, 106
Suppression de l'application 20

T

Tâche 110
Trace
fichier de traçage 130

Z

Zone d'analyse 125