# Kaspersky Security 8.0 for Microsoft Exchange Servers

## Manuel d'administrateur

VERSION DE L'APPLICATION : 8.0 MAINTENANCE RELEASE 2 CRITICAL FIX 1

Chers utilisateurs !

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



Date d'édition du document : 09/11/2013



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

# TABLE DES MATIERES


PRESENTATION DU MANUEL ..... 7
Dans ce document ..... 7
Conventions ..... 9
SOURCES D'INFORMATIONS SUR L'APPLICATION ..... 11
Sources d'informations pour une recherche indépendante ..... 11
Discussion sur les logiciels de Kaspersky Lab dans le forum ..... 12
Coordonnées du service Ventes ..... 12
Coordonnées du Service de localisation et de rédaction de la documentation technique ..... 13
KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS ..... 14
Distribution ..... 15
Configurations logicielle et matérielle ..... 15
ARCHITECTURE DE L'APPLICATION ..... 19
INTERFACE DE L'APPLICATION ..... 20
Fenêtre principale de la Console d'administration ..... 20
Arborescence de la console d'administration ..... 21
Panneau des résultats ..... 22
Panneau d'accès rapide ..... 22
Menu contexuel ..... 23
OCTROI DES LICENCES POUR L'APPLICATION ..... 24
Présentation du contrat de licence ..... 24
Présentation de la licence ..... 24
Organisation de la licence ..... 25
Présentation du fichier clé ..... 25
Présentation de la divulgation des données ..... 26
Ajout d'une clé ..... 27
Consultation des informations relatives aux clés ..... 28
Remplacement d'une clé ..... 29
Suppression d'une clé ..... 29
Configuration de la notification sur l'expiration de la durée de validité de la licence ..... 30
Particularités de la licence pour les serveurs de sécurité du profil ..... 31
LANCEMENT ET ARRET DE L'APPLICATION ..... 32
CONSULTATION DE L'ETAT DE LA PROTECTION DU SERVEUR ..... 33
Protection par défaut du serveur Microsoft Exchange ..... 33
Consultation des informations relatives à l'état de la protection du serveur Microsoft Exchange ..... 34
Consultation des informations relatives à l'état de la protection du profil ..... 39
PREMIERE UTILISATION ..... 43
Lancement de la Console d'administration ..... 43
Connexion de la console d'administration au serveur de sécurité ..... 43
ADMINISTRATION DES PROFILS ..... 45
Présentation des profils ..... 45
Création d'un profil ..... 46
Configuration des paramètres des Serveurs de protection dans un profil ..... 47

Particularités de l'administration des profils dans un groupe de disponibilité de base de données Microsoft Exchange ....48
Ajout de serveurs de sécurité à un profil ....48
Suppression du serveur de sécurité d'un profil ....49
Suppression d'un profil ....50

MISE A JOUR DES BASES ....51
Présentation de la mise à jour des bases ....51
Présentation des centres de mises à jour ....52
Présentation de la mise à jour des bases dans les configurations avec cluster ou DAG de serveurs ....52
Lancement de la mise à jour manuelle des bases ....53
Configuration de la mise à jour des bases programmée ....53
Sélection de la source des mises à jour ....54
Configuration des paramètres de connexion à la source des mises à jour ....56
Configuration des paramètres du serveur proxy ....56
Désignation d'un serveur comme centre de mises à jour et configuration de ses paramètres ....57

PROTECTION ANTIVIRUS ....59
A propos de la Protection antivirus ....59
Présentation de la participation au Kaspersky Security Network ....61
À propos de la technologie ZETA Shield ....61
Activation et désactivation de la protection antivirus du serveur ....61
Activation et désactivation de KSN dans l'Antivirus ....63
Activation et désactivation de la technologie ZETA Shield ....63
Configuration des paramètres de traitement des objets ....64
Configuration des paramètres de protection des boîtes aux lettres et des dossiers publics ....65
Configuration des exclusions de l'analyse antivirus ....66
Présentation des destinataires de confiance ....66
Configuration des exclusions selon les adresses des destinataires ....67
Configuration des exclusions selon des masques de fichiers ....69
Configurer les paramètres d'analyse des archives et des objets-conteneurs joints ....70
Configuration des paramètres de l'analyse en arrière-plan ....70

PROTECTION CONTRE LE COURRIER INDESIRABLE ET LE PHISHING ....73
Présentation de la protection contre le courrier indésirable ....73
Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable ....75
Présentation de la lutte contre les tentatives de phishing ....76
Activation et désactivation de la protection du serveur contre le courrier indésirable ....77
Activation et désactivation de la recherche d'éléments de phishing dans les messages ....78
Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing ....78
Configuration des listes noire et blanche des expéditeurs ....80
Configuration de la liste blanche des destinataires ....82
Configuration de l'augmentation du classement de courrier indésirable d'un message` ....83
Recours à des services externes pour la détection du courrier indésirable ....85
Configuration des paramètres avancés de recherche de courrier indésirable et d'éléments de phishing ....87

SAUVEGARDE ....89
A propos de la sauvegarde ....89
Consultation du contenu de la Sauvegarde ....90
Consultation des propriétés des objets placés dans la sauvegarde ....91
Configuration des filtres de la sauvegarde ....93

Enregistrement sur le disque d'un objet de la sauvegarde ....93
Envoi d'un objet de la sauvegarde à des destinataires ....94
Suppression des objets de la sauvegarde ....94
Configuration des paramètres de la sauvegarde ....95
Sélection de la base de données de la sauvegarde pour consulter son contenu depuis le profil ....96

NOTIFICATIONS ....97
Présentation des notifications ....97
Configuration des paramètres de notification ....97
Configuration des paramètres d'envoi des notifications ....98

RAPPORTS ....100
Présentation des rapports sur le fonctionnement de l'application ....100
Création de rapports rapides ....101
Création de la tâche de composition des rapports ....102
Modification des paramètres de la tâche de composition des rapports ....103
Lancement de la tâche de composition des rapports ....103
Suppression de la tâche de composition des rapports ....104
Consultation des tâches de composition des rapports ....104
Consultation des rapports prêts ....105
Enregistrement du rapport ....108
Suppression du rapport ....108

JOURNAUX DE L'APPLICATION ....109
Présentation des journaux de l'application ....109
Configuration des paramètres des journaux ....110
Configuration du niveau de diagnostic ....110

ADMINISTRATION DES CONFIGURATIONS ....112
Exportation de la configuration ....112
Importation de la configuration ....113

VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION ....114
Présentation du fichier d'essai EICAR ....114
Présentation des types de fichier d'essai EICAR ....114
Vérification du fonctionnement de l'application à l'aide du fichier d'essai EICAR ....116

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE ....118
Modes d'obtention de l'assistance technique ....118
Assistance technique par téléphone ....118
Assistance technique via Kaspersky CompanyAccount ....119
Utilisation du fichier de traçage et du script AVZ ....120

APPLICATION. SCRIPT D'ENVOI D'UN MESSAGE NON SOLLICITE POUR EXAMEN ....121
Présentation du script d'envoi d'un message non sollicité pour examen ....121
Mode de fonctionnement du script ....122
Paramètres de lancement du script ....123
Configuration des paramètres du fichier de configuration du script ....124
Journal de fonctionnement du script ....125

GLOSSAIRE....126
KASPERSKY LAB ZAO....130
INFORMATIONS SUR LE CODE TIERS....131
AVIS SUR LES MARQUES....132
INDEX....133

# PRESENTATION DU MANUEL

Ce manuel est le Manuel de l'administrateur de Kaspersky Security 8.0 for Microsoft® Exchange Servers (ci-après Kaspersky Security ou l'application).

Ce manuel est destiné aux techniciens chargés d'installer et d'administrer Kaspersky Security et d'offrir une assistance aux entreprises qui utilisent Kaspersky Security.

Le manuel vise les objectifs suivants :

- Aider à configurer l'application et à l'utiliser.
- Offrir un accès rapide aux solutions des problèmes liés à l'utilisation de Kaspersky Security.
- Présenter les sources d'informations complémentaires sur l'application et les méthodes disponibles pour bénéficier du support technique.

### DANS CETTE SECTION DE L'AIDE

Dans ce document ..... 7

Conventions ..... 9

## DANS CE DOCUMENT

Ce document reprend les sections suivantes :

**Sources d'informations sur l'application (cf. page 11)**

Cette section décrit les sources d'informations sur l'application et indique les sites Internet que vous pouvez utiliser pour discuter de l'utilisation de l'application.

**Kaspersky Security 8.0 for Microsoft Exchange Servers (cf. page 14)**

Cette section décrit les possibilités de l'application et fournit de brèves informations sur ses fonctionnalités et ses modules. Elle précise le contenu de la distribution et indique les services accessibles aux utilisateur enregistrés. Vous y trouverez également les informations relatives à la configuration matérielle et logicielle requise pour l'ordinateur sur lequel vous souhaitez installer l'application.

**Architecture de l'application (cf. page 19)**

Cette section décrit les composants de Kaspersky Security et la logique de leur interaction.

**Interface de l'application (cf. page 20)**

Cette section décrit les principaux éléments de l'interface de l'application : la fenêtre principale de la console d'administration, l'arborescence de la console d'administration, la fenêtre des résultats, les panneaux des résultats, le menu contextuel et le volet d'accès rapide.

**Octroi des licences pour l'application (cf. page 24)**

Cette section aborde les principales notions liées à l'activation de l'application. Cette section explique le rôle du contrat de licence, les modes d'activation de l'application et le renouvellement de la licence.

**Lancement et arrêt de l'application (cf. page 32)**

Cette section explique comment lancer et arrêter l'application.

**Etat de la protection du serveur (cf. page 33)**

Cette section présente les paramètres de fonctionnement par défaut de Kaspersky Security. Elle explique également comment utiliser la Console d'administration afin d'obtenir des informations sur la licence de l'application, sur l'état des modules et des bases de l'application ainsi que des statistiques sur les messages traités et le nombre de menaces et de messages non sollicités.

**Première utilisation (cf. page 43)**

Cette section contient des informations sur l'utilisation de Kaspersky Security, le lancement de la Console d'administration et la création des listes de serveurs à protéger.

**Administration des profils (cf. page 45)**

Cette section explique comment utiliser les profils, en créer et configurer leurs paramètres.

**Mise à jour des bases (cf. page 51)**

Cette section présente la mise à jour des bases de l'application et décrit la configuration des paramètres de celle-ci.

**Protection antivirus (cf. page 59)**

Cette section décrit la protection antivirus du serveur Microsoft Exchange, l'analyse des banque en arrière plan et la configuration des paramètres de protection et d'analyse.

**Protection contre le courrier indésirable et le phishing (cf. page 73)**

Cette section contient des informations sur le filtrage des spams et des éléments de phishing dans le flux de messagerie ainsi que des instructions sur la configuration des paramètres de ces fonctions.

**Sauvegarde (cf. page 89)**

Cette section décrit la sauvegarde et son utilisation.

**Notifications (cf. page 97)**

Cette section décrit les notifications et leur configuration.

**Rapports (cf. page 100)**

Cette section décrit les rapports sur le fonctionnement de l'application et leur configuration.

**Journaux de l'application (cf. page 109)**

Cette section décrit les journaux de l'application et leur configuration.

### Administration des configurations (cf. page 112)

Cette section contient des informations sur la manière d'exporter la configuration de l'application dans un fichier et de l'importer depuis un fichier.

### Vérification du fonctionnement de l'application (cf. page 114)

Cette section explique comment vérifier le fonctionnement de l'application, à savoir confirmer que l'application détecte les fichiers et leur modification et qu'elle exécute sur ceux-ci les actions configurées.

### Contacter le service d'assistance technique (cf. page 118)

Cette section présente les différentes manières de contacter le service d'assistance technique de Kaspersky Lab.

### Application. Script d'envoi d'envoi d'un message non sollicité pour examen (cf. page 121)

Cette section contient des informations sur le script d'envoi d'un message non sollicité aux experts de Kaspersky Lab pour examen et sur la configuration de ses paramètres.

### Glossaire (cf. page 126)

Cette section reprend les définitions de certains termes utilisés dans ce document.

### Kaspersky Lab ZAO (cf. page 130)

Cette section présente la société Kaspersky Lab ZAO.

### Informations sur le code tiers (cf. page 131)

Cette section reprend des informations relatives au code tiers utilisé dans l'application.

### Avis sur les marques (cf. page 132)

Cette section reprend les informations relatives aux marques citées dans le document et à leurs détenteurs.

### Index

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

# CONVENTIONS

Le texte du document contient des éléments sémantiques auxquels nous vous conseillons de prêter attention. Il s'agit d'avertissements, de conseils et d'exemples.

Des conventions stylistiques sont utilisées pour mettre ces éléments en évidence. Le tableau ci-dessous reprend ces conventions ainsi que des exemples d'utilisation.

*Table 1. Conventions*

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| N'oubliez pas que... | Les avertissements sont mis en évidence en rouge dans un cadre.<br>Les avertissements contiennent des informations relatives aux actions indésirables qui pourraient entraîner la perte d'informations ou des échecs dans le fonctionnement du matériel ou du système d'exploitation. |

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| Il est conseillé d'utiliser... | Les remarques figurent dans un cadre.<br>Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes de paramètres ou des cas particuliers importants dans le fonctionnement de l'application. |
| **Exemple :**<br>... | Les exemples sont présentés sur un fond jaune sous le titre « Exemple ». |
| La *mise à jour*, c'est ...<br>L'événement *Les bases sont dépassées* s'est produit. | Les éléments suivants sont présentés en italiques :<br>• nouveaux termes ;<br>• noms des états et des événements de l'application ;. |
| Appuyez sur la touche **ENTREE**.<br>Appuyez sur la combinaison de touches **ALT**+**F4**. | Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.<br>Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches. |
| Cliquez sur le bouton **Activer**. | Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont écrits en caractères gras. |
| ➧ *Pour planifier une tâche, procédez comme suit :* | Les phrases d'introduction des instructions sont en italique et sont précédées de l'icône « flèche ». |
| Dans la ligne de commande, saisissez le texte help<br>Les informations suivantes s'affichent :<br>Indiquez la date au format JJ:MM:AA. | Les types suivants de texte apparaissent dans un style spécial :<br>• texte de la ligne de commande ;<br>• texte des messages affichés sur l'écran par l'application ;<br>• données à saisir par l'utilisateur. |
| <Nom d'utilisateur> | Les variables sont écrites entre crochets pointus. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les crochets pointus sont omis. |

# SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section décrit les sources d'informations sur l'application et indique les sites Internet que vous pouvez utiliser pour discuter de l'utilisation de l'application.

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

### DANS CETTE SECTION DE L'AIDE


Sources d'informations pour une recherche indépendante ..... 11

Discussion sur les logiciels de Kaspersky Lab dans le forum ..... 12

Coordonnées du service Ventes ..... 12

Coordonnées du Service de localisation et de rédaction de la documentation technique ..... 13


# SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDEPENDANTE

Vous pouvez rechercher des informations sur l'application dans les sources suivantes :

- page sur le site de Kaspersky Lab ;
- page sur le site du Service d'assistance technique (dans la banque de solutions) ;
- aide électronique ;
- documentation.

Si vous ne trouvez pas la réponse à votre question, il est conseillé de contacter le Support technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 118).

La consultation des sources d'informations sur le site de Kaspersky Lab requiert une connexion Internet.

### Page sur le site de Kaspersky Lab

Chaque produit de Kaspersky Lab possède sa propre page sur le site.

La page http://www.kaspersky.fr/security-microsoft-exchange-servers offre des informations générales sur l'application, ses possibilités et ses caractéristiques de fonctionnement.

La page http://www.kaspersky.fr contient un lien vers la boutique en ligne. Où vous pourrez acheter l'application ou renouveler la licence.

### Page sur le site du Service d'assistance technique (dans la banque de solutions)

Base de connaissances : rubrique du site du service d'assistance technique contenant des recommandations relatives à l'utilisation des applications de Kaspersky Lab. Elle reprend des articles organisés par sujet.

La page de l'application dans la Base de connaissances (http://support.kaspersky.fr/exchange/security8.0) reprend des articles utiles, des recommandations et des réponses aux questions les plus souvent posées sur l'achat, l'installation et l'utilisation de l'application.

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

### Aide électronique

L'aide électronique de l'application reprend les fichiers d'aide.

L'aide contextuelle reprend des informations sur chaque fenêtre de l'application : liste et description des paramètres et liens vers les tâches dans lesquelles ces paramètres interviennent.

L'aide complète contient les informations détaillées sur l'administration de la protection, la configuration des paramètres de l'application et la résolution des tâches principales de l'utilisateur.

### Documentation

La page du site Internet de Kaspersky Lab (http://www.kaspersky.com/fr/product-updates/microsoft-exchange-server-antivirus) propose des documents contenant des informations sur l'installation de l'application sur les ordinateurs du réseau de l'entreprise et sur la configuration de ses paramètres. Vous y trouverez également des informations sur les principales fonctionnalités de l'application.

## DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.fr.

Dans le forum, vous pouvez consulter les discussions antérieures, publier des commentaires ou créer une nouvelle discussion.

## COORDONNEES DU SERVICE VENTES

Si vous avez des questions sur la sélection, l'achat ou le renouvellement d'une licence d'utilisation d'une application, vous pouvez contacter les membres du Service Ventes d'une des manières suivantes :

- En appelant notre siège principal à Moscou (http://www.kaspersky.fr/contacts).
- En envoyant votre question par courrier à l'adresse sales@kaspersky.com.

Le service est offert en anglais et en russe.

# COORDONNEES DU SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Si vous souhaitez contacter le Service de localisation et de rédaction de la documentation technique, vous pouvez écrire à l'adresse docfeedback@kaspersky.com. En guise d'objet, indiqué « Kaspersky Help Feedback: Kaspersky Security 8.0 for Microsoft Exchange Servers ».

# KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS

Kaspersky Security 8.0 for Microsoft Exchange Servers est une application qui a été développée pour assurer la protection des serveurs de messagerie tournant sous Microsoft Exchange Server contre les virus, les chevaux de Troie, les vers et autres types de menaces pouvant être diffusées par courrier électronique, ainsi que contre le spam et le phishing.

Kaspersky Security offre une protection contre le courrier indésirable au niveau du serveur de messagerie de l'organisation, ce qui signifie que les employés n'ont plus besoin de supprimer manuellement le courrier indésirable.

Kaspersky Security protège les boîtes aux lettres, les dossiers publics et le flux de messagerie en transit sur le serveur Microsoft Exchange contre les programmes malveillants, le courrier indésirable et le phishing. L'ensemble du flux de messagerie qui transite via le serveur Microsoft Exchange protégé est analysé.

Kaspersky Security permet de réaliser les opérations suivantes :

- Analyser le flux de messagerie entrant et sortant ainsi que les messages stockés sur le serveur Microsoft Exchange (y compris dans les dossiers publics) afin de détecter d'éventuels objets malveillants. Lors de l'analyse, toutes les pièces jointes sont traitées en plus du message. En fonction des paramètres définis, l'application répare ou supprime les objets malveillants découverts et fournit à l'utilisateur toutes les informations à leur sujet.

- Filtrer les messages non sollicités (spam) hors du flux de messagerie. Le composant spécial Anti-Spam analyse le flux de messagerie à la recherche de messages non sollicités. De plus, le composant Anti-Spam permet de créer des listes noire et blanche d'adresses d'expéditeurs et il prend en charge la configuration souple de l'agressivité de la recherche des messages non sollicités.

- Rechercher la présence éventuelle de liens malveillants et de liens de phishing dans le flux de messagerie.

- Créer dans la Sauvegarde des copies de sauvegarde des objets (pièces jointes ou corps du message) et des messages non sollicités avant leur réparation ou leur suppression afin de pouvoir les restaurer ultérieurement, ce qui exclut la possibilité de perdre des informations. Les copies originales peuvent être localisées aisément grâce aux filtres configurables.

- Signaler à l'expéditeur, au destinataire et à l'administrateur de la protection antivirus les messages contenant des objets malveillants.

- Administrer centralement les paramètres identiques dans un groupe de Serveurs de sécurité à l'aide des profils.

- Tenir des journaux des événements, récolter des statistiques et créer des rapports réguliers sur le fonctionnement de l'application. L'application permet créer des rapports manuellement ou selon un horaire défini.

- Configurer les paramètres de fonctionnement de l'application en fonction du volume et des caractéristiques du flux de messagerie et notamment, définir le délai de connexion maximum pour optimiser l'analyse.

- Mettre à jour les bases de Kaspersky Security automatiquement ou selon un horaire défini. Les serveurs FTP et HTTP de mises à jour de Kaspersky Lab sur Internet, un dossier local/de réseau contenant la sélection actuelle de mises à jour ou un serveur FTP ou HTTP défini par l'utilisateur peuvent faire office de source des mises à jour.

- Lancer une analyse programmée des anciens messages (analysés antérieurement) à la recherche de nouveaux virus. Cette analyse est exécutée en arrière-plan et n'a qu'une incidence négligeable sur les performances du serveur de messagerie.

- Offrir la protection contre les virus au niveau de l'espace de sauvegarde sur la base de la liste des espaces à protéger.

**DANS CETTE SECTION DE L'AIDE**

Distribution ..... 15

Configurations logicielle et matérielle ..... 15

# DISTRIBUTION

Vous pouvez acheter Kaspersky Security dans les boutiques en ligne de Kaspersky Lab (par exemple, http://www.kaspersky.fr, section **Boutique en ligne**) ou de nos partenaires.

Kaspersky Security est fourni dans le cadre des applications Kaspersky Security for Mail Servers et Kaspersky Total Security.

Une fois que vous aurez acheté la licence pour Kaspersky Security, vous recevrez un message électronique contenant un lien pour télécharger l'application depuis la boutique en ligne avec le fichier clé de l'application ou vous recevrez un cédérom avec le fichier d'installation de l'application ainsi que la documentation.

Avant de décacheter l'enveloppe contenant le CD, veuillez lire attentivement le contrat de licence.

Pour obtenir de plus amples informations sur les modes d'achat et de livraison de l'application, contactez le service Ventes à l'adresse sales@kaspersky.com.

# CONFIGURATIONS LOGICIELLE ET MATERIELLE

Pour garantir le fonctionnement de Kaspersky Security, l'ordinateur doit répondre aux configurations logicielle et matérielle suivantes.

### Configuration matérielle

La configuration matérielle requise pour l'installation du serveur de sécurité correspond à la configuration matérielle requise pour le serveur Microsoft Exchange protégé. En fonction des paramètres de l'application et du mode d'exploitation de celle-ci, il faudra peut-être prévoir une quantité considérable d'espace disque pour la sauvegarde et autres dossiers de service (selon la configuration par défaut, le dossier de la sauvegarde peut occuper jusqu'à 512 Mo). La console d'administration est installée avec le serveur de sécurité.

La console d'administration peut également être installée indépendamment du serveur de sécurité Configuration matérielle pour l'installation de la console d'administration uniquement :

- Processeur Intel® Pentium® 400 MHz ou supérieur (recommandé : 1 000 MHz) ;
- 256 Mo de mémoire vive disponible ;
- 500 Mo d'espace disque disponible pour l'installation de l'application.

### Configuration logicielle

L'installation du serveur de sécurité nécessite l'un des systèmes d'exploitation suivants :

- Microsoft Windows Server®2012 R2 ;
- Microsoft Windows Server 2012 ;
- Microsoft Small Business Server 2011

- Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 ;
- Microsoft Windows Server 2008 R2 Standard Edition Service Pack 1 ;
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2 ;
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2 ;
- Microsoft Small Business Server 2008 Standard x64 ;
- Microsoft Small Business Server 2008 Premium x64 ;
- Microsoft Essential Business Server 2008 Standard x64 ;
- Microsoft Essential Business Server 2008 Premium x64 ;
- Microsoft Windows Server 2003 x64 R2 Enterprise Edition Service Pack 2 ;
- Microsoft Windows Server 2003 x64 R2 Standard Edition Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Enterprise Edition Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Standard Edition Service Pack 2 ;

La configuration logicielle suivante est requise pour l'installation du serveur de sécurité :

- Un des serveurs de messagerie suivant :
  - Microsoft Exchange Server 2007 x64 Service Pack 3 ou Microsoft Exchange Server 2010 Service Pack 1, déployé dans un des rôles suivants : transport Hub, boîte aux lettres ou transport Edge ;
  - Microsoft Exchange Server 2013, déployé dans le rôle de boîte aux lettres.
- Microsoft .NET Framework 3.5 Service Pack 1.
- Un des SGBD suivants :
  - Microsoft SQL Server® 2012 ;
  - Microsoft SQL Server 2012 Express ;
  - Microsoft SQL Server 2008 R2 Enterprise Edition ;
  - Microsoft SQL Server 2008 R2 Standard Edition ;
  - Microsoft SQL Server 2008 R2 Express Edition ;
  - Microsoft SQL Server 2008 Enterprise Edition ;
  - Microsoft SQL Server 2008 Standard Edition ;
  - Microsoft SQL Server 2008 Express Edition ;
  - Microsoft SQL Server 2005 Enterprise Edition ;
  - Microsoft SQL Server 2005 Standard Edition ;
  - Microsoft SQL Server 2005 Express Edition.

L'installation de la console d'administration requiert un des systèmes d'exploitation suivants :

- Microsoft Windows® 8.1 ;
- Microsoft Windows Server 2012 R2 ;
- Microsoft Windows Server 2012 ;
- Microsoft Windows 8 ;
- Microsoft Windows 8 x64 ;
- Microsoft Small Business Server 2011 ;
- Microsoft Windows 7 Professional ;
- Microsoft Windows 7 Professional x64 ;
- Microsoft Windows 7 Enterprise ;
- Microsoft Windows 7 Enterprise x64 ;
- Microsoft Windows 7 Ultimate ;
- Microsoft Windows 7 Ultimate x64 ;
- Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1 ;
- Microsoft Windows Server 2008 R2 Standard Edition Service Pack 1 ;
- Microsoft Small Business Server 2008 Standard ;
- Microsoft Small Business Server 2008 Premium ;
- Microsoft Essential Business Server 2008 Standard ;
- Microsoft Essential Business Server 2008 Premium ;
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2 ;
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2 ;
- Microsoft Windows Server 2008 Enterprise Edition Service Pack 2 ;
- Microsoft Windows Server 2008 Standard Edition Service Pack 2 ;
- Microsoft Windows Vista® ;
- Microsoft Windows Vista x64 ;
- Microsoft Windows Server 2003 x64 R2 Standard Edition ;
- Microsoft Windows Server 2003 x64 R2 Enterprise Edition ;
- Microsoft Windows Server 2003 R2 Standard Edition ;
- Microsoft Windows Server 2003 R2 Enterprise Edition ;
- Microsoft Windows Server 2003 x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;

- Microsoft Windows XP Service Pack 3 ;
- Microsoft Windows XP x64 Service Pack 2.

La configuration logicielle suivante est requise pour l'installation de la Console d'administration :

- Microsoft Management Console 3.0 ;
- Microsoft .NET Framework 3.5 Service Pack 1.

# ARCHITECTURE DE L'APPLICATION

L'application contient deux composants principaux :

- Le **serveur de sécurité**, installé sur le serveur Microsoft Exchange, qui se charge du filtrage des messages non sollicités dans le trafic de messagerie et de la protection contre les virus. Il intercepte les messages qui arrivent sur le serveur Microsoft Exchange et utilise les modules intégrés Antivirus et Anti-Spam afin de détecter la présence éventuelle de virus et de messages non sollicités. Si le message reçu est infecté ou s'il s'agit d'un message non sollicité, l'application exécute une des actions définies dans les paramètres de l'Anti-Virus ou de l'Anti-Spam.

  Le serveur de sécurité est composé des modules suivants : Intercepteur de messages, Antivirus (cf. page 59), Anti-Spam (cf. page 73), Module d'administration interne de l'application et contrôle de l'intégrité.

- La **Console d'administration** est un composant enfichable isolé spécial intégré à MMC 3.0. La console d'administration permet de composer la liste des serveurs Microsoft Exchange à protéger et d'administrer les serveurs de sécurité. Vous pouvez installer la console d'administration sur le serveur Microsoft Exchange avec le serveur de sécurité ou sur un ordinateur distinct.

Pour que l'application fonctionne correctement, il est également nécessaire d'installer une base de données spéciale gérée par Microsoft SQL Server, appelée *base de données de la sauvegarde et des statistiques* (ci-après, la *base de données*). Dans cette base de données, l'application enregistre les données de sauvegarde et les statistiques de fonctionnement de l'application.

Pour en savoir plus sur l'architecture de l'application, consultez le *Guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Servers*.

# INTERFACE DE L'APPLICATION

La console d'administration assure l'interface d'administration de l'application. Il s'agit d'un composant enfichable isolé spécial intégré à MMC.

### DANS CETTE SECTION DE L'AIDE


Fenêtre principale de la Console d'administration ..... 20

Arborescence de la console d'administration ..... 21

Panneau des résultats ..... 22

Panneau d'accès rapide ..... 22

Menu contextuel ..... 23


# FENETRE PRINCIPALE DE LA CONSOLE D'ADMINISTRATION

La fenêtre principale de la Console d'administration (cf. ill. ci-après) contient les éléments suivants :

- **Menu**. Situé au-dessus de la barre d'outils. Le menu permet d'administrer les fichiers et les fenêtres et offre également l'accès aux fichiers d'aide.
- **Barre d'outils**. Elle se trouve dans la partie supérieure de la fenêtre principale. Les boutons de la barre d'outils offrent un accès direct à quelques-unes des fonctions les plus utilisées de l'application.
- **Arborescence de la console d'administration**. Située dans la partie gauche de la fenêtre principale. L'arborescence de la console d'administration permet de voir les profils, les serveurs de sécurité connectés ainsi que les paramètres de Kaspersky Security. Les profils, les serveurs de sécurité connectés et les paramètres de Kaspersky Security sont présentés sous la forme de nœuds.
- **Panneau des résultats**. Situé dans la partie droite de la fenêtre principale. Le panneau des résultats affiche le contenu du nœud sélectionné dans l'arborescence de la console d'administration.

- **Panneau d'accès rapide**. Situé à droite du panneau des résultats. Le panneau d'accès rapide permet d'exécuter les actions pour le nœud sélectionné.

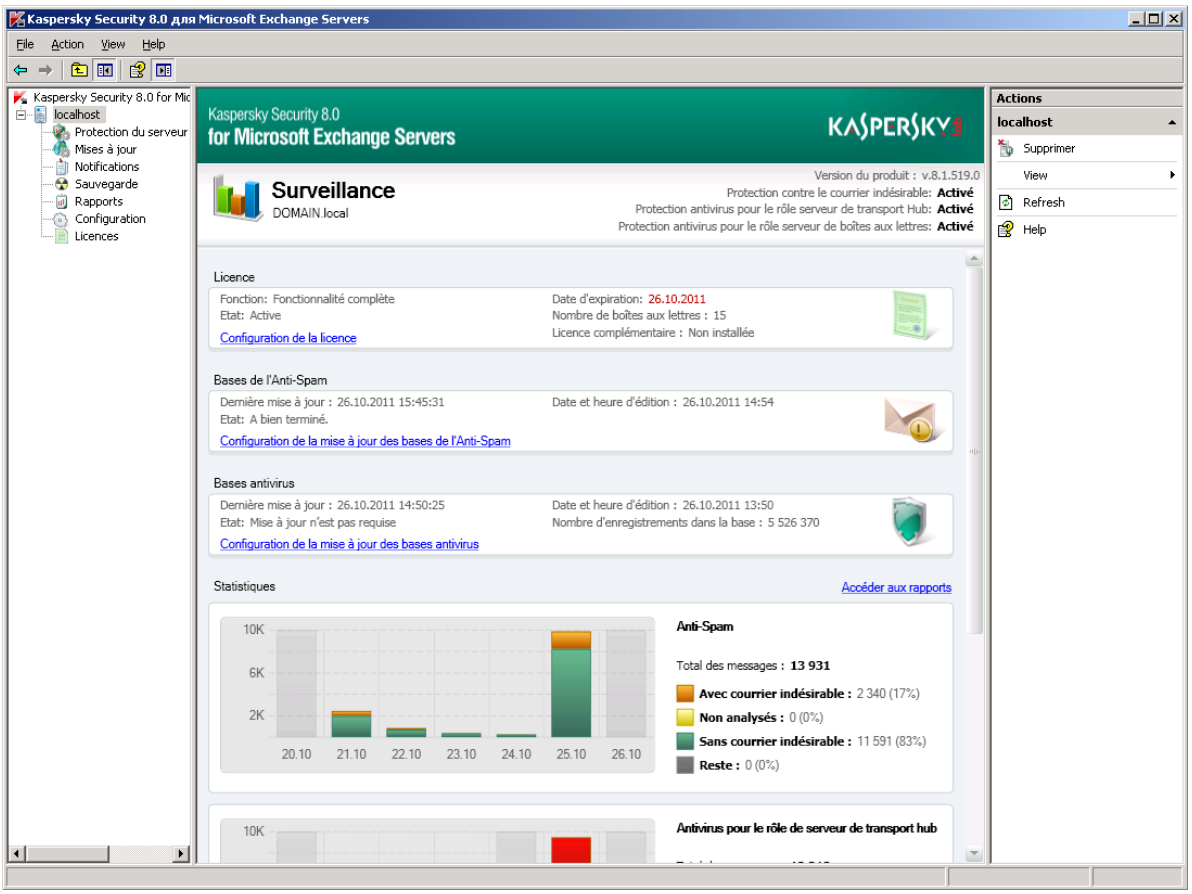


*Figure 1. Fenêtre principale de l'application*

# ARBORESCENCE DE LA CONSOLE D'ADMINISTRATION

L'arborescence de la console d'administration permet d'afficher la structure des profils, des serveurs Microsoft Exchange, ainsi que les nœuds imbriqués pour l'administration des fonctions de l'application.

La console d'administration de Kaspersky Security apparaît dans l'arborescence de la console MMC avec le nœud racine **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Il contient les sous-nœuds **Profils** et **<Nom du serveur>**.

Le nœud **Profils** contient des nœuds portant les noms de tous les nœuds créés dans le profil et qui apparaissent comme **<Nom du profil>**. Chaque nœud **<Nom du profil>** contient le nœud **Serveurs** qui affichent les sous-nœuds portant les noms des serveurs Microsoft Exchange.

Le nœud **<Nom du serveur>** apparaît pour chacun des serveurs Microsoft Exchange protégés auquel la Console d'administration se connecte. Ainsi, l'arborescence de la console d'administration peut contenir plusieurs nœuds portant les noms des serveurs Microsoft Exchange.

Pour chaque nœud **<Nom du profil>**, chaque nœud **<Nom du serveur>** et chaque sous-nœud **<Nom d serveur>** dans le nœud **Serveurs**, l'arborescence de la Console d'administration affiche les sous-nœuds suivants prévus pour l'administration des fonctions de l'application :

- **Protection du serveur** : administration de la protection du flux de messagerie contre les objets malveillants et le courrier indésirable.

- **Mises à jour** : administration des mises à jour des bases de l'application.

- **Notifications** : configuration des paramètres de notification de l'administrateur et d'autres personnes intéressées sur les événements survenus pendant l'utilisation de l'application.
- **Sauvegarde** : configuration des paramètres de Sauvegarde et gestion des objets sauvegardés.
- **Rapports** : configuration des paramètres des rapports sur le fonctionnement de l'application (n'apparaît pas pour les sous-nœuds **<Nom du serveur>** dans le nœud **Serveurs**).
- **Configuration** : configuration des paramètres généraux de fonctionnement de l'application.
- **Licence** : informations sur les clés ajoutées, ajout et suppression de clés.

# PANNEAU DES RESULTATS

Le panneau des résultats reprend des informations relatives à l'état actuel de la protection des serveurs Microsoft Exchange, des informations relatives à Kaspersky Security et les paramètres de fonctionnement de l'application.

L'apparence du panneau des résultats dépend du nœud sélectionné dans l'arborescence de la console d'administration.

# PANNEAU D'ACCES RAPIDE

La sélection de liens présentés dans le panneau d'accès rapide dépend du nœud sélectionné dans l'arborescence de la Console d'administration. Outre les liens standards de la console MMC, le panneau d'accès rapide propose également des liens qui permettent de manipuler le nœud sélectionné (cf. tableau ci-après).

*Table 2. Liens du panneau d'accès rapide*

| NŒUD | LIEN | FONCTION DU LIEN |
|---|---|---|
| **Kaspersky Security 8.0 for Microsoft Exchange Servers** | **Se connecter au serveur** | La fenêtre **Se connecter au serveur** s'ouvre. |
| | **Activer le diagnostic du composant enfichable** | Active la journalisation dans la console d'administration. |
| **Profils** | **Ajouter le profil** | Ouvre la fenêtre **Créer un profil**. |
| **<nom du profil>** | **Ajouter un serveur** | Ouvre l'Assistant d'ajout d'un serveur de sécurité au profil |
| | **Renommer** | Ouvre la fenêtre **Donner un autre nom au profil**. |
| | **Supprimer** | Supprime le profil. |
| **Serveurs** | **Ajouter un serveur** | Ouvre l'Assistant d'ajout d'un serveur de sécurité au profil |
| **Profils → <nom du serveur de sécurité>** | **Supprimer du profil** | Supprime le serveur de sécurité du profil. |
| **Kaspersky Security 8.0 for Microsoft Exchange Servers → <nom du serveur de sécurité>** | **Supprimer le serveur** | Supprime le serveur de sécurité de l'arborescence de la console d'administration |
| **Mise à jour** | **Mettre à jour les bases de l'Antivirus** | Mise à jour des bases de l'Antivirus. |
| | **Mettre à jour les bases de l'Anti-Spam** | Mise à jour des bases de l'Anti-Spam |
| **Notifications** | **Paramètres d'envoi des notifications** | Ouvre la fenêtre **Paramètres d'envoi des notifications**. |

# MENU CONTEXUEL

Chaque catégorie de nœud de l'arborescence de la console d'administration possède son propre menu contextuel qui s'ouvre d'un clic droit de la souris.

Outre les options standards du menu contextuel de la console MMC, vous y retrouverez également des options qui permettent de manipuler le nœud sélectionné (cf. tableau ci-après).

*Table 3. Options du menu contextuel des nœuds de la console d'administration*

| NŒUD | COMMANDE DU MENU | FONCTION |
|---|---|---|
| **Kaspersky Security 8.0 for Microsoft Exchange Servers** | **Se connecter au serveur** | La fenêtre **Se connecter au serveur** s'ouvre. |
| | **Activer le diagnostic du composant enfichable** | Active la journalisation dans la console d'administration. |
| **Profils** | **Ajouter le profil** | Ouvre la fenêtre **Créer un profil**. |
| **<nom du profil>** | **Ajouter un serveur** | Ouvre l'Assistant d'ajout d'un serveur de sécurité au profil |
| | **Renommer** | Ouvre la fenêtre **Donner un autre nom au profil**. |
| | **Supprimer** | Supprime le profil. |
| **Serveurs** | **Ajouter un serveur** | Ouvre l'Assistant d'ajout d'un serveur de sécurité au profil |
| **Profils → <nom du serveur de sécurité>** | **Supprimer du profil** | Supprime le serveur de sécurité du profil. |
| **Kaspersky Security 8.0 for Microsoft Exchange Servers → <nom du serveur de sécurité>** | **Supprimer le serveur** | Supprime le serveur de sécurité de l'arborescence de la console d'administration |
| **Mise à jour** | **Mettre à jour les bases de l'Antivirus** | Mise à jour des bases de l'Antivirus. |
| | **Mettre à jour les bases de l'Anti-Spam** | Mise à jour des bases de l'Anti-Spam |
| **Notifications** | **Paramètres d'envoi des notifications** | Ouvre la fenêtre **Paramètres d'envoi des notifications**. |

# OCTROI DES LICENCES POUR L'APPLICATION

Cette section aborde les principales notions liées à l'activation de l'application. Cette section explique le rôle du contrat de licence, les modes d'activation de l'application et le renouvellement de la licence.

Vous y trouverez également les instructions sur l'utilisation des clés, la configuration des notifications de l'expiration prochaine de la licence et sur la création de la liste des boîtes aux lettres et des référentiels protégés.

### DANS CETTE SECTION DE L'AIDE


Présentation du contrat de licence ..... 24

Présentation de la licence ..... 24

Schémas d'octroi des licences ..... 25

Présentation du fichier clé ..... 25

Présentation de la divulgation des données ..... 26

Ajout d'une clé ..... 27

Consultation des informations relatives aux clés ..... 28

Remplacement d'une clé ..... 29

Suppression d'une clé ..... 29

Configuration de la notification sur l'expiration de la durée de validité de la licence ..... 30

Particularités de la licence pour les serveurs de sécurité du profil ..... 31


## PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est l'accord légal conclu entre vous et 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.

La confirmation de votre accord avec le texte du Contrat de licence lors de l'installation vaut acceptation des conditions de ce dernier. Si vous rejetez les termes du contrat, vous devez interrompre l'installation de l'application ou arrêter d'utiliser celle-ci.

## PRESENTATION DE LA LICENCE

*La licence* est un droit limité dans le temps pour l'utilisation de l'application octroyé dans le cadre d'un contrat de licence.

La licence donne droit aux services suivants :

- Utilisation de l'application pour la protection d'un nombre déterminé de boîtes aux lettres.

- Recours au service d'assistance technique de Kaspersky Lab.
- Accès à divers services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence.

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

Il existe différents types de licence :

- *Evaluation* : licence gratuite qui permet de découvrir les fonctions de l'application.

  La durée de validité de ce genre de licence est en général assez courte. Une fois que la validité de la licence d'évaluation est écoulée, Kaspersky Security arrête de remplir toutes ses fonctions. Pour pouvoir continuer à utiliser l'application, vous devez acheter une licence commerciale.

- *Commerciale* : licence payante octroyée suite à l'achat de l'application.

  Une fois la licence commerciale expirée, l'application continue à fonctionner, mais avec certaines restrictions. Vous pouvez continuer à utiliser tous les composants de l'application, mais uniquement avec les bases installée avant l'expiration de la licence. Pour pouvoir continuer à profiter de toutes les fonctions de Kaspersky Security, il faut renouveler la licence commerciale.

  Il est conseillé de renouveler la licence avant son expiration afin de garantir la protection maximum contre toutes les menaces informatiques et le courrier indésirable.

# ORGANISATION DE LA LICENCE

En fonction du mode de déploiement de l'application, vous devez ajouter les clés selon le mode d'octroi des licences suivant :

- Si l'application est utilisée sur des serveurs Microsoft Exchange indépendants, il faut ajouter une clé distincte pour chaque serveur.
- Si l'application est utilisée dans une grappe de serveurs Microsoft Exchange, il suffit d'installer une seule clé qui sera valide pour l'ensemble de la grappe.
- Si l'application est utilisée sur des serveurs Microsoft Exchange qui appartiennent à un DAG, il suffit d'ajouter une clé qui sera valide pour l'ensemble du DAG.
- Si vous administrez plusieurs serveurs de sécurité via un profil, il faut ajouter une clé pour un profil dont l'action couvre tous les serveurs de sécurité du profil (cf. section "Particularités de la licence pour les serveurs de sécurité du profil" à la page 31).

# PRESENTATION DU FICHIER CLE

*Le fichier clé* est un fichier du type xxxxxxx.key. Vous ne pouvez pas utiliser l'application sans fichier de clé.

Il reprend les informations suivantes :

- Clé : séquence unique de caractères alphanumériques. La clé sert par exemple pour obtenir l'assistance technique de Kaspersky Lab.
- Date de création du fichier clé.
- Durée de validité de la licence – Durée d'utilisation du logiciel indiquée sur le certificat de licence.

  La durée de validité de la licence n'expire pas après la validité du fichier clé utilisé pour activer l'application.

- Durée de validité du fichier clé : période définie à partir de la date de création du fichier clé.. La durée de validité du fichier clé peut être de plusieurs années. Vous pouvez utiliser l'application à l'aide de cette clé uniquement avant l'expiration de ce délai.

# PRESENTATION DE LA DIVULGATION DES DONNEES

Si vous acceptez de rejoindre le Kaspersky Security Network (cf. section "Présentation de la participation au Kaspersky Security Network" à la page 61), Kaspersky Lab recevra automatiquement les informations suivantes suite à l'utilisation de Kaspersky Security sur l'ordinateur :

- nom de l'application ;
- type d'application ;
- version de l'application ;
- identifiant de l'installation de l'application ;
- version du système d'exploitation ;
- version du paquet de mise à jour du système d'exploitation ;
- langue du système d'exploitation ;
- adresse IP du serveur de Microsoft Exchange sur lequel Kaspersky Security est installé ;
- adresse IP de l'expéditeur du message potentiellement infecté ;
- somme de contrôle (MD5) des adresses électroniques de l'expéditeur du message potentiellement infecté ;
- URL ou adresse IP (au format IPv4 et iPV6) du lien de phishing ;
- URL ou adresse IP (au format IPv4 et IPv6) du lien de phishing ;
- sommes de contrôle (MD5) des objets graphiques du message ;
- sommes de contrôle (MD5) des noms des fichiers joints au message ;
- date et heure de diffusion des bases de l'Antivirus ;
- informations du module Antivirus sur l'état de l'analyse du message ;
- informations du module Anti-Phishing sur l'état de l'analyse, y compris la valeur du niveau de confiance, la pondération et l'état ;
- la cible de l'attaque de phishing (nom court de l'organisation, adresse du site Internet) ;
- état de l'analyse du module Anti-Spam ;
- catégories identifiées de la base de filtrage du contenu du module Anti-Spam (sujet défini par l'application auquel appartient le texte) ;
- informations techniques liées au mode de détection de l'application d'un message potentiellement infecté ;
- informations techniques liées au mode de détection par l'application d'un message potentiellement indésirable ;
- brèves signatures textuelles sur le texte du message pour le filtrage des diffusions de messages non sollicités connues et la solution de l'application à leur sujet.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Kaspersky Lab utilise les informations obtenues uniquement sous forme de statistiques générales. Les statistiques générales sont créées de manière automatique à partir des infirmations initiales obtenues et ne contiennent pas de données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme cryptée et sont supprimées au fur et à mesure de leur accumulation (deux fois par an). Les données des statistiques générales sont conservées de manière illimitée.

La participation au Kaspersky Security Network est volontaire. Vous pouvez à tout moment vous retirer du Kaspersky Security Network (cf. section "Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing" à la page 78). Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour connaître les données que l'application transmet dans le cadre du Kaspersky Security Network, lisez le Règlement du KSN (cf. section "Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing" à la page 78).

# AJOUT D'UNE CLE

Vous pouvez ajouter une clé séparément pour le serveur de sécurité ou ajouter une clé pour un profil pour que la licence couvre tous les serveurs de sécurité du profil (cf. section "Particularités de la licence des serveurs de sécurité du profil" à la page 31).

Si Kaspersky Security fonctionne dans une configuration avec un cluster de serveur ou un DAG, il suffit d'ajouter une clé pour tout le cluster ou tout le DAG. Vous pouvez l'ajouter en connectant la console d'administration à n'importe quel des serveurs du cluster ou du DAG.

*Pour ajouter une clé pour le serveur de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez l'entrée **Licence**.
3. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez ajouter une clé active, cliquez sur **Ajouter** dans le groupe **Clé active**.
   - Si vous souhaitez ajouter une clé complémentaire, cliquez sur **Ajouter** dans la section **Clé complémentaire**.

   Une clé complémentaire ne peut être ajoutée que si une clé active existe.

   La clé complémentaire doit être une clé pour une licence commerciale. Il est impossible d'ajouter une clé pour licence d'évaluation en tant que clé complémentaire.
4. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Nom du fichier** le chemin d'accès au fichier clé (fichier portant l'extension *.key), puis cliquez sur le bouton **Ouvrir**.

La clé est ajoutée et les informations qui la concernent apparaissent dans le groupe adéquat.

*Pour ajouter une clé, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Développez le nœud du profil auquel vous souhaitez ajouter une clé.
3. Sélectionnez l'entrée **Licence**.
4. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez ajouter une clé active, cliquez sur **Ajouter** dans le groupe **Clé active**.

- Si vous souhaitez ajouter une clé complémentaire, cliquez sur **Ajouter** dans le groupe **Clé complémentaire**.

Une clé complémentaire ne peut être ajoutée que si une clé active existe.

La clé complémentaire doit être une clé pour une licence commerciale. Il est impossible d'ajouter une clé pour licence d'évaluation en tant que clé complémentaire.

5. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Nom du fichier** le chemin d'accès au fichier clé (fichier portant l'extension *.key), puis cliquez sur le bouton **Ouvrir**.

La clé est ajoutée et les informations qui la concernent apparaissent dans le groupe adéquat.

# CONSULTATION DES INFORMATIONS RELATIVES AUX CLES

*Pour consulter les informations relatives aux clés ajoutées pour le serveur de sécurité ou un profil, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - Si vous souhaitez consulter les informations relatives aux clés ajoutées pour le serveur de sécurité, déployez le nœud du Serveur de sécurité dont vous souhaitez consulter les informations de la clé.

   - Si vous souhaitez consulter les informations relatives aux clés du profil, développez le nœud **Profils**, puis le nœud du profil dont vous souhaitez consulter les informations de la clé.

2. Sélectionnez l'entrée **Licence**.

Le panneau des résultats affiche les informations suivantes sur la clé :

- **Etat**. Peut avoir une des valeurs suivantes :

  - Licence active. La validité de la licence n'est pas écoulée, les fonctionnalités de la licence ne sont pas restreintes.

  - Durée de validité de la licence d'évaluation écoulée. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.

  - La durée de validité de la licence a expiré. La durée de validité de la licence est écoulée, la mise à jour est interdite, la participation à KSN est inaccessible (cf. section "Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable" à la page 75).

  - Les bases sont corrompues. Les bases de l'Antivirus et de l'Anti-Spam manquent ou sont endommagées.

  - La clé est absente. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.

  - La clé a été bloquée. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.

  - La liste noire des clés est endommagée ou introuvable. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.

- **Clé**. Séquence unique de caractères alphanumériques.

- **Type de licence**. Le type de licence (évaluation, commerciale).

- **Représentant**. Contact au sein de l'organisation qui a accepté le contrat de licence.
- **Nombre d'utilisateurs**. Nombre maximal d'utilisateurs de l'application dont les boîtes aux lettres peuvent être protégées par l'application avec cette clé.
- **Date d'expiration**. Fin de validité de la licence.

# REMPLACEMENT D'UNE CLE

*Pour remplacer une clé ajoutée pour le serveur de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez l'entrée **Licence**.
3. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez remplacer une clé active, cliquez sur **Remplacer** dans la section **Clé active**.
   - Si vous souhaitez remplacer une clé complémentaire, cliquez sur **Remplacer** dans la section **Clé complémentaire**.
4. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Nom du fichier** le chemin d'accès au fichier clé (fichier portant l'extension *.key), puis cliquez sur le bouton **Ouvrir**.

La clé est ajoutée et les informations qui la concernent apparaissent dans le groupe adéquat.

*Pour remplacer une clé ajoutée pour un profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Développez le nœud du profil dont vous souhaitez remplacer la clé.
3. Sélectionnez l'entrée **Licence**.
4. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez remplacer une clé active, cliquez sur **Remplacer** dans la section **Clé active**.
   - Si vous souhaitez remplacer une clé complémentaire, cliquez sur **Remplacer** dans la section **Clé complémentaire**.
5. Dans la fenêtre qui s'ouvre, indiquez dans le champ **Nom du fichier** le chemin d'accès au fichier clé (fichier portant l'extension *.key), puis cliquez sur le bouton **Ouvrir**.

La clé est ajoutée et les informations qui la concernent apparaissent dans le groupe adéquat.

# SUPPRESSION D'UNE CLE

*Pour supprimer une clé ajoutée pour le serveur de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez l'entrée **Licence**.
3. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez supprimer la clé active, cliquez sur **Supprimer** dans le groupe **Clé active**.

- Si vous souhaitez supprimer la clé complémentaire, cliquez sur **Supprimer** dans le groupe **Clé complémentaire**.

L'application supprime la clé sélectionnée. Quand la clé active est supprimée, la clé complémentaire (si elle existe) devient la clé active.

*Pour supprimer une clé ajoutée pour un profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Développez le nœud du profil dont vous souhaitez supprimer la clé.
3. Sélectionnez l'entrée **Licence**.
4. Dans le panneau des résultats, exécutez une des actions suivantes :
   - Si vous souhaitez supprimer la clé active, cliquez sur **Supprimer** dans le groupe **Clé active**.
   - Si vous souhaitez supprimer la clé complémentaire, cliquez sur **Supprimer** dans le groupe **Clé complémentaire**.

L'application supprime la clé sélectionnée. Quand la clé active est supprimée, la clé complémentaire (si elle existe) devient la clé active.

Le remplacement automatique de la clé active par la clé complémentaire à l'expiration de la licence, à compter de la date d'ajout de la clé active, est réalisé sur chacun des serveurs de sécurité du profil selon la date et l'heure du serveur physique sur lequel le Serveur de sécurité est installé.

# CONFIGURATION DE LA NOTIFICATION SUR L'EXPIRATION DE LA DUREE DE VALIDITE DE LA LICENCE

Après chaque mise à jour des bases, l'application vérifie la licence active. Si l'application définit que la licence arrive bientôt à échéance, elle ajoute une entrée à ce sujet dans le journal de l'application et commence à envoyer des notifications à l'adresse de messagerie reprise dans les paramètres des notifications.(cf. rubrique "Configuration des paramètres de notification" à la page 97). Par défaut, l'application commence à envoyer des notifications à partir de 15 jours avant l'expiration de la licence. Vous pouvez modifier le nombre de jours à partir duquel ces notifications seront envoyées.

*Pour configurer les paramètres de notification sur l'expiration de la licence du serveur de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez l'entrée **Licence**.
3. Dans la partie inférieure du panneau des résultats, indiquez le nombre de jours avant l'expiration de la licence à partir de quand vous souhaitez recevoir les notifications pour le paramètre **Signaler l'expiration de la durée de validité de licence**.
4. Cliquez sur le bouton **Enregistrer**.

*Pour configurer les paramètres de notification sur l'expiration de la licence pour le profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer la notification relative à l'expiration de la validité de la licence.
3. Sélectionnez l'entrée **Licence**.

4. Dans la partie inférieure du panneau des résultats, indiquez le nombre de jours avant l'expiration de la licence à partir de quand vous souhaitez recevoir les notifications pour le paramètre **Signaler l'expiration de la durée de validité de licence**.

5. Cliquez sur le bouton **Enregistrer**.

# PARTICULARITES DE LA LICENCE POUR LES SERVEURS DE SECURITE DU PROFIL

Au moment d'utiliser les profils, vous devez tenir compte des particularités suivantes des licences pour les Serveurs de sécurité ajoutés au profil :

- Le remplacement automatique de la clé active par la clé complémentaire à l'expiration de la licence, à compter de la date d'ajout de la clé active, est réalisé sur chacun des serveurs de sécurité du profil selon la date et l'heure du serveur physique sur lequel le Serveur de sécurité est installé. C'est élément est à prendre en compte si, par exemple, les serveurs de sécurité du profil se trouvent dans des fuseaux horaires distincts.

- Dans la console d'administration, panneau des résultats du nœud **Profils → <nom du profil> → Licence**, les clés et les dates d'expiration des licences pour chacune des clés ajoutées sont affichées selon l'heure de la console d'administration. Si, selon la date et l'heure du serveur d'administration, la licence a expiré, conformément à la clé active, et qu'une clé complémentaire avait été ajoutée, seule cette clé complémentaire et ses propriétés apparaissent dans le panneau des résultats.

- Vous ne pouvez pas ajouter, remplacer ou supprimer une clé séparément pour un serveur de sécurité ajouté au profil. Vous pouvez ajouter, remplacer ou supprimer une clé uniquement pour l'ensemble du profil et cette licence touche tous les serveurs de sécurité du profil.

- Une fois qu'un serveur de sécurité a été ajouté à un profil, il est couvert par la licence au niveau du profil, même si une autre licence était active pour ce serveur de sécurité avant son ajout au profil. La clé active du Serveur de sécurité est remplacée par la clé active du profil.

- Après la suppression d'un serveur de sécurité d'un profil, il est toujours couvert par la licence au niveau du profil d'où il a été supprimé. Dans ce cas, la clé active du profil pour ce Serveur de sécurité est toujours affichée dans le volet des résultats du nœud **Licence**.

# LANCEMENT ET ARRET DE L'APPLICATION

Kaspersky Security démarre automatiquement lorsque le serveur Microsoft Exchange est lancé, au démarrage de Microsoft Windows sur le serveur sur lequel le serveur de sécurité est installé, lors du passage du premier message via le serveur Microsoft Exchange ainsi que lors de la connexion de la console d'administration au serveur de sécurité installé sur le serveur Microsoft Exchange. Si la protection du serveur Microsoft Exchange est activée au moment de l'installation, l'analyse antivirus et antispam du flux de messagerie est lancée et arrêtée en même temps que le lancement et l'arrêt du serveur Microsoft Exchange.

Vous pouvez activer et désactiver séparément la protection antivirus du serveur Microsoft Exchange dans le rôle de boîte aux lettres et de transport hub et la protection du serveur Microsoft Exchange contre le courrier indésirable.

- *Pour arrêter l'application, procédez comme suit :*

1. Dans la console d'administration, désactivez la protection antivirus (cf. section "Activation et désactivation de la protection antivirus du serveur à la page 61) et la protection contre le courrier indésirable (cf. section "Activation et désactivation de la protection antispam" à la page 77).

2. Sur l'ordinateur où est installé le serveur de sécurité, utilisez les méthodes standard du système d'exploitation Windows pour arrêter le service *Kaspersky Security 8.0 for Microsoft Exchange Servers* et définissez pour celui-ci le type de lancement **Désactivé**.

- *Pour lancer l'application après l'arrêt, procédez comme suit :*

1. Lancez le service *Kaspersky Security 8.0 for Microsoft Exchange Servers* via les outils du système d'exploitation Windows.

2. Confirmez que sur l'ordinateur où est installé le serveur de sécurité, le type de lancement *Automatique* est défini pour le service **Kaspersky Security 8.0 for Microsoft Exchange Servers** dans le système d'exploitation Windows.

3. Dans la console d'administration, activez la protection antivirus (cf. section "Activation et désactivation de la protection antivirus du serveur à la page 61) et la protection contre le courrier indésirable (cf. section "Activation et désactivation de la protection antispam" à la page 77).

# CONSULTATION DE L'ETAT DE LA PROTECTION DU SERVEUR

Cette section présente les paramètres de fonctionnement par défaut de Kaspersky Security. Elle explique également comment utiliser la Console d'administration afin d'obtenir des informations sur la licence de l'application, sur l'état des modules et des bases de l'application ainsi que des statistiques sur les messages traités et le nombre de menaces et de messages non sollicités.

### DANS CETTE SECTION DE L'AIDE


Protection par défaut du serveur Microsoft Exchange ..... 33

Consultation des informations relatives à l'état de la protection du serveur Microsoft Exchange ..... 34

Consultation des informations relatives à l'état de la protection du profil ..... 39


# PROTECTION PAR DEFAUT DU SERVEUR MICROSOFT EXCHANGE

La protection du serveur Microsoft Exchange contre les programmes malveillants et le courrier indésirable est opérationnelle directement après l'installation du module Serveur de sécurité, à condition qu'il n'ait pas été désactivé dans l'Assistant de configuration de l'application (cf. *Guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Servers*).

Le mode de fonctionnement de l'application suivant est adopté par défaut :

- L'application recherche la présence éventuelle de tous les programmes malveillants repris dans les bases de l'Antivirus dans les messages selon les paramètres suivants :
  - l'application analyse porte sur le corps du message et les objets joints de n'importe quel format, à l'exception des archives et des objets conteneurs au-delà du 32ème niveau d'imbrication.
  - L'application analyse toutes les banques de dossiers publics et toutes les banques de boîtes aux lettres.
  - La sélection de l'action en cas de découverte d'un objet infecté dépend du rôle de serveur Microsoft Exchange déployé sur lequel l'objet a été découvert :
    - En cas de découverte d'un objet infecté sur un serveur Microsoft Exchange dans le rôle transport Hub ou transport Edge, l'objet est supprimé automatiquement et l'application conserve une copie de sauvegarde du message dans la sauvegarde et la note [Malicious object deleted] est ajoutée à l'objet du message.
    - En cas de découverte d'un objet infecté sur un serveur Microsoft Exchange dans le rôle de boîte aux lettres, l'application conserve la copie d'origine de l'objet (pièce jointe ou contenu du message) dans la sauvegarde et tente de le réparer. Si la réparation n'est pas possible, l'application supprime l'objet et le remplace par un fichier texte contenant le message suivant :

      L'objet malveillant <nom_virus> a été découvert. Le fichier (<nom_objet>) a été supprimé par Kaspersky Security 8.0 for Microsoft Exchange Servers. Nom du serveur: <nom_du_serveur>
  - L'application ignore tout objet protégé par un mot de passe ou endommagé. Si vous avez configuré la suppression d'un objet ou la suppression d'un message en cas de détection de ces catégories d'objet, l'application supprime le message et conserve sa copie originale dans la sauvegarde.

- L'application recherche d'éventuels messages non sollicités selon les paramètres suivants :

  - L'application recherche les messages non sollicités selon un niveau d'agressivité faible. Ce niveau offre la combinaison optimale de rapidité et de qualité de l'analyse.

  - L'application ignore tous les messages, mais dans le cas des messages auxquels sont attribués les états *Courrier indésirable*, *Courrier indésirable potentiel*, *Envois massifs* ou *Expéditeur interdit*, les notes [!!SPAM], [!!Probable Spam], [!!Mass Mail] et [!!Blacklisted] sont respectivement ajoutées à l'objet des messages.

  - Durée maximale d'analyse des messages : 30 secondes

  - La taille maximale du message à analyser avec les pièces jointes est de 1536 Ko (1,5 Mo).

  - Les services externes d'analyse des adresses IP et des URL sont utilisés : DNSBL et SURBL (cf. section "Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable" à la page 75). Ces services permettent de filtrer le courrier indésirable à l'aide de listes noires diffusées d'adresses IP et d'URL.

  - Si vous avez activé l'utilisation de KSN dans l'Assistant de configuration de l'application, les services KSN et Reputation Filtering sont activés. Dans le cas contraire, l'utilisation des services KSN et Reputation Filtering est désactivée.

  - Si vous avez activé l'utilisation du service Enforced Anti-Spam Updates Service dans l'Assistant de configuration de l'application, l'utilisation du service Enforced Anti-Spam Updates Service est activée. Dans le cas contraire, l'utilisation du service Enforced Anti-Spam Updates Service est désactivée.

- Si vous aviez activé la fonction de mise à jour des bases de l'application dans l'Assistant de configuration de l'application, les bases seront mises à jour régulièrement depuis les serveurs de mise à jour de Kaspersky Lab (la fréquence peut être d'une fois par heure pour les bases de l'Antivirus ou d'une fois toutes les cinq minutes pour les bases de l'Anti-Spam).

# CONSULTATION DES INFORMATIONS RELATIVES A L'ETAT DE LA PROTECTION DU SERVEUR MICROSOFT EXCHANGE

*Pour consulter les informations relatives à l'état de la protection du serveur Microsoft Exchange, procédez comme suit :*

1. Lancez la console d'administration via le menu **Démarrer → Programmes → Kaspersky Security 8.0 for Microsoft Exchange Servers → Console d'administration**.

2. Dans l'arborescence de la console d'administration, sélectionner le serveur de sécurité installé sur le serveur Microsoft Exchange dont vous souhaitez consulter l'état.

Le panneau des résultats du nœud sélectionné du serveur de sécurité affiche les informations suivantes sur l'état de la protection du serveur :

- Le groupe **Profil** affiche les informations relatives à la configuration des paramètres du Serveur de sécurité à l'aide des profils.

- Le groupe paramètres **Informations sur l'application** reprend les informations relatives au serveur Microsoft Exchange et aux modules de l'application :

- **Nom du serveur**.

  Le nom du serveur peut avoir les valeurs suivantes :

  - Nom du serveur physique, si la console d'administration est connectée au serveur de sécurité installée sur un serveur Microsoft Exchange distinct, un nœud passif du cluster ou un serveur appartenant au DAG.
  - Nom du serveur virtuel si la console d'administration est connectée à un serveur virtuel ou à son nœud actif.

- **Informations sur le schéma de déploiement de l'application**.

  Le champ prend une des valeurs suivantes :

  - **Serveur virtuel**, si la console d'administration est connectée à un serveur virtuel Microsoft Exchange ou à son nœud actif.
  - **<Nom du DAG>**, si la console d'administration est connectée à un Serveur de sécurité installé sur un serveur Microsoft Exchange dans un DAG.

- **Version**.

  Informations relatives à la version installée de l'application.

- **Module Anti-Spam**.

  Etat du module Anti-Spam. S'affiche si le serveur Microsoft Exchange est déployé dans le rôle Transport Hub ou Transport Edge. Peut avoir une des valeurs suivantes :

  - **Désactivé** : le module Anti-Spam est activé, le contrôle de la messagerie contre le courrier indésirable est désactivé.
  - **Hors-service** : le module Anti-Spam est installé, le contrôle de la messagerie contre le courrier indésirable est activé, mais le module Anti-Spam ne recherche pas les messages non sollicités potentiels en raison d'une erreur de licence, d'une erreur dans les bases ou d'une erreur d'analyse.
  - **Pas installé** : le module Anti-Spam n'est pas installé.
  - **Activé** : le module Anti-Spam fonctionne, le contrôle de la messagerie contre le courrier indésirable est activé et le module Anti-Spam recherche la présence d'éventuels messages non sollicités.

- **Module Antivirus pour le rôle de serveur de transport hub**.

  Etat du module Antivirus pour le rôle Transport Hub. S'affiche si le serveur Microsoft Exchange est déployé dans le rôle Transport Hub ou Transport Edge. Peut avoir une des valeurs suivantes :

  - **Désactivé** : le module Antivirus pour le rôle de serveur de transport hub ou transport edge est installé, la protection antivirus du rôle serveur de transport Hub est désactivée.
  - **Hors service** : le module Antivirus pour le rôle de serveur de transport hub ou transport edge est installé, la protection antivirus du rôle serveur de transport Hub est activée, mais le module Antivirus ne recherche pas la présence éventuelle de virus ou d'autres menaces en raison d'une erreur de licence, d'une erreur dans les bases ou d'une erreur d'analyse.
  - **Pas installé** : le module Antivirus pour le rôle de serveur de transport hub ou de transport edge n'est pas installé.
  - **En service** : le module Antivirus pour le rôle de serveur de transport hub ou transport edge est installé, la protection antivirus du rôle serveur de transport Hub est activée et le module Antivirus recherche la présence éventuelle de virus et autres menaces.

- **Module Antivirus pour le rôle serveur de boîtes aux lettres**.

  Etat du module Antivirus pour le rôle Boîte aux lettres. S'affiche si le serveur Microsoft Exchange est déployé dans le rôle Boîte aux lettres. Peut avoir une des valeurs suivantes :

  - **Désactivé** : le module Antivirus pour le rôle serveur de boîtes aux lettres est installé, la case **Activer la protection antivirus du rôle serveur de boîtes aux lettres** n'est pas cochée.
  - **Hors service** : le module Antivirus pour le rôle de serveur de boîte aux lettres est installé, la case **Activer la protection antivirus du rôle serveur de boîtes aux lettres** est cochée, mais le module Antivirus ne recherche pas la présence éventuelle de virus ou d'autres menaces en raison

d'une erreur de licence, d'une erreur dans les bases ou d'une erreur d'analyse.

- **Pas installé** : le module Antivirus pour le rôle de serveur de boîte aux lettres n'est pas installé.
- **En service** : le module Antivirus pour le rôle de serveur de boîte aux lettres est installé, la case **Activer la protection antivirus du rôle serveur de boîtes aux lettres** est cochée et le module Antivirus recherche la présence éventuelle de virus et autres menaces

La sélection de champs qui affichent l'état des modules du Serveur de sécurité peut être réduite en fonction de la configuration du serveur Microsoft Exchange. Si un champ correspondant à un module ne s'affiche pas, cela signifie que ce dernier n'est peut-être pas installé dans cette configuration du serveur Microsoft Exchange.

Si le serveur SQL est inaccessible, les **informations relatives à l'erreur de connexion au serveur SQL apparaissent dans le groupe de paramètres** Informations sur l'application

Le lien **Passer à la configuration de la protection du serveur** ouvre le panneau des résultats du nœud **Protection du serveur**.

- Le groupe de paramètres **Licence** reprend les informations relatives à a licence :
  - **Fonction**.

    Niveau de fonctionnalité de l'application, défini par la licence active. Peut avoir une des valeurs suivantes :

    - Fonctionnalité complète.
    - La durée de validité de la licence a expiré. La mise à jour des bases est interdite, l'utilisation de KSN n'est pas disponible.
    - Uniquement les mises à jour.
    - Uniquement l'administration.
  - **Etat**.

    Peut avoir une des valeurs suivantes :

    - Licence active. La fonctionnalité de l'application est illimitée.
    - Durée de validité de la licence d'évaluation écoulée. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.
    - La durée de validité de la licence a expiré. La mise à jour est interdite, l'utilisation de KSN n'est pas disponible.
    - Les bases sont corrompues. Les bases de l'Antivirus et de l'Anti-Spam manquent ou sont endommagées.
    - La clé est absente. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.
    - La clé a été bloquée. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.
    - La liste noire des clés est endommagée ou introuvable. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.

  Si le champ **Etat** affiche une valeur autre que *Licence active*, le groupe **Licence** est mis en évidence en rouge. Dans ce cas, il faut ajouter une clé active(cf. section «Ajout d'une clé» à la page 27), en accédant au nœud **Licence** via le lien **Passer à l'administration des clés**.

  - **Date d'expiration**.

    Fin de validité de la licence.

Si le champ **Date d'expiration** est mis en évidence en rouge, il faut renouveler la licence, par exemple en ajoutant une clé complémentaire (cf. section "Ajout d'une clé" à la page 27), en accédant au nœud **Licence** via le lien **Passer à l'administration des clés**.

La période précédant l'expiration de la licence pendant laquelle le champ est mis en évidence en rouge est définie par le paramètre **Signaler l'expiration de la durée de validité de licence : X jours** (cf. section "**Configuration de la notification sur l'expiration de la durée de validité de la licence**" à la page 30) situé dans le volet des résultats du nœud **Licence**. Cette limite est fixée par défaut à 15 jours.

- **Nombre d'utilisateurs**.

  Nombre maximal d'utilisateurs dont les boîtes aux lettres peuvent être protégées par l'application avec cette clé.

- **Clé complémentaire**.

  Informations relatives à la présence d'une clé complémentaire : **Ajoutée** ou **Absente**.

Le lien **Passer à l'administration des clés** ouvre le panneau des résultats du nœud **Licence** où il est possible d'ajouter ou de supprimer des clés.

- Le groupe de paramètres **Bases de l'Anti-Spam** affiche les informations sur l'état des bases de l'Anti-Spam :

  - **Dernière mise à jour**.

    Date de la dernière mise à jour des bases de l'Anti-Spam.

  - **Etat**.

    Etat de la dernière mise à jour des bases de l'Anti-Spam. Peut avoir une des valeurs suivantes :

    - **Les bases ont été actualisées** : la mise à jour des bases a réussi ;
    - **Soldé sur une erreur** : une erreur s'est produite lors de la mise à jour des bases ;
    - **Non exécuté** : la mise à jour n'a pas eu lieu.

  - **Date et heure d'édition**.

    Date et heure de diffusion des bases de l'Anti-Spam. S'affichent selon le format défini dans les paramètres du système d'exploitation.

    Si les bases de l'Anti-Spam sont dépassées de plus d'une heure, le texte de ce champ apparaît en rouge.

Si le groupe **Bases de l'Anti-Spam** et le champ **Date et heure d'édition** dans ce groupe apparaissent en rouge, il faut actualiser les bases de l'Anti-Spam (cf. rubrique "Lancement de la mise à jour manuelle des bases" à la page 53). Le cas échéant, vous pouvez configurer les paramètres de la mise à jour des bases de l'Anti-Spam (cf. section « Configuration de la mise à jour programmée des bases » à la page 53).

Si la dernière mise à jour des bases de l'Anti-Spam s'est soldée sur un échec, le groupe **Bases de l'Anti-Spam** apparaît en rouge et le champ **Etat** affiche un message sur l'erreur.

Le lien **Passer à la configuration de la mise à jour** ouvre le panneau des résultats du nœud **Mises à jour**.

- Le groupe de paramètres **Bases de l'Antivirus** affiche les informations sur l'état des bases de l'Antivirus :

  - **Dernière mise à jour**.

    Date de la dernière mise à jour des bases de l'Antivirus.

- **Etat**.

  Etat de la dernière mise à jour des bases de l'Antivirus. Peut avoir une des valeurs suivantes :

  - **Les bases ont été actualisées** : la mise à jour des bases a réussi ;
  - **Soldé sur une erreur** : une erreur s'est produite lors de la mise à jour des bases ;
  - **Non exécuté** : la mise à jour n'a pas eu lieu.

- **Date et heure d'édition**.

  Date et heure de diffusion des bases de l'Antivirus. S'affichent selon le format défini dans les paramètres du système d'exploitation.

  Si les bases de l'Antivirus sont dépassées de plus de 24 heures, le texte de ce champ apparaît en rouge.

- **Nombre d'enregistrements dans la base**.

  Nombre d'enregistrements relatifs aux menaces connues contenues dans les bases de l'Antivirus.

Si le groupe **Bases de l'Antivirus** et le champ **Date et heure d'édition** dans ce groupe apparaissent en rouge, il faut actualiser les bases de l'Antivirus (cf. section "Lancement de la mise à jour manuelle" à la page 53). Le cas échéant, vous pouvez configurer les paramètres de la mise à jour des bases de l'Antivirus (cf. section « Configuration de la mise à jour programmée des bases » à la page 53).

Si la dernière mise à jour des bases de l'Antivirus s'est soldée sur un échec, le groupe **Bases antivirus** apparaît en rouge et le champ **Etat** affiche un message sur l'erreur.

Le lien **Passer à la configuration de la mise à jour** ouvre le panneau des résultats du nœud **Mises à jour**.

- Le groupe de paramètres **Statistiques** reprend les compteurs qui fournissent des informations sur le nombre de messages placés en quarantaine en vue d'une nouvelle recherche de courrier indésirable (cf. page 73) :

  - **Total de messages placés en quarantaine pendant l'utilisation de l'application**.

    Nombre de messages placés en quarantaine depuis le début de la collecte des statistiques.

  - **Nombre de messages maintenant en quarantaine**.

    Nombre de messages actuellement en quarantaine.

  Sous les compteurs dans le groupe de paramètres **Statistiques**, vous trouverez les diagrammes suivants contenant les statistiques sur le fonctionnement des modules de l'application au cours des sept derniers jours :

  - **Anti-Spam**.

    Le diagramme reprend les informations suivantes :

    - **Total des messages**. Nombre de messages traités.
    - **Phishing ou courrier indésirable**. Nombre de messages analysés considérés comme indésirable ou de phishing.
    - **Non analysés**. Nombre de messages non analysés.
    - **Sains**. Nombre de messages analysés ne contenant aucun élément de courrier indésirable ou de phishing.
    - **Autres**. Nombre de messages appartenant aux catégories suivantes :
      - Spam potentiel
      - Notification formelle.
      - Envoi massif.
      - Message soumis à l'action des listes noire ou blanche.

- **Antivirus pour le rôle serveur de transport hub**.

  Le diagramme reprend les informations suivantes :

  - **Total des messages**. Nombre de messages traités.
  - **Infectés**. Nombre de messages infectés détectés.
  - **Non analysés**. Nombre de messages non analysés.
  - **Sains**. Nombre de messages analysés ne contenant aucun virus.
  - **Autres**. Nombre de messages appartenant aux catégories suivantes :
    - Potentiellement infecté.
    - Protégés.
    - Endommagés.

- **Antivirus pour le rôle serveur de boîtes aux lettres**.

  Le diagramme reprend les informations suivantes :

  - **Nom du serveur**. Nom du serveur connecté.
  - **Nombre total d'objets**. Nombre de messages traités.
  - **Infectés**. Nombre de messages infectés détectés.
  - **Non analysés**. Nombre de messages non analysés.
  - **Sains**. Nombre de messages analysés ne contenant aucun virus.
  - **Autres**. Nombre de messages appartenant aux catégories suivantes :
    - Potentiellement infecté.
    - Protégés.
    - Endommagés.

L'ensemble de diagrammes peut être réduit en fonction de la configuration de l'application.

Le lien **Accéder aux rapports** ouvre le panneau des résultats du nœud **Rapports** où il est possible de créer des rapports sur le fonctionnement de l'application.

# CONSULTATION DES INFORMATIONS RELATIVES A L'ETAT DE LA PROTECTION DU PROFIL

*Pour consulter les informations relatives à l'état de la protection du profil, procédez comme suit :*

1. Lancez la console d'administration via le menu du système d'exploitation **Démarrer → Programmes → Kaspersky Security 8.0 for Microsoft Exchange Servers → Console d'administration**.

2. Dans le nœud **Profils** de l'arborescence de la console d'administration, sélectionnez le nœud du profil dont vous souhaitez consulter les informations sur l'état de la protection.

Les informations suivantes sont reprises dans le panneau d'information du profil sélectionné :

- Le groupe de paramètres **Licence** reprend les informations relatives à la licence pour le profil :
  - **Fonction**.

    Niveau de fonctionnalité de l'application, défini par la licence active. Peut avoir une des valeurs suivantes :

    - Fonctionnalité complète.
    - La durée de validité de la licence a expiré. La mise à jour des bases est interdite, l'utilisation de KSN n'est pas disponible.
    - Uniquement les mises à jour.
    - Uniquement l'administration.
  - **Etat**.

    Peut avoir une des valeurs suivantes :

    - Licence active. La fonctionnalité de l'application est illimitée.
    - Durée de validité de la licence d'évaluation écoulée. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.
    - La durée de validité de la licence a expiré. La mise à jour est interdite, l'utilisation de KSN n'est pas disponible.
    - Les bases sont corrompues. Les bases de l'Antivirus et de l'Anti-Spam manquent ou sont endommagées.
    - La clé est absente. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles et la mise à jour est interdite.
    - La clé a été bloquée. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.
    - La liste noire des clés est endommagée ou introuvable. Seule la mise à jour des bases est disponible. Les fonctionnalités des modules Antivirus et Anti-Spam ne sont pas disponibles.

  Si le champ **Etat** affiche une valeur autre que *Licence active*, le groupe **Licence** est mis en évidence en rouge. Dans ce cas, il faut ajouter une clé active(cf. section «Ajout d'une clé» à la page 27), en accédant au nœud **Licence** via le lien **Passer à l'administration des clés**.

  - **Date d'expiration**.

    Fin de validité de la licence.

  Si le champ **Date d'expiration** est mis en évidence en rouge, il faut renouveler la licence, par exemple en ajoutant une clé complémentaire (cf. section "Ajout d'une clé" à la page 27), en accédant au nœud **Licence** via le lien **Passer à l'administration des clés**.

  La période précédant l'expiration de la licence pendant laquelle le champ est mis en évidence en rouge est définie par le paramètre **Signaler l'expiration de la durée de validité de licence : X jours** (cf. section "**Configuration de la notification sur l'expiration de la durée de validité de la licence**" à la page 30) situé dans le volet des résultats du nœud **Licence**. Cette limite est fixée par défaut à 15 jours.

  - **Nombre d'utilisateurs**.

    Nombre maximal d'utilisateurs dont les boîtes aux lettres peuvent être protégées par l'application avec cette clé.
  - **Clé complémentaire**.

    Informations relatives à la présence d'une clé complémentaire : **Ajoutée** ou **Absente**.

Le lien **Passer à l'administration des clés** ouvre le panneau des résultats du nœud **Licence** où il est possible d'ajouter ou de supprimer des clés.

- Le groupe de paramètres **Etat des serveurs** contient un tableau qui reprend les informations relatives à l'état des serveurs du profil, des mises à jour, des modules de l'application et du serveur SQL :

  - **Serveur**.

    Le nom du serveur peut avoir les valeurs suivantes :

    - <Nom de domaine du serveur> si le profil accueille un Serveur de sécurité installé sur un serveur Microsoft Exchange qui n'appartient pas à un DAG et qui n'est pas un nœud passif d'un cluster.
    - <Nom DAG – Nom de domaine du serveur>, si un Serveur de sécurité installé sur le serveur Microsoft Exchange, appartenant au DAG, est ajouté au profil.
    - <Nom du serveur virtuel – Nom de domaine du serveur>, si un serveur virtuel est ajouté au profil.

  - **État des mises à jour**.

    Etat de la mise à jour des bases sur le serveur. Peut avoir une des valeurs suivantes :

    - **Les bases sont à jour** : la mise à jour des bases a réussi ;
    - **Erreur de bases** : une erreur s'est produite lors de la mise à jour des bases. Les bases sont dépassées, elles sont endommagées ou la mise à jour n'a pas eu lieu ;
    - **Serveur inaccessible** : le serveur est inaccessible via le réseau ou il est désactivé.

  - **Module Antivirus**.

    Etat du module Antivirus. Peut avoir une des valeurs suivantes :

    - **Désactivé** : le module antivirus du rôle serveur de transport Hub ou serveur de boîtes aux lettres est installé, la case **Activer la protection antivirus du rôle serveur de transport Hub** ou **Activer la protection antivirus du rôle serveur de boîtes aux lettres** n'est pas cochée.
    - **Hors-service** : le module antivirus du rôle serveur de transport Hub, du rôle serveur de transport Edge ou du serveur de boîtes aux lettres est installé, la **Activer la protection antivirus du rôle serveur de transport Hub** ou **Activer la protection antivirus du rôle serveur de boîtes aux lettres** est cochée, mais le module Antivirus ne recherche pas la présence éventuelle de virus ou d'autres menaces en raison d'une erreur des bases ou d'une erreur d'analyse.
    - **Pas installé** : le module antivirus du rôle serveur de transport Hub, du rôle serveur de transport Edge ou du serveur de boîtes aux lettres n'est pas installé.
    - **Activé** : le module antivirus du rôle serveur de transport Hub, du rôle serveur de transport Edge ou du serveur de boîtes aux lettres est installé, la **Activer la protection antivirus du rôle serveur de transport Hub** ou **Activer la protection antivirus du rôle serveur de boîtes aux lettres** est cochée, mais le module Antivirus recherche la présence éventuelle de virus ou d'autres menaces en raison d'une erreur des bases ou d'une erreur d'analyse.

  - **Module Anti-Spam**.

    Etat du module Anti-Spam. S'affiche si le serveur Microsoft Exchange est déployé dans le rôle Transport Hub ou Transport Edge. Peut avoir une des valeurs suivantes :

    - **Désactivé** : le module Anti-Spam est activé, le contrôle de la messagerie contre le courrier indésirable est désactivé.
    - **Hors-service** : le module Anti-Spam est installé, le contrôle de la messagerie contre le courrier indésirable est activé, mais le module Anti-Spam ne recherche pas les messages non sollicités potentiels en raison d'une erreur de licence, d'une erreur dans les bases ou d'une erreur d'analyse.
    - **Pas installé** : le module Anti-Spam n'est pas installé.
    - **Activé** : le module Anti-Spam fonctionne, le contrôle de la messagerie contre le courrier indésirable est activé et le module Anti-Spam recherche la présence d'éventuels messages non sollicités.

- **Serveur SQL**.

  L'état du serveur SQL peut prendre une des valeurs suivantes :

  - **Accessible**.
  - **Inaccessible**.

Si le serveur n'est pas accessible, la colonne **Etat des mises à jour** affiche l'état *Serveur inaccessible*, et les colonnes **Etat des mises à jour**, **Module Antivirus** et **Module Anti-Spam** apparaissent en rouge.

Si la colonne **Etat des mises à jour** contient une valeur différente de *Les bases sont à jour*, la colonne apparaît en rouge.

Si l'état du module Antivirus ou du module Anti-Spam est *Désactivé* ou *Hors-service*, la colonne qui correspond au module est mise en évidence en rouge.

Le lien du nom du serveur dans la colonne **Serveur** ouvre le panneau des résultats du nœud du serveur.

# PREMIERE UTILISATION

Cette section contient des informations sur l'utilisation de Kaspersky Security, le lancement de la Console d'administration et la création des listes de serveurs à protéger.

L'administration du fonctionnement de l'application est réalisée depuis le poste de travail de l'administrateur, c.-à-d. l'ordinateur sur lequel la console d'administration est installée. Vous pouvez connecter à la console d'administration n'importe quel nombre de serveurs de sécurité et les administrer localement ou à distance.

### DANS CETTE SECTION DE L'AIDE

Lancement de la console d'administration..... 43

Connexion de la console d'administration au serveur de sécurité..... 43

## LANCEMENT DE LA CONSOLE D'ADMINISTRATION

- *Pour lancer la console d'administration,*

  via le menu **Démarrer → Programmes → Kaspersky Security 8.0 for Microsoft Exchange Servers → Console d'administration**.

Une fois que la console d'administration a été lancée, elle se connecte automatiquement au serveur de sécurité local et l'arborescence de la console d'administration affiche alors l'icône de l'application, le nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers** et le nœud du serveur de sécurité local (si il avait été installé) connecté à la console d'administration.

Pour connecter la console d'administration à un serveur de sécurité installé sur un serveur Microsoft Exchange distant, il faut ajouter le service *Kaspersky Security 8.0 for Microsoft Exchange Server* à la liste des applications de confiance du pare-feu sur le serveur Microsoft Exchange distant ou autoriser la connexion selon RPC.

## CONNEXION DE LA CONSOLE D'ADMINISTRATION AU SERVEUR DE SECURITE

Pour administrer le fonctionnement de l'application, vous devez connecter la Console d'administration à tous les Serveurs de sécurité installés sur les serveurs Microsoft Exchange que vous souhaitez protéger. Vous pouvez connecter la Console d'administration aussi bien à un ordinateur local qu'à un serveur Microsoft Exchange installé dans le réseau.

Vous ne pouvez pas ajouter un DAG Microsoft Exchange à la liste des serveurs protégés. Par contre, vous pouvez ajouter n'importe lequel des serveurs qui appartiennent au DAG afin d'établir une connexion à celui-ci pour exécuter les actions générales pour le DAG ou ajouter un serveur Microsoft Exchange distinct (y compris un membre du DAG) pour configurer ses paramètres individuels.

Parmi les actions générales pour un DAG, citons par exemple la configuration des paramètres de la protection antivirus pour le rôle Boîte aux lettres, la configuration des paramètres des rapports de fonctionnement de l'Antivirus pour le rôle Boîte aux lettres, la configuration des paramètres de notification, la configuration des paramètres de mise à jour des bases de l'Antivirus, la consultation du contenu de la sauvegarde ou l'ajout d'une clé.

Parmi les paramètres individuels du serveur Microsoft Exchange, citons par exemple les paramètres de la protection antivirus pour le rôle serveur de transport Hub, les paramètres antispam, les paramètres de la sauvegarde, les paramètres des rapports sur le fonctionnement de l'Anti-Spam et sur le fonctionnement de l'Antivirus pour le rôle serveur de transport Hub et les paramètres de mise à jour des bases de l'Anti-Spam.

*Pour connecter la Console d'administration au Serveur de sécurité, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez le nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers**.

2. Ouvrez la fenêtre **Se connecter au serveur** d'une des méthodes suivantes :

   - Sélectionner l'option **Se connecter au serveur** dans le menu **Action** ;
   - Sélectionner l'option **Se connecter au serveur** dans le menu contextuel du nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers** ;
   - Cliquer sur le bouton **Se connecter au serveur** dans le panneau des résultats ;
   - Cliquer sur le lien **Se connecter au serveur** dans le panneau d'accès rapide.

3. Sélectionnez, dans la fenêtre **Se connecter au serveur**, le Serveur de sécurité installé sur le serveur Microsoft Exchange auquel vous souhaitez connecter la Console d'administration :

4. Si vous souhaitez connecter une Console d'administration à un Serveur de sécurité déployé sur un ordinateur local, sélectionnez l'option Ordinateur local.

5. Si vous souhaitez connecter une Console d'administration à un Serveur de sécurité déployé sur un serveur Microsoft Exchange distant, sélectionnez l'option Autre ordinateur.

   Pour connecter la console d'administration à un serveur de sécurité qui se trouve sur un serveur distant, il faut ajouter le service *Kaspersky Security 8.0 for Microsoft Exchange Servers* à la liste des applications de confiance du pare-feu sur le serveur distant ou autoriser la connexion selon RPC.

6. Si vous avez choisi l'option **Autre ordinateur**, indiquez dans le champ le serveur Microsoft Exchange distant sur lequel le serveur de sécurité est installé. Vous pouvez sélectionner le serveur Microsoft Exchange distant dans la liste à l'aide du bouton **Parcourir** ou vous pouvez saisir manuellement une des valeurs suivantes pour le serveur Microsoft Exchange distant :

   - l'adresse IP ;
   - le nom de domaine complet (au format <nom de l'ordinateur>.<DNS du nom de domaine>) ;
   - le nom de l'ordinateur dans le réseau Microsoft Windows (nom NetBIOS).

7. Cliquez sur **OK**.

Le Serveur de sécurité connecté apparaît dans l'arborescence de la console d'administration.

# ADMINISTRATION DES PROFILS

Cette section explique comment utiliser les profils, en créer et configurer leurs paramètres.

### DANS CETTE SECTION DE L'AIDE


Présentation des profils ..... 45

Création d'un profil ..... 46

Configuration des paramètres des Serveurs de protection dans un profil ..... 47

Particularités de l'administration des profils dans un groupe de disponibilité de base de données Microsoft Exchange 48

Ajout de serveurs de sécurité à un profil ..... 48

Suppression du serveur de sécurité d'un profil ..... 49

Suppression d'un profil ..... 50


## PRESENTATION DES PROFILS

Si le réseau de l'organisation compte plusieurs serveurs Microsoft Exchange dotés de l'application, vous serez peut-être amené à gérer simultanément les paramètres de l'application dans un groupe de serveurs. Il pourrait s'agir par exemple de serveurs Microsoft Exchange dotés de critères de sécurité identiques. Afin d'administrer des paramètres identiques dans un groupe de serveurs de sécurité via Kaspersky Security, vous pouvez utiliser les *profils*. Un profil est un ensemble de paramètres identiques appliqués simultanément à plusieurs serveurs de sécurité. L'utilisation des profils permet de configurer des paramètres identiques pour tous les serveurs de sécurité du même type du profil simultanément et d'éviter la configuration des paramètres pour chaque serveur de sécurité individuellement.

Le recours aux profils peut être utile dans les cas suivants :

- Le réseau de l'organisation compte plusieurs serveurs Microsoft Exchange doté de l'application et vous devez administrer ceux-ci de la même manière. Dans ce cas, vous pouvez créer un profil, y ajouter tous les serveurs de sécurité et configurer les paramètres de l'application dans le profil.

- Le réseau de l'organisation compte aux moins deux groupes de serveurs de sécurité et vous devez configurer ces groupes de manière différente. Dans ce cas, vous pouvez utiliser les profils d'une des manières suivantes :

    - Si chaque groupe compte plus d'un serveur de sécurité, vous pouvez créer plusieurs profils avec des paramètres différents et y ajouter les différents serveurs de sécurité.

    - Si un des serveurs de sécurité requiert une configuration individuelle, vous pouvez créer un profil pour un groupe de serveurs avec des paramètres identiques et gérer les paramètres de ces serveurs à l'aide des profils créés et pour ce serveur de sécurité qui n'appartient pas au groupe, il n'est pas nécessaire de créer un profil car vous pouvez configurer ses paramètres séparément. Un serveur de sécurité unique qui ne figure dans aucun profil est un *serveur de sécurité non réparti*. Vous pouvez configurer les paramètres d'un serveur de sécurité non réparti séparément dans le nœud de ce serveur.

L'utilisation des profils n'est pas obligatoire. Vous pouvez également configurer les paramètres des serveurs de sécurité séparément dans le nœud de chaque serveur de sécurité.

Si l'organisation possède plusieurs sites, il faut tenir compte des retards de réplications lors de la création et de la modification de profils car les informations relatives aux profils de l'application sont conservées dans Active Directory.

Pour utiliser les profils, procédez comme suit :

1. Créer un profil (cf. section "Création d'un profil" à la page 46).
2. Configurer les paramètres du profil (cf. section "Configuration des paramètres des serveurs de sécurité dans le profil" à la page 47).
3. Ajouter des serveurs de protection au serveur (cf. section "Ajout de serveurs de sécurité au profil" à la page 48).

Il se peut que les paramètres du Serveur de sécurité ne puissent pas être modifiés si le Serveur de sécurité a été ajouté à un profil et s'il hérite des paramètres du profil (cf. section "Configuration des paramètres des Serveurs de protection dans un profil" à la page 47). Dans ce cas, un cadenas apparaît en regard du paramètre inaccessible. Pour attribuer aux paramètres du Serveur de sécurité des valeurs différentes de celles des paramètres du profil, il faut supprimer le Serveur de sécurité du profil (cf. section "Suppression du serveur de sécurité d'un profil" à la page 49).

Vous pouvez créer n'importe quel nombre de profils et y ajouter des serveurs de sécurité ou en supprimer comme vous le voulez (cf. section "Suppression d'un serveur de sécurité du profil" à la page 49).

La suppression d'un serveur de sécurité du profil peut être nécessaire dans les cas suivants :

- vous devez configurer un serveur de sécurité selon des paramètres différents de ceux du profil ;
- vous devez ajouter le serveur de sécurité à un autre profil (dans ce cas, commencez par le supprimer du profil dans lequel il a été ajouté).

Si vous n'avez plus besoin du profil créé, vous pouvez le supprimer de la configuration de l'application (cf. section "Suppression d'un profil" à la page. 50).

# CREATION D'UN PROFIL

*Pour créer un profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Utilisez une des méthodes suivantes pour ajouter un nouveau profil :
   - Sélectionner l'option **Ajouter le profil** dans le menu **Action**.
   - Sélectionner l'option **Ajouter le profil** dans le menu contextuel du nœud **Profils**.
   - Cliquer sur le bouton **Ajouter le profil** dans le panneau des résultats.
   - Cliquer sur le lien **Ajouter le profil** dans le panneau d'accès rapide.
3. Saisissez le nom du profil dans la fenêtre **Créer un profil** qui s'ouvre.
4. Cliquez sur le bouton **OK**.

Le sous-nœud portant le nom du profil créé apparaît dans le nœud **Profils**.

Pour pouvoir utiliser un profil, vous devez configurer ses paramètres (cf. section "Configuration des paramètres des Serveurs de protection dans un profil" à la page 47) et ajouter des serveurs de sécurité au profil (cf. section "Ajout de serveurs de sécurité à un profil" à la page 48).

# CONFIGURATION DES PARAMETRES DES SERVEURS DE PROTECTION DANS UN PROFIL

Vous pouvez exécuter les opérations générales suivantes pour les serveurs de sécurité d'un même profil (dans les sous-nœuds du profil) :

- configurer les paramètres de la protection antivirus (cf. section "Configuration des paramètres de traitement des objets" à la page 64) et de la protection contre le courrier indésirable (cf. section "Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing" à la page 78), ou encore les paramètres avancés de l'Antivirus (cf. section "Configuration des exclusions de l'analyse antivirus" à la page 66) dans le nœud **Protection du serveur** ;

- configurer la programmation de la mise à jour automatique des bases (cf. section "Configuration de la mise à jour programmée des bases" à la page 53) et la source des mises à jour (cf. section "Sélection de la source des mises à jour" à la page 54) dans le nœud **Mises à jour** ;

- configurer les paramètres des notifications (cf. section "Configuration des paramètres de notifications" à la page 97) dans les nœuds **Notifications** et **Configuration** ;

- configurer les paramètres des journaux des événements (cf. section "Configuration des paramètres des journaux" à la page 110) et du niveau de diagnostic (cf. section "Configuration du niveau de diagnostic" à la page 110) dans le nœud **Configuration** ;

- configurer les paramètres des clés (cf. section "Consultation des informations relatives aux clés" à la page 24) et les paramètres de notification sur l'expiration de la validité de la licence (cf. section "Configuration de la notification sur l'expiration de la durée de validité de la licence" à la page 30) dans le nœud **Licence** ;

- configurer les paramètres des rapports (cf. section "Rapports" à la page 100) dans le nœud **Rapports**.

De leurs côtés, les paramètres individuels suivants des serveurs de sécurité et les actions exécutées par l'application pour les serveurs de sécurité ne changent pas :

- le lancement de l'analyse en arrière-plan (cf. section "Configuration des paramètres de l'analyse en arrière-plan" à la page 70) du nœud **Protection du serveur** ;

- le lancement de la mise à jour des bases (cf. section "Lancement de la mise à jour manuelle des bases" à la page 53) dans le nœud **Mises à jour** ;

- les paramètres du centre de mises à jour (cf. section "Définir un serveur comme centre de mises à jour et configurer ses paramètres" à la page 57) dans le nœud **Mises à jour** ;

- l'envoi test d'une notification (cf. section "Configuration des paramètres d'envoi des notifications" à la page 98) dans les nœuds **Notifications** et **Configuration** ;

- les paramètres de la sauvegarde (cf. section "Configuration des paramètres de la sauvegarde" à la page 95) dans le nœud **Configuration**.

Comme auparavant, vous pouvez configurer les paramètres et exécuter les actions uniquement de manière individuelle pour chaque serveur de sécurité (dans les sous-nœuds de chaque serveur de sécurité ou dans le nœud du profil dans l'arborescence du nœuds **Serveurs** pour chaque serveur Microsoft Exchange).

# PARTICULARITES DE L'ADMINISTRATION DES PROFILS DANS UN GROUPE DE DISPONIBILITE DE BASE DE DONNEES MICROSOFT EXCHANGE

Si vous avez modifié, dans la console d'administration Exchange, la configuration du DAG ajoutée au profil dans Kaspersky Security, il conviendra de tenir compte des particularités suivantes des paramètres des serveurs de sécurité de ce DAG dans l'application Kaspersky Security :

- Si vous installez Kaspersky Security sur un serveur Microsoft Exchange appartenant à un DAG ajouté au profil, les paramètres de ce profil seront appliqués au serveur de sécurité correspondant dans Kaspersky Security après l'installation.

- Si vous ajoutez un serveur Microsoft Exchange doté de Kaspersky Security dans un DAG dans la console d'administration Exchange, les paramètres de ce profil sont appliqués au serveur de sécurité correspondant dans Kaspersky Security. Si le DAG n'est pas ajouté au profil, les paramètres individuels de ce DAG sont appliqués aux serveurs de sécurité correspondant dans Kaspersky Security.

- Si, dans la console d'administration Exchange, vous réunissez plusieurs serveurs Microsoft Exchange dotés de l'application ajoutés au profil dans un nouveau DAG, les paramètres de ce DAG sont appliqués aux serveurs de sécurité dans Kaspersky Security. Autrement dit, les paramètres généraux par défaut sont activés (sauf la liste des stockages protégés et des dossiers partagés) et les paramètres individuels des serveurs et les paramètres de la liste des stockages protégés des dossiers partagés ont la même valeur qu'avant l'ajout de serveurs au DAG.

  Si les serveurs avaient été ajoutés à un profil avant d'être regroupés dans un DAG, ils apparaissent toujours après le regroupement non seulement dans la liste des serveurs du DAG, mais également dans ces profils, mais vous ne pouvez pas administrer les paramètres de ces serveurs au départ des profils. Vous pouvez administrer les paramètres de ces serveurs uniquement depuis le profil auquel le DAG a été ajouté ou via les paramètres individuels du DAG (si le DAG ne figure pas dans un profil). Au besoin, vous pouvez supprimer manuellement du profil les serveurs qui y apparaissent.

- Si vous excluez, dans la console d'administration Exchange, un serveur Microsoft Exchange doté de l'application d'un DAG ajouté à un profil dans Kaspersky Security, le serveur de sécurité correspondant est exclu du profil dans Kaspersky Security et reçoit les paramètres par défaut. Une fois exclu du DAG, ce serveur de sécurité n'apparaît plus dans la liste des serveurs du profil et il faudra l'ajouter manuellement à la liste des serveurs Microsoft Exchange protégés (cf. section "Connexion de la console d'administration au serveur de sécurité" à la page 43) ou dans un des profils (cf. section "Ajout de serveurs de sécurité à un profil" à la page 48) et configurer ses paramètres (cf. section "Configuration des paramètres des serveurs de protection dans un profil" à la page 47).

# AJOUT DE SERVEURS DE SECURITE A UN PROFIL

*Pour ajouter des serveurs de sécurité à un profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.

2. Sélectionnez le nœud du profil auquel vous souhaitez ajouter un serveur de sécurité ou déployez le nœud du profil et choisissez le nœud **Serveurs**.

3. Ouvrez l'Assistant d'ajout d'un serveur au profil d'une des manières suivantes :

   - Sélectionner l'option **Ajouter un serveur** dans le menu **Action**.

   - Sélectionner l'option **Ajouter un serveur** dans le menu contextuel du nœud.

   - Cliquer sur le lien **Ajouter un serveur** dans le panneau d'accès rapide.

- Cliquer sur le bouton **Ajouter un serveur** dans le panneau des résultats de la Console d'administration (uniquement pour le nœud de profil sélectionné).

4. Dans la fenêtre de l'Assistant **Sélection des serveurs**, sélectionnez dans le champ **Serveurs non répartis** les serveurs de sécurité que vous souhaitez ajouter au profil.

   Le champ **Serveurs non répartis** affiche les serveurs de sécurité qui n'ont été ajoutés à aucun profil.

5. Dans la fenêtre de l'Assistant **Sélection des serveurs**, cliquez sur le bouton **>>**.

   Les serveurs de sécurité sélectionnés apparaissent dans le champ **Ajoutés au profil**.

6. Cliquez sur le bouton **Suivant**.

7. Dans la fenêtre **Confirmation** de l'Assistant qui s'ouvre, cliquez sur le bouton **Terminer**.

Les serveurs de sécurité ajoutés apparaissent dans la liste des serveurs du panneau des résultats du nœud du profil et dans le nœud du profil dans l'arborescence du nœud **Serveurs**. Les paramètres généraux des serveurs de sécurité du profil (cf. section "Configuration des paramètres des Serveurs de protection dans un profil" à la page 47) sont appliqués aux serveurs ajoutés au profil dans les 5 minutes.

Vous pouvez ajouter les serveurs qui appartiennent au DAG ou à une grappe de serveurs au profil uniquement tous ensemble simultanément ; Lors de l'ajout d'un DAG au profil, tous les serveurs et tous leurs rôles (y compris celui de transport Hub) sont ajoutés à ce profil.

Vous ne pouvez pas ajouter au profil un Serveur de sécurité installé sur un ordinateur sur lequel un serveur Microsoft Exchange dans le rôle serveur de transport Edge a été déployé.

Une fois qu'un serveur de sécurité a été ajouté à un profil, il est couvert par la licence au niveau du profil, même si une autre licence était active pour ce serveur de sécurité avant son ajout au profil.

# SUPPRESSION DU SERVEUR DE SECURITE D'UN PROFIL

*Pour supprimer des serveurs de sécurité d'un profil, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.

2. Sélectionnez le serveur de sécurité que vous souhaitez supprimer d'une des manières suivantes :

   - sélectionnez le nœud du profil d'où vous souhaitez supprimer le serveur de sécurité et dans la liste des serveurs du panneau des résultats, sélectionnez le serveur de sécurité que vous souhaitez supprimer ;

   - développez le nœud du profil d'où vous souhaitez supprimer le serveur de sécurité, développez le nœud **Serveurs** et dans la liste des serveurs, sélectionnez le serveur de sécurité que vous souhaitez supprimer.

3. Utilisez une des méthodes suivantes pour supprimer le serveur de sécurité sélectionné :

   - Si vous avez sélectionné un serveur de sécurité dans le panneau des résultats, cliquez sur le bouton **Supprimer le serveur**.

   - Si vous avez sélectionné le serveur de sécurité dans la liste des serveurs du nœud **Serveurs**, supprimez-le d'une des manières suivantes :

     - Sélectionnez **Supprimer** dans le menu **Action**.

     - Sélectionnez **Supprimer** dans le menu contextuel du nœud.

- Cliquez sur le lien **Supprimer** dans le panneau d'accès rapide.

4. Confirmez la suppression du serveur dans la fenêtre qui s'ouvre.

   L'application supprimera le serveur de sécurité de la liste des serveurs du panneau des résultats du nœud du profil et du nœud **Serveurs** dans l'arborescence du nœud du profil dans les 5 minutes. Les paramètres du serveur de sécurité ne changent pas, mais vous ne pourrez plus les configurer depuis le profil. Vous pourrez les configurer uniquement de manière individuelle pour le serveur de sécurité dans le nœud de ce serveur de sécurité.

Vous pouvez supprimer du profil tous les serveurs du DAG ou de la grappe de serveurs uniquement simultanément.

Après la suppression d'un serveur de sécurité d'un profil, il est toujours couvert par la licence au niveau du profil d'où il a été supprimé.

# SUPPRESSION D'UN PROFIL

*Pour supprimer un profil, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez d'une des méthodes suivantes le profil que vous souhaitez supprimer :

   - sélectionnez le nœud **Profils** et dans le panneau des résultats, sélectionnez le profil que vous souhaitez supprimer dans la liste des profils ;

   - développez le nœud **Profils** et dans la liste des nœuds, sélectionnez le nœud que vous souhaitez supprimer.

2. Utilisez une des méthodes suivantes pour supprimer le profil sélectionné :

   - Si vous avez sélectionné un profil dans le panneau des résultats, cliquez sur le bouton **Supprimer le profil**.

   - Si vous avez sélectionné un nœud du profil appartenant au nœud **Profils**, supprimez-le d'une des manières suivantes :

     - Sélectionnez **Supprimer** dans le menu **Action**.

     - Sélectionnez **Supprimer** dans le menu contextuel du nœud du profil.

     - Cliquez sur le lien **Supprimer** dans le panneau d'accès rapide.

3. Confirmez la suppression du profil dans la fenêtre qui s'ouvre.

L'application supprime le profil de l'arborescence du nœud **Profils**. Les serveurs de sécurité qui figuraient dans le profil deviendront des serveurs non répartis. Les paramètres des serveurs de sécurité non répartis ne sont pas modifiés, mais vous ne pourrez configurer tous les paramètres pour chaque serveur de sécurité que de manière individuelle dans le nœud de chaque serveur.

# MISE A JOUR DES BASES

Cette section aborde la mise à jour des bases de l'application (ci-après, *mise à jour, mise à jour des bases*) et la configuration des paramètres de la mise à jour.

### DANS CETTE SECTION DE L'AIDE


Présentation de la mise à jour des bases ..... 51

Présentation des centres de mises à jour ..... 52

Présentation de la mise à jour des bases dans les configurations avec cluster ou DAG de serveurs ..... 52

Lancement de la mise à jour manuelle des bases ..... 53

Configuration de la mise à jour des bases programmée ..... 53

Sélection de la source de mises à jour ..... 54

Configuration des paramètres de connexion à la source des mises à jour ..... 56

Configuration du serveur proxy ..... 56

Désignation d'un serveur comme centre de mises à jour et configuration de ses paramètres ..... 57


## PRESENTATION DE LA MISE A JOUR DES BASES

La mise à jour des bases de Kaspersky Security garantit l'actualité de la protection des serveurs Microsoft Exchange.

De nouveaux virus et programmes dangereux ainsi que de nouveaux types de courrier indésirable apparaissent chaque jour. Les informations relatives aux menaces et au courrier indésirable ainsi que les données sur les modes de neutralisation se trouvent dans les *bases de l'application*, à savoir dans les bases de l'Antivirus et dans les bases de l'Anti-Spam. Afin de pouvoir détecter à temps les nouvelles menaces et les nouveaux types de messages non sollicités, il faut mettre à jour les bases de l'application selon un intervalle régulier.

Il est conseillé de mettre les bases de l'application à jour directement après l'installation de l'application car les bases présentes dans la distribution sont dépassées au moment de l'installation. Les bases de l'Antivirus sont mises à jour toutes les heures sur les serveurs de Kaspersky Lab. Les bases de l'Anti-Spam sont actualisées toutes les cinq minutes. Il est conseillé d'adopter la même fréquence pour la configuration de la mise à jour programmée des bases (cf. section «Configuration de la mise à jour des bases programmées» à la page 53).

Kaspersky Security peut récupérer les mises à jour depuis les sources de mises à jour suivantes :

- les serveurs de mises à jour de Kaspersky Lab en ligne ;
- un autre serveur HTTP/FTP (par exemple, votre serveur Intranet) ;
- une source de mises à jour locale (dossier local ou de réseau) ;
- le centre de mises à jour, un des serveurs dotés de Kaspersky Security, qui a été désigné comme Centre de mises à jour (cf. section « Présentation des centres de mises à jour » à la page 52).

La mise à jour des bases peut être exécutée manuellement ou selon une programmation. Une fois que les fichiers ont été copiés depuis la source de mises à jour indiquée, l'application utilise automatiquement les bases récupérées.

# PRESENTATION DES CENTRES DE MISES A JOUR

Tout serveur Microsoft Exchange disposant de l'application Kaspersky Security peut être défini comme centre de mises à jour (cf. section "Définir un serveur comme centre de mises à jour et configurer ses paramètres" à la page 57). Les centres de mises à jour obtiennent les bases les plus récentes sur les serveurs de Kaspersky Lab et peuvent remplir le rôle de sources de mises à jour des bases de l'application (cf. section « Sélection de la source de la mise à jour » à la page 54) pour d'autres serveurs Microsoft Exchange dotés de l'application.

Le recours aux centres de mises à jour peut être utile dans les cas suivants :

- Si le réseau de l'entreprise compte plusieurs serveurs Microsoft Exchange dotés de l'application, vous pouvez désigner l'un d'entre eux comme centre de mises à jour chargé de recevoir les bases depuis les serveurs de Kaspersky Lab. Désignez-le en tant que source de mises à jour pour les autres serveurs Microsoft Exchange du réseau. Ainsi, vous réduirez le trafic Internet, garantirez l'homogénéité des états des bases de tous les serveurs Microsoft Exchange et vous n'aurez pas besoin de configurer la connexion à Internet pour chaque serveur Microsoft Exchange et d'assurer la protection de ces connexions.

- Si le réseau de l'entreprise comprend des segments de serveurs séparés géographiquement et unis par des canaux de communication lents, vous pouvez créer un centre de mises à jour pour chaque segment régional. Vous réduirez ainsi le trafic réseau entre les segments régionaux et vous accélérerez la diffusion des mises à jour sur tous les serveurs du réseau de l'organisation.

# PRESENTATION DE LA MISE A JOUR DES BASES DANS LES CONFIGURATIONS AVEC CLUSTER OU DAG DE SERVEURS

Dans les configurations impliquant des cluster ou des DAG de serveurs Microsoft Exchange, les paramètres de la mise à jour des bases sont identiques pour l'ensemble du cluster/du DAG de serveurs. Ceci permet de configurer la mise à jour centralisée des bases sur tous les serveurs appartenant à la configuration.

Vous pouvez configurer les modes suivants de mise à jour centralisée des bases :

- **Depuis les serveurs de mise à jour de Kaspersky Lab**. Si vous choisissez cette méthode, chacun des serveurs du cluster/du DAG se connecte aux serveurs de mise à jour de Kaspersky Lab à l'heure indiquée et indépendamment des autres serveurs, ce qui entraîne une augmentation du trafic Internet. Pour cette raison, l'utilisation de cette méthode est déconseillée dans les configurations qui comptent un grand nombre de serveurs. Le point faible de cette méthode est l'obligation de configurer la connexion Internet pour chaque serveur faisant partie de la configuration. Son avantage se situe au niveau de l'augmentation de la fiabilité car la mise à jour est réalisée directement depuis les serveurs de Kaspersky Lab sans intermédiaires.

- **Depuis un serveur intermédiaire ou un dossier réseau**. Si vous choisissez cette méthode, les serveurs du cluster/du DAG téléchargent les mises à jour depuis un serveur HTTP ou FTP intermédiaire ou depuis un dossier réseau qui se trouve hors de la configuration des serveurs Microsoft Exchange. Cette méthode permet de limiter le trafic Internet de l'organisation et d'améliorer la vitesse et la synchronisation des mises à jour sur tous les serveurs de la configuration. Toutefois, elle entraîne des frais supplémentaires pour la maintenance du matériel complémentaire.

- **Depuis un centre de mises à jour**. Cette méthode exige que l'un des serveurs de la grappe/du DAG soit défini comme centre de mises à jour (cf. section "Définir un serveur comme centre de mises à jour et configurer ses paramètres" à la page 57). Les avantages de cette méthode se situent au niveau de la réduction du trafic Internet de l'organisation et de la rapidité et de la synchronisation de la mise à jour sur tous les serveurs de la configuration. Toutefois, cette méthode requiert une excellente fiabilité du serveur désigné comme centre de mises à jour.

# LANCEMENT DE LA MISE A JOUR MANUELLE DES BASES

*Pour consulter les informations relatives à la mise à jour des bases de l'Antivirus et mettre à jour ces bases manuellement, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez le nœud **Mises à jour**.
3. Le groupe de paramètres **Mise à jour des bases de l'Antivirus** du panneau des résultats affiche les informations suivantes :
   - **Résultat de la dernière mise à jour**. Informations relatives à l'état de la mise à jour des bases de l'Antivirus.
   - **Heure d'édition des bases**. Heure d'édition des bases de l'Antivirus utilisées actuellement par l'application sur le serveur de Kaspersky Lab (UTC).
   - **Nombre d'enregistrements**. Nombre de définitions de virus contenues dans la version actuelle des bases de l'Antivirus.
4. Si vous souhaitez lancer la mise à jour des bases de l'Antivirus, cliquez sur le bouton **Lancer la mise à jour**.
5. Pour arrêter la mise à jour, cliquez sur **Arrêter**.

Si l'application fonctionne dans un cluster ou dans un DAG de serveurs Microsoft Exchange, la mise à jour manuelle des bases de l'Antivirus doit être effectuée sur chacun des serveurs de sécurité appartenant au cluster ou au DAG.

*Pour consulter les informations relatives à la mise à jour des bases de l'Anti-Spam et mettre à jour ces bases manuellement, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez le nœud **Mises à jour**.
3. Le groupe de paramètres **Mise à jour des bases de l'Anti-Spam** du panneau des résultats affiche les informations suivantes :
   - **Résultat de la dernière mise à jour**. Informations relatives à l'état de la mise à jour des bases de l'Anti-Spam.
   - **Heure d'édition des bases**. Heure d'édition des bases de l'Anti-Spam utilisées actuellement par l'application sur le serveur de Kaspersky Lab (UTC).
4. Si vous souhaitez lancer la mise à jour des bases de l'Anti-Spam, cliquez sur le bouton **Lancer la mise à jour**.
5. Pour arrêter la mise à jour, cliquez sur **Arrêter**.

# CONFIGURATION DE LA MISE A JOUR DES BASES PROGRAMMEE

*Pour configurer la mise à jour programmée des bases de l'Antivirus, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer la mise à jour programmée des bases de l'Antivirus pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

- si vous souhaitez configurer la mise à jour programmée des bases de l'Antivirus pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer la mise à jour des bases de l'Antivirus.

2. Sélectionnez le nœud **Mises à jour**.
3. Dans le panneau des résultats, déployez le groupe de paramètres **Mise à jour des bases de l'Antivirus**.
4. Dans la liste déroulante **Mode de lancement**, sélectionnez une des options suivantes :

   - **Périodiquement**. Dans le champ **toutes les <X> min/ h / jour**, désignez la fréquence des mises à jour des bases en minutes/heures/jours.
   - **Chaque jour**. Dans le champ à liste déroulante, indiquez l'heure précise locale du serveur.
   - **Le jour sélectionné**. Cochez les cases en regard des jours de la semaine où les bases de l'Antivirus devront être mises à jour, puis définissez l'heure de la mise à jour.

5. Cliquez sur le bouton **Enregistrer**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres de mise à jour programmée des bases de l'Anti-Virus configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer la mise à jour programmée sur les autres serveurs du DAG.

*Pour configurer la mise à jour programmée des bases de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer la mise à jour programmée des bases de l'Anti-Spam pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;
   - si vous souhaitez configurer la mise à jour programmée des bases de l'Anti-Spam pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer la mise à jour des bases de l'Anti-Spam.

2. Sélectionnez le nœud **Mises à jour**.
3. Dans le panneau des résultats, déployez le groupe de paramètres **Mise à jour des bases de l'Anti-Spam**.
4. Dans la liste déroulante **Mode de lancement**, sélectionnez une des options suivantes :

   - **Périodiquement**. Dans le champ **toutes les <X> min/ h / jour**, désignez la fréquence des mises à jour des bases en minutes/heures/jours.
   - **Chaque jour**. Dans le champ à liste déroulante, indiquez l'heure précise locale du serveur.
   - **Le jour sélectionné**. Cochez les cases en regard des jours de la semaine où les bases de l'Anti-Spam devront être mises à jour, puis définissez l'heure de la mise à jour.

5. Cliquez sur le bouton **Enregistrer**.

# SELECTION DE LA SOURCE DES MISES A JOUR

*Pour sélectionner la source des mises à jour des bases de l'Antivirus, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez sélectionner la source des mises à jour des bases de l'Antivirus pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

- Si vous souhaitez sélectionner la source des mises à jour des bases de l'Antivirus pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez sélectionner la source des mises à jour.

2. Sélectionnez le nœud **Mises à jour**.

3. Dans le panneau des résultats, développez le groupe de paramètres **Mise à jour des bases de l'Anti-Virus** et sélectionnez une des options suivantes :

   - Si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab, choisissez l'option **Serveurs de mise à jour de Kaspersky Lab**.

     Cette source de mises à jour est sélectionnée par défaut.

   - Si vous souhaitez télécharger les mises à jour depuis un serveur intermédiaire, un dossier réseau ou un dossier local, choisissez l'option **Serveur HTTP, FTP, dossier local ou réseau**. Ensuite, saisissez dans le champ l'adresse du serveur ou le chemin d'accès complet au dossier local ou réseau.

   - Si vous souhaitez charger les mises à jour depuis le centre de mises à jour, choisissez l'option **Stockage du centre de mises à jour**. Ensuite, sélectionnez le serveur centre de mises à jour dans la liste déroulante.

     Vous pouvez désigner cette source de mises à jour si au moins un centre de mises à jour a été créé dans votre configuration (cf. section «Désignation d'un serveur comme centre de mises à jour et configuration de ses paramètres» à la page 57). Si le serveur Microsoft Exchange pour lequel vous sélectionnez la source de mises à jour a été déployé dans le rôle Transport Edge, le nom du serveur centre de mises à jour n'apparaîtra peut-être pas dans la liste déroulante. Dans ce cas, saisissez manuellement le nom du serveur centre de mises à jour.

4. Cliquez sur le bouton **Enregistrer**.

Si l'application fonctionne dans un cluster ou un DAG de serveurs Microsoft Exchange, les paramètres de mise à jour des bases de l'Antivirus (en particulier, la source de mises à jour) définis sur un des serveurs sont appliqués automatiquement aux autres serveurs du cluster ou du DAG. Il n'est pas nécessaire de configurer les paramètres de la mise à jour sur les autres serveurs du DAG.

*Pour sélectionner la source des mises à jour des bases de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez sélectionner la source des mises à jour des bases de l'Anti-Spam pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - Si vous souhaitez sélectionner la source des mises à jour des bases de l'Anti-Spam pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez sélectionner la source des mises à jour.

2. Sélectionnez le nœud **Mises à jour**.

3. Dans le panneau des résultats, développez le groupe de paramètres **Mise à jour des bases de l'Anti-Spam** et réalisez une des opérations suivantes :

   - Si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab, choisissez l'option **Serveurs de mise à jour de Kaspersky Lab**.

     Cette source de mises à jour est sélectionnée par défaut.

   - Si vous souhaitez télécharger les mises à jour depuis un serveur intermédiaire, un dossier réseau ou un dossier local, choisissez l'option **Serveur HTTP, FTP, dossier local ou réseau**. Ensuite, saisissez dans le champ l'adresse du serveur ou le chemin d'accès complet au dossier local ou réseau.

- Si vous souhaitez charger les mises à jour depuis le centre de mises à jour, choisissez l'option **Stockage du centre de mises à jour**. Ensuite, sélectionnez le serveur centre de mises à jour dans la liste déroulante.

  Vous pouvez choisir cette source de mises à jour si au moins un centre de mises à jour a été créé dans votre configuration. Si le serveur Microsoft Exchange pour lequel vous sélectionnez la source de mises à jour a été déployé dans le rôle Transport Edge, le nom du serveur centre de mises à jour n'apparaîtra peut-être pas dans la liste déroulante. Dans ce cas, saisissez manuellement le nom du serveur centre de mises à jour.

4. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES PARAMETRES DE CONNEXION A LA SOURCE DES MISES A JOUR

*Pour configurer les paramètres de connexion à la source des mises à jour, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres de connexion à la source des mises à jour pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les paramètres de connexion à la source des mises à jour pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres de connexion à la source des mises à jour.

2. Sélectionnez le nœud **Mises à jour**.

3. Dans le panneau des résultats, déployez le groupe de paramètres **Configuration de connexion**.

4. Si la connexion à Internet s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy**.

5. Dans le champ **Délai d'attente maximum pour la connexion**, saisissez le délai d'attente maximum pour la connexion avec la source de mises à jour (en secondes).

   Il s'agit de la période pendant laquelle le serveur Microsoft Exchange tente de se connecter à la source des mises à jour. Par défaut, la valeur de ce paramètre est égale à 60 secondes. Il faudra peut-être augmenter cette valeur si votre connexion à Internet est lente.

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

Si la connexion à Internet s'opère via un serveur proxy, il convient de configurer les paramètres du serveur proxy (cf. section "Configuration du serveur proxy" à la page 56).

# CONFIGURATION DES PARAMETRES DU SERVEUR PROXY

*Pour configurer les paramètres du serveur proxy, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres de connexion au serveur proxy pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

- si vous souhaitez configurer les paramètres de connexion au serveur proxy pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres de connexion au serveur proxy.

2. Sélectionnez le nœud **Configuration**.
3. Dans le panneau des résultats, déployez le groupe de paramètres **Paramètres du serveur proxy**.
4. Dans le champ **Adresse du serveur proxy**, saisissez l'adresse du serveur proxy.
5. Indiquez le numéro du port du serveur proxy dans le champ **Port**.

   Le port utilisé par défaut est 8080.
6. Si la connexion au serveur proxy requiert une authentification, cochez la case **Utiliser l'authentification**, puis indiquez le compte utilisateur sélectionné dans le champ **Compte utilisateur** et le mot de passe, dans le champ **Mot de passe**.
7. Cliquez sur le bouton **Enregistrer**.

# DESIGNATION D'UN SERVEUR COMME CENTRE DE MISES A JOUR ET CONFIGURATION DE SES PARAMETRES

Il est déconseillé de désigner un centre de mise à jour et de le configurer pendant la mise à jour vers une nouvelle version de l'application sur les serveurs appartenant à des configurations de cluster ou de DAG de serveurs Microsoft Exchange. Les actions décrites dans cette section doivent être réalisées uniquement après la fin de la mise à jour de l'application sur tous les serveurs (pour en savoir plus, voir le *Guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Servers*).

Il est déconseillé de désigné un serveur virtuel Microsoft Exchange en tant que centre de mises à jour.

Le serveur Microsoft Exchange désigné comme centre de mises à jour doit être connecté en permanence à Internet et il doit compter 500 Mo d'espace disque supplémentaire.

*Pour désigner un serveur comme centre de mises à jour et configurer ses paramètres, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez le nœud **Mises à jour**.
3. Dans la panneau des résultats, déployez le groupe de paramètres **Paramètres du centre de mises à jour**.
4. Cochez la case **Le serveur est le centre de mises à jour**.
5. Sélectionnez la source de mises à jour où le centre de mises à jour va récupérer les bases.

   - Si vous souhaitez télécharger les mises à jour dans le centre de mises à jour depuis les serveurs de Kaspersky Lab, choisissez l'option **Serveurs de mise à jour de Kaspersky Lab**.

     Cette source de mises à jour est sélectionnée par défaut.

   - Si vous souhaitez télécharger les mises à jour dans le centre de mises à jour depuis un serveur intermédiaire, un dossier réseau ou un dossier local, choisissez l'option **Serveur HTTP, FTP, dossier local ou réseau**. Ensuite, saisissez dans le champ l'adresse du serveur ou le chemin d'accès complet au dossier local ou réseau.

- Si vous souhaitez charger les mises à jour dans le centre de mises à jour depuis un autre centre de mises à jour, choisissez l'option **Stockage du centre de mises à jour**. Ensuite, sélectionnez le serveur centre de mises à jour dans la liste déroulante.

6. Programmez la mise à jour des bases pour le centre de mises à jour. Pour ce faire, choisissez une des options suivantes dans la liste déroulante **Mode de lancement** :

   - **Périodiquement**. Désignez la fréquence de la mise à jour des bases via la liste **Toutes les X minutes / heures / 24 heures**.

   - **Chaque jour**. Indiquez l'heure locale exacte dans le champ **à HH**:**MM**.

   - **Le jour sélectionné**. Cochez les cases en regard des jours de la semaine où les bases devront être mises à jour, puis définissez l'heure de la mise à jour.

   Il est déconseillé de choisir le mode de lancement **Manuel** pour le centre de mises à jour car dans ce cas, il est impossible de garantir l'actualité des bases dans le centre et sur tous les serveurs qui utilisent ce centre en guise de source de mises à jour.

7. Si la connexion à Internet s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy pour le centre de mises à jour** et configurez les paramètres du serveur proxy selon une des options suivantes :

   - Si vous souhaitez connecter le centre de mises à jour à Internet en utilisant les paramètres du serveur proxy indiqué dans e nœud **Configuration**, choisissez l'option **Utiliser les paramètres du serveur proxy définis dans le nœud "Configuration"**.

   - Si vous souhaitez connecter le centre de mises à jour à Internet en utilisant d'autres paramètres du serveur proxy, choisissez l'option **Définir les paramètres du serveur proxy pour le chargement des mises à jour par le centre de mises à jour** et réalisez les opérations suivantes :

     a. Saisissez l'adresse et le port du serveur proxy dans les champs **Adresse du serveur proxy** et **Port** respectivement.

     b. Si la connexion au serveur proxy requiert une authentification, cochez la case **Utiliser l'authentification**, puis indiquez le compte utilisateur sélectionné dans le champ **Compte utilisateur** et le mot de passe, dans le champ **Mot de passe**.

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

Le serveur Microsoft Exchange sélectionné sera désigné comme centre de mises à jour. Plus tard, il pourra être sélectionné en tant que source de mises à jour pour les autres serveurs (cf. section « Sélection de la source de la mise à jour » à la page 54).

# PROTECTION ANTIVIRUS

Cette section décrit la protection antivirus du serveur Microsoft Exchange, l'analyse des banques en arrière-plan et la configuration des paramètres de protection et d'analyse.

### DANS CETTE SECTION DE L'AIDE


Présentation de la protection antivirus ..... 59

Présentation de la participation au Kaspersky Security Network ..... 61

À propos de la technologie ZETA Shield ..... 61

Activation et désactivation de la protection antivirus du serveur ..... 61

Activation et désactivation de KSN dans l'Antivirus ..... 63

Activation et désactivation de la technologie ZETA Shield ..... 63

Configuration des paramètres de traitement des objets ..... 64

Configuration des paramètres de protection des boîtes aux lettres et des dossiers publics ..... 65

Configuration des exclusions de l'analyse antivirus ..... 66

Configuration des paramètres de l'analyse en arrière-plan ..... 70


# A PROPOS DE LA PROTECTION ANTIVIRUS

Une des fonctions principale de Kaspersky Security est de garantir la protection antivirus dans le cadre de laquelle l'application recherche la présence éventuelle de virus dans le flux de messagerie et dans les messages des boîtes aux lettres et répare les objets infectés à l'aide des bases de l'Antivirus.

L'application analyse en temps réel tous les messages qui arrivent sur le serveur Microsoft Exchange. L'application traite le trafic de messagerie entrant et sortant, ainsi que le trafic des messages en transit. Si la protection antivirus du serveur est activée, le lancement et l'arrêt de l'analyse du trafic de messagerie s'opèrent en même temps que le lancement et l'arrêt du serveur Microsoft Exchange.

Quand la protection antivirus du serveur est activée, l'application se trouve en permanence dans la mémoire vive de l'ordinateur. L'intercepteur de messages analyse le flux de messagerie électronique en provenance du serveur Microsoft Exchange et transmet les messages électroniques au module Antivirus pour le traitement.

L'Antivirus analyse les messages électroniques à l'aide de la dernière version des bases téléchargée, du dispositif d'analyse heuristique, et du service dans le nuage Kaspersky Security Network, si l'utilisation de ce service pour la protection antivirus est activée (cf. section "Activation et désactivation de KSN dans l'Antivirus" à la page 63).

Au terme de l'analyse de l'Antivirus, l'un des états suivants est attribué à chaque objet :

- *Infecté* : contient au moins un virus connu.
- *Sain* : ne contient pas de virus.
- *Protégé* : l'objet est protégé par un mot de passe.
- *Endommagé* : l'objet est endommagé.

Si un message électronique est endommagé ou partiellement endommagé, l'Antivirus traite l'objet malveillant détecté conformément aux paramètres définis (cf. section "Configuration des paramètres de traitement des objets" à la page 64).

Vous pouvez configurer l'exécution des actions suivantes sur les messages contenant des objets malveillants :

- Ignorer le message et l'objet malveillant qu'il contient.
- Supprimer l'objet malveillant et laisser passer le message.
- Supprimer le message et l'objet malveillant.

Avant le traitement, une copie du message peut être enregistrée dans la sauvegarde (cf. page 89).

Lors de la suppression d'un objet malveillant sur un serveur Microsoft Exchange, déployé dans un rôle de boîte aux lettres, le message ou la pièce jointe contenant l'objet malveillant est remplacé par un fichier texte qui reprend le nom de l'objet malveillant, la date d'édition des bases qui ont permis de détecter l'objet et nom du serveur Microsoft Exchange sur lequel l'objet a été détecté. Si l'objet malveillant a été détecté sur un serveur Microsoft Exchange, déployé dans le rôle de transport Hub, le texte Malicious object deleted est également ajouté à l'objet du message.

Si l'utilisateur dont les boîtes aux lettres sont protégées crée des messages dans les dossiers partagés de serveurs non protégés Microsoft Exchange, Kaspersky Security n'analyse pas ces messages. Quand un message est transféré depuis les Dossiers publics d'une banque non protégée vers une banque protégée, il est analysé par l'application. Lors de la réplication des données entre des banques protégées et non protégées, les modifications introduites par l'application suite à l'analyse antivirus ne sont pas synchronisées.

Si l'analyse en arrière-plan des banques est activée (cf. section "Configuration des paramètres de l'analyse en arrière-plan"à la page 70), l'application analyse à intervalle régulier les messages stockés sur le serveur Microsoft Exchange ainsi que le contenu des dossiers partagés à l'aide de la dernière version des bases. L'analyse en arrière-plan permet de réduire la charge sur les serveurs aux heures de pointe et d'augmenter la sécurité de l'infrastructure de messagerie dans son ensemble. L'analyse a lieu en arrière-plan et peut être lancée manuellement ou selon une programmation définie.

L'analyse en arrière-plan peut entraîner un ralentissement du serveur Microsoft Exchange et par conséquent, il est conseillé d'utiliser ce type d'analyse quand la charge des serveurs de messagerie est minime, par exemple pendant la nuit.

Pendant l'analyse en arrière-plan, l'application reçoit du serveur Microsoft Exchange, conformément aux paramètres, tous les messages situés dans les dossiers publics et dans les banques protégées. Si le message n'a pas été analysé à l'aide des bases antivirus les plus récentes, l'application le transmet au module Antivirus pour traitement. Le traitement des objets pendant l'analyse en arrière-plan se déroule comme pour l'analyse antivirus du flux de messagerie en temps réel.

L'application vérifie le contenu du message ainsi que les pièces jointes, quel que soit leur format.

Kaspersky Security distingue différents types d'objets : un objet simple (corps de message, pièce jointe simple, par exemple sous la forme d'un fichier exécutable) et un objet conteneur (composé de plusieurs objets, par exemple une archive, un message avec un message joint).

Lors de l'analyse d'archives multivolume, chaque volume est traité par l'application comme un objet séparé. Dans cas, Kaspersky Security peut découvrir le code malveillant uniquement s'il est contenu entièrement dans un de ces volumes. Si le code malveillant est également scindé en plusieurs parties lors du chargement partiel des données, il ne sera pas détecté dans le cadre de l'analyse. La propagation d'un code malveillant après le rétablissement de l'intégrité de l'objet reste alors une possibilité. Les archives multivolumes peuvent être analysées après l'enregistrement sur le disque par l'application antivirus installée sur l'ordinateur de l'utilisateur.

Le cas échéant, vous pouvez définir une liste d'objets qui ne seront pas soumis à l'analyse antivirus. Vous pouvez exclure de l'analyse les archives, tous les objets conteneur au-delà d'un niveau d'imbrication défini, des fichiers selon des masques de noms et des messages envoyés à des destinataires définis (cf. section « Configuration des exclusions de l'analyse antivirus » à la page 66).

Les fichiers dont la taille est supérieure à 1 Mo sont enregistrés pour le traitement dans le dossier de service store situé dans le dossier data de conservation des données de l'application. Le dossier data contient également le référentiel de

fichiers temporaires, le dossier tmp. Il faut exclure les dossiers store et tmp de l'analyse réalisée par des logiciels tournant sur des ordinateurs dotés d'un serveur Microsoft Exchange.

# PRESENTATION DE LA PARTICIPATION AU KASPERSKY SECURITY NETWORK

Afin d'améliorer l'efficacité de la protection de l'ordinateur de l'utilisateur, Kaspersky Security utilise les données obtenues auprès d'utilisateurs issus du monde entier. Le réseau *Kaspersky Security Network* permet de récolter ces données.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la banque de solutions de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs de l'Anti-Spam est réduite.

L'implication des utilisateurs dans le Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les types et les sources des nouvelles menaces, de développer des moyens de neutralisation et de traiter les messages non sollicités avec une plus grande précision.

De plus, la participation au Kaspersky Security Network donne accès aux données sur la réputation des applications et des sites Internet.

Si vous participez au Kaspersky Security Network, certaines statistiques, obtenues pendant l'utilisation de Kaspersky Security sur l'ordinateur de l'utilisateur sont envoyées automatiquement à Kaspersky Lab (cf. section "Présentation de la divulgation des données" à la page 26). De même, des fichiers (ou leurs parties) dont le risque d'utilisation par les individus malintentionnés peut nuire à l'ordinateur ou aux données peuvent être envoyés à Kaspersky Lab pour une analyse complémentaire.

Vous pouvez activer ou désactiver l'utilisation du Kaspersky Security Network dans le cadre du fonctionnement de l'Antivirus (cf. section "Activation et désactivation de KSN dans l'Antivirus" à la page 63) et de l'Anti-spam (cf. section "Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing" à la page 78) séparément.

La participation au Kaspersky Security Network est volontaire. Vous pouvez suspendre à tout moment votre participation au Kaspersky Security Network. Les données personnelles de l'utilisateur ne sont ni recueillies, ni traitées, ni enregistrées. Pour en savoir plus sur les données que Kaspersky Security transmet à Kaspersky Security Network, vous pouvez également lire les conditions de KSN.

# À PROPOS DE LA TECHNOLOGIE ZETA SHIELD

La technologie ZETA Shield permet de détecter les attaques ciblées sur le réseau local d'une entreprise, de les distinguer des autres logiciels malveillants et de les contrer efficacement. Les attaques ciblées exploitent une vulnérabilité connue d'un réseau local et sont généralement destinées à un nombre limité de destinataires. La technologie ZETA Shield est utilisée conjointement avec le module Antivirus.

Vous pouvez activer ou désactiver la technologie ZETA Shield (cf. section "Activation et désactivation de la technologie ZETA Shield" à la page 63). L'utilisation de la technologie ZETA Shield est activée par défaut.

# ACTIVATION ET DESACTIVATION DE LA PROTECTION ANTIVIRUS DU SERVEUR

Lorsque la protection antivirus du serveur est activée, l'analyse antivirus du flux de messagerie est lancée et arrêtée en même temps que le lancement et l'arrêt du serveur Microsoft Exchange. L'analyse en arrière-plan des banques (cf.

section "Configuration des paramètres de l'analyse en arrière-plan" à la page 70) peut être lancée manuellement ou automatiquement selon une planification.

La désactivation de la protection antivirus du serveur augmente sensiblement le risque de pénétration d'un programme malveillant via le système de messagerie. Il n'est dès lors pas recommandé de désactiver la protection antivirus sans raison.

La protection antivirus du serveur Microsoft Exchange déployé dans les rôles de boîte aux lettres ou de Transport Hub est activée séparément.

*Pour activer ou désactiver la protection antivirus du serveur Microsoft Exchange dans le rôle de boîte aux lettres, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez activer ou désactiver la protection antivirus d'un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - Si vous souhaitez activer ou désactiver la protection antivirus des Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité dont vous souhaitez configurer la protection antivirus.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de boîtes aux lettres**, réalisez une des opérations suivantes dans le groupe de paramètres **Paramètres d'analyse de l'Antivirus** :

   - Cochez la case **Activer la protection antivirus du rôle serveur de boîtes aux lettres** si vous souhaitez activer la protection antivirus du serveur Microsoft Exchange ;

   - Décochez la case **Activer la protection antivirus du rôle serveur de boîtes aux lettres** si vous souhaitez désactiver la protection antivirus du serveur Microsoft Exchange ;

4. Cliquez sur le bouton **Enregistrer**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, la protection antivirus d'un serveur dans le rôle de boîte aux lettres activée sur un des serveurs est activée automatiquement sur tous les autres serveurs du DAG. Il n'est pas nécessaire d'activer la protection antivirus du serveur dans le rôle de boîtes aux lettres sur les autres serveurs du DAG.

*Pour activer la protection antivirus du serveur Microsoft Exchange pour le rôle Transport Hub, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez activer ou désactiver la protection antivirus d'un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - Si vous souhaitez activer ou désactiver la protection antivirus des Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité dont vous souhaitez configurer la protection antivirus.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, réalisez une des opérations suivantes dans le groupe de paramètres **Paramètres d'analyse de l'Antivirus** :

   - Cochez la case **Activer la protection antivirus du rôle serveur de transport Hub** si vous souhaitez activer la protection antivirus du serveur Microsoft Exchange ;

- Décochez la case **Activer la protection antivirus du rôle serveur de transport Hub** si vous souhaitez désactiver la protection antivirus du serveur Microsoft Exchange ;

4. Cliquez sur le bouton **Enregistrer**.

# ACTIVATION ET DESACTIVATION DE KSN DANS L'ANTIVIRUS

*Pour activer ou désactiver l'utilisation de KSN dans l'Antivirus, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez activer ou désactiver KSN dans l'Antivirus pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez activer ou désactiver KSN dans l'Antivirus pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer la recherche d'éléments de phishing.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sélectionnez l'onglet **Paramètres avancés de l'Antivirus**.

4. Cochez la case **Utiliser Kaspersky Security Network (KSN)**.

   La case **Utiliser Kaspersky Security Network (KSN)** est accessible si la case **J'accepte les conditions de KSN** dans le groupe **Paramètres KSN** et dans l'entrée **Configuration** est cochée.

5. Le cas échéant, indiquez le délai d'attente maximum pour les requêtes adressées au serveur KSN via le champ **Durée maximale d'attente pour la requête à KSN**.

   La valeur par défaut est de 10 s.

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

# ACTIVATION ET DESACTIVATION DE LA TECHNOLOGIE ZETA SHIELD

*Pour activer ou désactiver l'utilisation de la technologie ZETA Shield, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez activer ou désactiver la technologie ZETA Shield pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez activer ou désactiver l'utilisation de la technologie ZETA Shield pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez effectuer cette action.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sélectionnez l'onglet **Paramètres avancés de l'Antivirus**.

4. Cochez/décochez la case **Utiliser la technologie ZETA Shield** si vous souhaitez activer/désactiver l'utilisation de la technologie ZETA Shield.

5. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES PARAMETRES DE TRAITEMENT DES OBJETS

Vous pouvez configurer le traitement antivirus des objets en sélectionnant une action que l'application devra exécuter sur chaque type d'objet.

Si le serveur Microsoft Exchange est déployé dans un rôle de boîte aux lettres ou de Transport Hub, les paramètres de traitement des objets pour ces rôles doivent être configurés séparément.

*Pour configurer les paramètres de traitement des objets, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres du traitement antivirus des objets pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les paramètres du traitement antivirus des objets pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres du traitement antivirus des objets.

2. Sélectionnez le nœud **Protection du serveur**.

3. Réalisez une des actions suivantes :

   - Si vous souhaitez configurer les paramètres de traitement des objets pour le serveur Microsoft Exchange dans le rôle de boîte aux lettres, sous l'onglet **Protection pour le rôle serveur de boîtes aux lettres** de la fenêtre des résultats, développez le groupe de paramètres **Paramètres d'analyse de l'Antivirus**.

   - Si vous souhaitez configurer les paramètres de traitement des objets pour un rôle de transport Hub, sous l'onglet **Protection pour le rôle serveur de transport Hub** du panneau des résultats, développez le groupe de paramètres **Paramètres d'analyse de l'Antivirus**.

4. Dans la liste déroulante **Objet infecté** de la rubrique **Paramètres de traitement des objets**, sélectionnez le type d'action à exécuter sur les objets infectés :

   - Si vous souhaitez que l'application accepte le message et l'objet infecté qu'il contient, choisissez l'option **Ignorer**.

   - Si vous souhaitez que l'application supprime l'objet infecté mais accepte le message, choisissez l'option **Supprimer l'objet**.

   - Si vous souhaitez que l'application supprime le message contenant l'objet infecté ainsi que toutes les pièces jointes, choisissez l'option **Supprimer le message**.

5. La protection d'un objet par mot de passe peut gêner l'analyse antivirus. Dans la liste déroulante **Objet protégé**, sélectionnez le type d'action à exécuter sur les objets protégés :

   - Sélectionnez l'option **Ignorer** si vous souhaitez que l'application accepte les messages avec des objets protégés par mot de passe.

   - Sélectionnez l'option **Supprimer le message** si vous souhaitez que l'application supprime les messages avec des objets protégés par mot de passe.

6. Dans la liste déroulante **Objet endommagé**, sélectionnez le type d'action :

   - Sélectionnez l'option **Ignorer** si vous souhaitez que l'application accepte les messages avec des objets endommagés.

   - Sélectionnez l'option **Supprimer le message** si vous souhaitez que l'application supprime les messages avec des objets endommagés.

7. Si vous souhaitez placer une copie d'un objet dans la sauvegarde (cf. page 89) avant de le traiter, cochez la case **Enregistrer une copie de l'objet dans la Sauvegarde**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres de traitement des objets configurés pour le rôle de serveur de boîte aux lettres sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres de traitement des objets pour le rôle de serveur de boîte aux lettres sur les autres serveurs du DAG. Toutefois, les paramètres de traitement des objets pour le rôle de serveur de transport Hub doivent être configurés individuellement sur chaque serveur du DAG.

# CONFIGURATION DES PARAMETRES DE PROTECTION DES BOITES AUX LETTRES ET DES DOSSIERS PUBLICS

L'application protège un nombre de boîtes aux lettres définit par les dispositions de la clé active (cf. section "Consultation des informations relatives aux clés" à la page 28). Si le nombre de boîtes couvertes par la licence n'est pas suffisant, vous pouvez transférer la protection de certaines des boîtes aux lettres à d'autres. Pour ce faire, vous pouvez déplacer les boîtes dont vous avez désactivé la protection dans les banques qui ne seront pas protégées. Par défaut, tous les dossiers partagés du serveur de messagerie sont également soumis à la protection. Vous pouvez désactiver la protection des dossiers partagés si vous estimez que celle-ci n'est pas nécessaire.

L'application protège les banques de messageries et les banques de dossiers partagés du serveur Microsoft Exchange protégé qui existaient déjà lors de l'installation de l'application ainsi que toutes les nouvelles banques.

*Pour configurer la protection des boîtes aux lettres et des dossiers publics, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres de protection des boîtes aux lettres et des dossiers partagés pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les paramètres de protection des boîtes aux lettres et des dossiers partagés pour les serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres de la protection des boîtes aux lettres et des dossiers partagés.

2. Sélectionnez le nœud **Protection du serveur**.

3. Sous l'onglet **Protection antivirus pour le rôle serveur de boîtes aux lettres** de la fenêtre des résultats, développez le groupe de paramètres **Protection des boîtes aux lettres**.

   Les listes **Banques de boîtes aux lettres à protéger** et **Banques de dossiers publics à protéger** reprennent les banques de boîtes aux lettres et de dossiers publics du serveur Microsoft Exchange protégé.

   Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, ces listes reprennent les banques de boîtes aux lettres et de dossiers publics qui se trouvent sur tous les serveurs de ce DAG.

   Lors de la consultation du profil, la liste **Banques de boîtes aux lettres à protéger** reprend uniquement les boîtes aux lettres des serveurs Microsoft Exchange doté du module Antivirus pour le rôle Boîte aux lettres.

4. Dans la liste **Banques de boîtes aux lettres à protéger**, cochez les cases en regard des banques de boîtes aux lettres que vous souhaitez protéger.

5. Dans la liste **Banques de dossiers publics**, cochez les cases en regard des banques des dossiers publics que vous souhaitez protéger.

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

# CONFIGURATION DES EXCLUSIONS DE L'ANALYSE ANTIVIRUS

Afin de réduire la charge sur le serveur lors de l'analyse antivirus, vous pouvez configurer des exclusions qui limitent la liste d'objets à analyser. Les exclusions de l'analyse antivirus fonctionnent aussi bien pendant l'analyse du flux de messagerie que lors de l'analyse en arrière-plan des banques.

Vous pouvez configurer des exclusions de l'analyse antivirus d'une des manières suivantes :

- Désactiver l'analyse des archives et des objets-conteneurs (cf. section « Configurer les paramètres d'analyse des archives et des objets-conteneurs joints » à la page 70).

- Configurer les exclusions selon un masque de noms de fichiers (cf. rubrique « Configuration des exclusions selon des masques de fichiers » à la page 69).

  Les fichiers dont le nom correspondant au masque défini ne sont pas soumis à la recherche de virus.

- Configurer les exclusions selon les adresses des destinataires.

  Les messages envoyés aux destinataires indiqués ne sont pas soumis à la recherche de virus.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les exclusions de l'analyse en arrière-plan configurées sur un des serveurs sont appliquées automatiquement aux autres serveurs Microsoft Exchange du DAG. Il n'est pas nécessaire de configurer les exclusions de l'analyse pour les autres serveurs du DAG.

# PRESENTATION DES DESTINATAIRES DE CONFIANCE

Vous pouvez exclure de l'analyse antivirus les messages envoyés à des destinataires particuliers en ajoutant l'adresse de ces derniers à la liste des *destinataires de confiance* (cf. section « *Configuration des exclusions selon les adresses des destinataires* » à la page 67). Par défaut, la liste est vide.

Vous pouvez ajouter des adresses de destinataires à la liste des destinataires de confiance sous la forme des entrées suivantes :

- Objets Active Directory :

  - Simples utilisateurs (User).

  - Contacts (Contact).

  - Groupes de diffusion (Distribution Group).

  - Groupes de sécurité (Security Group).

  Il est conseillé d'ajouter les adresses sous la forme d'entrées de ce type.

- Adresses SMTP au format mailbox@domain.com.

  Les entrées de ce type doivent être ajoutées si l'Antivirus pour le rôle serveur de transport Hub est activé et si l'adresse à exclure est introuvable dans Active Directory.

Pour exclure le dossier public de l'analyse par l'Antivirus pour le rôle serveur de transport Hub, il faut ajouter à la liste des destinataires de confiance toutes ses adresses SMTP s'il en possède plusieurs. Si certaines adresses SMTP du dossier public manquent à la liste, il se peut que les messages qui arrivent dans le dossier public soient analysés par l'Antivirus.

- Noms d'utilisateurs ou de groupes (Display Name).

  Les entrées de ce type doivent être ajoutées si l'Antivirus pour le rôle de boîte aux lettres est activé et si l'adresse à exclure est introuvable dans Active Directory.

- Dossiers publics (Public Folder).

  Les enregistrements de ce type doivent être ajoutés si l'Antivirus est installé pour le rôle de serveur de boîtes aux lettres. Les dossiers publics ne peuvent être sélectionnés depuis Active Directory. Pour ajouter ces enregistrements, il faut indiquer le chemin d'accès complet au dossier public.

Si l'Antivirus pour le rôle de boîte aux lettres et le rôle de serveur de transport Hub est activé et si l'adresse à exclure est introuvable dans Active Directory, il faut ajouter à la liste des destinataires deux entrées qui correspondent à l'adresse : adresse SMTP et nom de l'utilisateur/du groupe. Dans le cas contraire, les messages envoyés à cette adresse ne seront pas exclus de l'analyse.

Les adresses des destinataires définies sous la forme d'objets Active Directory sont exclues de l'analyse antivirus selon les règles suivantes :

- Si l'adresse du destinataire est définie sous la forme d'un simple utilisateur, d'un contact ou d'un dossier public, les messages qui lui sont destinés sont exclus de l'analyse.

- Si l'adresse est définie sous la forme d'un groupe de diffusion, les messages destinés à ce groupe sont exclus de l'analyse. Toutefois, les messages adressés personnellement aux membres du groupe ne sont pas exclus de l'analyse si ces adresses n'ont pas été ajoutées séparément à la liste.

- Si l'adresse est définie en tant que groupe de sécurité, les messages destinés à ce groupe et à ses membres sont exclus de l'analyse. Toutefois, si un membre du groupe est un groupe de sécurité intégré, les messages destinés à ses membres ne sont pas exclus de l'analyse si ces adresses n'ont pas été ajoutées séparément à la liste.

L'application actualise automatiquement les adresses des destinataires obtenues via Active Directory après la modification des entrées correspondantes dans Active Directory (par exemple, en cas de modification de l'adresse électronique de l'utilisateur ou en cas d'ajout d'un nouveau membre au groupe de sécurité). L'actualisation s'opère une fois par jour.

## CONFIGURATION DES EXCLUSIONS SELON LES ADRESSES DES DESTINATAIRES

Vous pouvez exclure de la recherche de virus dans les messages destinés à des destinataires particuliers en indiquant les adresses de ces destinataires dans la liste des destinataires de confiance.

*Pour configurer les exclusions en fonction des adresses des destinataires, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les exclusions selon les adresses de destinataire pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les exclusions selon les adresses de destinataire pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer les exclusions.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sélectionnez l'onglet **Paramètres avancés de l'Antivirus**.
4. Cochez la case **Ne pas analyser les messages pour les destinataires**.
5. Ajoutez l'adresse du destinataire à la liste des adresses de confiance. Pour ce faire, procédez comme suit :
   - Pour ajouter un enregistrement d'Active Directory à la liste, procédez comme suit :
     a. cliquez sur le bouton ;
     b. dans la fenêtre qui s'ouvre, localisez l'enregistrement requis d'Active Directory, puis cliquez sur **OK**.

     Les adresses sélectionnées dans Active Directory sont désignées par les icônes suivantes dans la liste :
     - – utilisateurs simples, contacts, groupes de diffusion ;
     - – groupes de sécurité.
   - Pour ajouter l'adresse SMTP à la liste, le nom d'utilisateur ou le dossier partagé, procédez comme suit :
     - Pour ajouter une adresse SMTP ou un nom d'utilisateur, saisissez les données dans le champ, puis cliquez sur le bouton .
     - Pour ajouter un dossier partagé, saisissez le chemin d'accès au dossier et cliquez sur le bouton .

     Les adresses ajoutées de cette manière sont accompagnées de l'icône .

     Les adresses ajoutées de cette manière ne sont pas soumises au contrôle de leur existence dans Active Directory.
6. Pour supprimer l'adresse d'un destinataire de la liste des destinataires de confiance, sélectionnez la ligne contenant le destinataire, puis cliquez sur le bouton .
7. Pour exporter la liste des destinataires de confiance dans un fichier, procédez comme suit :
   a. cliquez sur le bouton ;
   b. dans la fenêtre qui s'ouvre, saisissez le nom du fichier dans le champ **Nom du fichier**.
   c. Cliquez sur le bouton **Enregistrer**.
8. Pour importer la liste des adresses de confiance depuis un fichier, procédez comme suit :
   a. cliquez sur le bouton ;
   b. dans le champ **Nom du fichier** de la fenêtre qui s'ouvre, saisissez le nom du fichier contenant la liste des destinataires de confiance.
   c. Cliquez sur le bouton **Ouvrir**.
9. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES EXCLUSIONS SELON DES MASQUES DE FICHIERS

*Pour configurer les exclusions selon un masque de nom de fichiers, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer les exclusions selon des masques de nom de fichier pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;
   - si vous souhaitez configurer les exclusions selon des masques de nom de fichier pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer l'exclusion.
2. Sélectionnez le nœud **Protection du serveur**.
3. Dans le panneau des résultats, sélectionnez l'onglet **Paramètres avancés de l'Antivirus**.
4. Cochez la case **Ne pas analyser les fichiers en fonction des masques**.
5. Ajoutez le masque des noms de fichiers (ci-après, le masque) à la liste des masques. Pour ce faire, procédez comme suit :
   a. Saisissez le masque dans le champ.

**Exemples de masques de nom de fichier autorisés** :

- *.txt : tous les fichiers avec l'extension txt, par exemple readme.txt ou notes.txt ;
- readme.??? : tous les fichiers readme avec une extension de trois lettres, par exemple readme.txt ou readme.doc ;
- test : tous les fichiers portant le nom test sans extension.

   a. Cliquez sur le bouton  situé à droite du champ.

1. Pour supprimer un masque de la liste, sélectionnez la ligne contenant le masque, puis cliquez sur le bouton  .
2. Pour exporter la liste des masques dans un fichier, procédez comme suit :
   a. cliquez sur le bouton  ;
   b. dans la fenêtre qui s'ouvre, saisissez le nom du fichier dans le champ **Nom du fichier**.
   c. Cliquez sur le bouton **Enregistrer**.
3. Pour importer la liste des masques depuis un fichier, procédez comme suit :
   a. cliquez sur le bouton  ;
   b. indiquez le fichier contenant la liste des masques dans le champ **Nom du fichier**.
   c. Cliquez sur le bouton **Ouvrir**.
4. Cliquez sur le bouton **Enregistrer**.

# CONFIGURER LES PARAMETRES D'ANALYSE DES ARCHIVES ET DES OBJETS-CONTENEURS JOINTS

Kaspersky Security analyse par défaut les archives et les coffres-forts joints aux messages. Pour optimiser le fonctionnement de Kaspersky Security, réduire la charge sur le serveur et accélérer le traitement du flux de messagerie, vous pouvez désactiver l'analyse des pièces jointes ou limiter le niveau d'imbrication de tels objets. Il est déconseillé de désactiver l'analyse des pièces jointes pour une longue durée car elles peuvent contenir des virus et autres objets malveillants.

*Pour configurer l'analyse des archives jointes et des coffres-forts, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer l'analyse des archives intégrées et des coffres-forts pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;
   - si vous souhaitez configurer l'analyse dans les archives intégrées et les coffres-forts pour les Serveurs de sécurité profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez configurer les exclusions.
2. Sélectionnez le nœud **Protection du serveur**.
3. Dans le panneau des résultats, sélectionnez l'onglet **Paramètres avancés de l'Antivirus**.
4. Activez/désactivez l'analyse des archives intégrées et des coffres-forts, en exécutant une des actions suivantes :
   - Si vous voulez que l'application analyse tels objets, cochez la case **Vérifier les archives/les coffres-forts joints avec le niveau d'encastrement pas plus de N**.
   - Si vous voulez que l'application n'analyse pas tels objets, décochez cette case.
5. Indiquez le niveau d'imbrication accessible des coffres-forts joints et des archives dans le champ de saisie avec le roulement.
6. Cliquez sur le bouton **Enregistrer**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres d'analyse des archives et des coffres-forts configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres d'analyse des archives et des coffres-forts joints sur les autres serveurs du DAG.

# CONFIGURATION DES PARAMETRES DE L'ANALYSE EN ARRIERE-PLAN

En mode d'analyse en arrière-plan, Kas**persky Security** reçoit du serveur Microsoft Exchange, conformément aux paramètres, tous les messages situés dans les dossiers publics et dans les banques protégées et les analyse à l'aide des bases de l'Antivirus. Seuls les messages qui n'avaient pas encore été analysés à l'aide des bases de l'Antivirus les plus récentes sont analysés.

L'analyse en arrière-plan est disponible uniquement pour le serveur Microsoft Exchange déployé dans un rôle de boîte aux lettres. L'application analyse le corps du message et les fichiers joints conformément aux paramètres définis pour l'analyse antivirus du serveur Microsoft Exchange déployé dans le rôle de boîte aux lettres. L'analyse en arrière-plan n'est pas disponible pour les autres rôles.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres d'analyse en arrière-plan configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres d'analyse en arrière-plan sur les autres serveurs du DAG.

*Pour configurer et lancer l'analyse en arrière-plan des messages stockés sur le serveur et du contenu des dossiers publics, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres d'une analyse en arrière-plan pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer les paramètres d'une analyse en arrière-plan pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres d'analyse en arrière-plan.

2. Sélectionnez le nœud **Protection du serveur**.

3. Sous l'onglet **Protection pour le rôle serveur de boîtes aux lettres** de la fenêtre des résultats, développez le groupe de paramètres **Protection des boîtes aux lettres**.

4. Dans la section **Analyse en arrière-plan**, choisissez l'option souhaitée dans la liste déroulante **Planification** :

   - **Manuel**. L'analyse en arrière-plan est lancée manuellement.

   - **Chaque jour**. L'analyse en arrière-plan est exécutée chaque jour. Indiquez l'heure précise de l'analyse dans le champ de saisie de l'heure au format **<HH:MM>**.

   - **Le jour sélectionné**. L'analyse en arrière-plan est exécutée les jours sélectionnés. Cochez les cases en regard des jours de la semaine où vous souhaitez lancer l'analyse en arrière-plan et saisissez l'heure exacte de son lancement dans le champ au format **<HH:MM>**.

   - **Chaque mois**. L'analyse en arrière-plan est réalisée une fois par mois. Indiquez dans le champ le jour du mois où vous souhaitez lancer l'analyse en arrière-plan et précisez l'heure exacte du lancement dans le champ correspondant au format **<HH:MM>**.

5. Si vous souhaitez que l'application analyse le corps du message dans le cadre de l'analyse en arrière-plan, cochez la case **Vérifier le contenu du message**.

6. Si vous souhaitez que l'application analyse les messages reçus au cours d'une période définie avant l'analyse en arrière-plan, cochez la case **Vérifier uniquement les messages récents** et indiquez le nombre de jours dans le champ **Vérifier les messages reçus pas plus tard que <N> jours avant le lancement de l'analyse en arrière-plan**.

   La valeur maximale du paramètre est 364 jours.

7. Cochez la case **Limiter l'analyse dans le temps** et définissez la valeur du paramètre **Arrêter l'analyse dans <N> heures après le lancement** afin d'optimiser la durée de l'analyse.

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

9. Si vous souhaitez lancer l'analyse en arrière-plan du serveur Microsoft Exchange immédiatement, cliquez sur le bouton **Lancer l'analyse**.

   L'analyse en arrière-plan est lancée dans la minute qui suit le clic sur le bouton.

L'analyse en arrière-plan sera lancée uniquement sur le serveur Microsoft Exchange sur lequel le serveur de sécurité sélectionné est installé. Ceci concerne n'importe quelle configuration des serveurs Microsoft Exchange, y compris le DAG. Si vous souhaitez lancer l'analyse en arrière-plan immédiatement sur les autres serveurs du DAG, il faut la lancer séparément pour chaque serveur Microsoft Exchange.

10. Si vous souhaitez arrêter l'analyse en arrière-plan du serveur Microsoft Exchange, cliquez sur le bouton **Arrêter**.

L'analyse en arrière-plan est arrêtée dans la minute qui suit le clic sur le bouton.

# PROTECTION CONTRE LE COURRIER INDESIRABLE ET LE PHISHING

Cette section contient des informations sur le filtrage des spams et des éléments de phishing dans le flux de messagerie ainsi que des instructions sur la configuration des paramètres de ces fonctions.

### DANS CETTE SECTION DE L'AIDE


Présentation de la protection contre le courrier indésirable ..... 73

Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable ..... 75

Présentation de la lutte contre les tentatives de phishing ..... 76

Activation et désactivation de la protection du serveur contre le courrier indésirable ..... 77

Activation et désactivation de la recherche d'éléments de phishing dans les messages ..... 78

Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing ..... 78

Configuration des listes noire et blanche des expéditeurs ..... 80

Configuration de la liste blanche des destinataires ..... 82

Configuration de l'augmentation du classement de courrier indésirable d'un message` ..... 83

Recours à des services externes pour la détection du courrier indésirable ..... 85

Configuration des paramètres avancés de recherche de courrier indésirable et d'éléments de phishing ..... 87


## PRESENTATION DE LA PROTECTION CONTRE LE COURRIER INDESIRABLE

Une des principales tâches de Kaspersky Security consiste à filtrer le courrier indésirable dans le flux de messagerie qui transite via le serveur Microsoft Exchange. Le module Anti-Spam filtre le courrier entrant avant qu'il n'arrive dans les boîtes aux lettres des utilisateurs.

L'Anti-Spam analyse les types de données suivants :

- Le flux de messagerie interne et externe via le protocole SMTP avec vérification anonyme de l'authenticité sur le serveur.
- Les messages qui arrivent sur le serveur via des connexions externes anonymes (serveur edge).

L'Anti-Spam n'analyse pas les types de données suivants :

- Le flux de messagerie interne de l'organisation.
- Le flux de messagerie externe qui arrive sur le serveur via une session d'authentification. Vous pouvez activer manuellement l'analyse d'un tel flux de messagerie (cf. section « Configuration des paramètres avancés de recherche de courrier indésirable et d'éléments de phishing » à la page 87) à l'aide du paramètre **Analyser les connexions autorisées**.

- Les messages arrivant d'autres serveurs de l'infrastructure de messagerie Microsoft Exchange, car la connexion entre les serveurs d'une même infrastructure Microsoft Exchange est considérée comme fiable. Ainsi, si un message arrive sur l'infrastructure via un serveur sur lequel aucun Anti-Spam n'est installé ou activé, il ne sera pas analysé par le filtre anti-spam ni par aucun des serveurs suivants de l'infrastructure empruntés par le message. Vous pouvez activer manuellement l'analyse d'un tel flux de messagerie (cf. section « Configuration des paramètres avancés de recherche de courrier indésirable et d'éléments de phishing » à la page 87) à l'aide du paramètre **Analyser les connexions autorisées**.

L'Anti-Spam analyse les en-têtes et le contenu des messages, les fichiers joints, les éléments de composition et d'autres attributs du message. L'analyse repose sur l'utilisation d'algorithmes linguistiques et heuristiques à partir de la comparaison du message avec des exemples de messages ainsi que sur l'utilisation de services cloud supplémentaires comme Kaspersky Security Network (cf. section « Présentation de la participation au Kaspersky Security Network » à la page 61).

Sur la base des résultats du filtrage, l'Anti-Spam attribue un des états suivants aux messages :

- *Courrier indésirable*. Le message affiche des éléments caractéristiques du courrier indésirable.
- *Courrier indésirable potentiel*. Le message présente des caractéristiques du courrier indésirable, mais le classement de courrier indésirable ne permet pas de le classer comme tel.
- *Envoi massif*. Le message appartient à la catégorie des envois massifs (généralement des newsletters ou de la publicité) mais ne présente pas suffisamment de caractéristiques permettant de le considérer comme un spam.
- *Notification formelle*. Message technique, par exemple sur la remise d'un message au destinataire.
- *Normal*. Le message n'affiche aucun élément caractéristique du courrier indésirable.
- *Ajouté à la liste noire*. L'adresse IP de l'expéditeur du message ou son adresse de messagerie figure dans la liste noire des adresses.

Vous pouvez sélectionner les actions que l'application va exécuter sur les messages possédant un certain état (cf. section « Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing » à la page 78). Vous avez le choix entre les actions suivantes :

- **Ignorer**. Le message sera remis au destinataire sans aucune modification.
- **Rejeter**. Le serveur expéditeur reçoit un message d'erreur lors de l'envoi du message (code d'erreur 500) et le message n'est pas remis au destinataire.
- **Supprimer**. Le serveur expéditeur du message reçoit une notification sur l'envoi du message (code 250), mais ce message n'est pas remis au destinataire.
- **Ajouter un classement SCL**. Les messages recevront une évaluation sur la probabilité de courrier indésirable (SCL). L'évaluation SCL se présente sous la forme d'un nombre qui peut être compris entre 1 et 9. Un résultat SCL élevé indique une probabilité élevée que le message soit non sollicité. L'évaluation SCL s'obtient en divisant le classement de courrier indésirable du message par 10. Si à la fin du calcul la valeur est supérieure à 9, l'évaluation SCL est égale à 9. L'évaluation SCL attribuée aux messages est prise en compte lors du traitement ultérieur des messages par l'infrastructure Microsoft Exchange.
- **Ajouter une note à l'en-tête du message**. Les messages qui reçoivent l'état *Courrier indésirable*, *Courrier indésirable potentiel*, *Envois massifs* ou *Ajouté à la liste noire* sont signalés par les notes spéciales [!!SPAM], [!!Probable Spam] [!!Mass Mail] ou [!!Blacklisted] dans le champ Objet du message. Vous pouvez modifier le contenu de ces notes (cf. section « Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing » à la page 78).

L'application prend en charge quatre niveaux d'agressivité dans la recherche de courrier indésirable :

- *Maximal*. Ce niveau d'agressivité doit être utilisé si vous recevez très souvent des messages non sollicités. Si vous sélectionnez ce niveau d'agressivité, la fréquence d'identification d'un courrier normal en tant que courrier indésirable peut augmenter.
- *Élevé*. Si vous choisissez ce niveau, la fréquence de faux positif diminue (par rapport au niveau *maximal*) et la vitesse d'analyse augmente. Le niveau *Élevé* doit être utilisé si vous recevez souvent du courrier indésirable.

- *Faible*. Si vous choisissez ce niveau, la fréquence de faux positif diminue (par rapport au niveau *Élevé*) et la vitesse d'analyse augmente. Le niveau *Faible* offre la combinaison optimale de rapidité et de qualité de l'analyse.

- *Minimum*. Ce niveau d'agressivité doit être utilisé si vous recevez rarement des messages non sollicités.

Par défaut, la protection contre le courrier indésirable s'opère selon les paramètres du niveau *Faible*. Vous pouvez augmenter ou diminuer le niveau d'agressivité (cf. section « Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing » à la page 78). En fonction du niveau de contrôle de l'analyse et du classement obtenu suite à celle-ci, le message peut recevoir l'état *Courrier indésirable* ou *Courrier indésirable potentiel* (cf. tableau ci-dessous).

*Table 4. Seuils du classement de courrier indésirable en fonction du niveau d'agressivité de l'analyse*

| NIVEAU D'AGRESSIVITÉ | COURRIER POTENTIELLEMENT INDÉSIRABLE | COURRIER INDÉSIRABLE |
|---|---|---|
| Maximal | 60 | 75 |
| Élevé | 70 | 80 |
| Faible | 80 | 90 |
| Minimum | 90 | 100 |

# PRESENTATION DES SERVICES, DES FONCTIONS ET DES TECHNOLOGIES COMPLEMENTAIRES DE PROTECTION CONTRE LE COURRIER INDESIRABLE

Pour une protection plus poussée du courrier indésirable, l'application utilise les fonctions, les technologies et les services complémentaires suivants de Kaspersky Lab :

- DNSBL (Domain Name System Block List). Service de récupération d'informations depuis des serveurs DNSBL contenant des listes publiques d'adresses IP identifiées dans la diffusion de courrier indésirable.

- SURBL (Spam URI Realtime Block List). Service de récupération d'informations depuis des serveurs SURBL contenant des listes de liens publiques qui mènent à des ressources en ligne pour la promotion des expéditeurs de courrier indésirable. Ainsi, si le message contient une URL de cette liste, il sera considéré comme indésirable.

  Les listes des serveurs DNSBL et SURBL sont actualisées depuis les serveurs de mises à jour de Kaspersky Lab en même temps que les bases de l'Anti-Spam toutes les cinq minutes. Les réponses des serveurs DNSBL et SURBL sont prises en compte dans le calcul du classement de courrier indésirable du message. Le classement de courrier indésirable est un nombre entier compris entre 0 et 100. Le poids de chaque serveur DNSBL et SURBL qui répond est pris en compte dans le calcul du classement de courrier indésirable. Si le classement global des serveurs qui répondent est supérieur à 100, alors le classement de courrier indésirable du message atteint 100. Si le classement global est inférieur à 100, le classement de courrier indésirable du message n'est pas augmenté.

- KSN (Kaspersky Security Network). Infrastructure de service en ligne et de services qui améliorent la protection des utilisateurs, qui accélère la réaction des applications de Kaspersky Lab face aux nouvelles menaces et aux nouveaux exemples de courrier indésirable et qui réduit le nombre de faux positifs de l'Anti-Spam.

  Par défaut, la participation au KSN est désactivée (cf. section "Présentation de la participation au Kaspersky Security Network" à la page 61). Pour commencer à utiliser le service KSN, vous devez accepter les conditions

de KSN qui définissent l'ordre de réception et d'utilisation des informations en provenance d'un ordinateur sur lequel Kaspersky Security fonctionne.

- Enforced Anti-Spam Updates Service. Service de mise à jour rapide des bases de l'Anti-Spam Quand l'utilisation de l'Enforced Anti-Spam Updates Service est activée, l'application est en communication constante avec les serveurs de Kaspersky Lab et actualise les bases de l'Anti-Spam dès que de nouvelles définitions de messages indésirables sont chargées sur les serveurs de Kaspersky Lab. Ceci accélère la vitesse de réaction de l'Anti-Spam face aux nouvelles diffusions.

  Enforced Anti-Spam Updates Service requiert l'exécution des conditions suivantes :

  - connexion Internet permanente pour l'ordinateur sur lequel le Serveur de sécurité est installé.
  - mise à jour régulière des bases de l'Anti-Spam (la fréquence recommandée des mises à jour : chaque 5 minutes).

- Reputation Filtering. Service de réputation dans le Cloud pour l'analyse complémentaire des messages qui place les messages qui le nécessitent dans un dossier temporaire appelé la *quarantaine*. Pendant la période définie (50 minutes), l'application analyse à nouveau le message à l'aide d'informations complémentaires obtenues sur les serveurs de Kaspersky Lab (par exemple, via le réseau KSN). Si au cours de la période définie l'application ne parvient pas à classer le message parmi les messages non sollicités, il l'ignore. Le recours au service Reputation Filtering augmente la précision de l'identification du courrier indésirable et réduit la probabilité de faux positifs dans l'Anti-Spam.

  Pour pouvoir utiliser le service Reputation Filtering, vous devez confirmer votre participation à Kaspersky Security Network (KSN) et acceptez les conditions de l'accord KSN.

  Les messages placés par Reputation Filtering dans la quarantaine et qui ne sont pas considérés comme indésirables seront remis aux destinataires à l'issue des 50 minutes, même si l'application est arrêtée ou suspendue.

- Client DNS dynamique. Fonction qui définit l'appartenance potentielle de l'adresse IP de l'expéditeur à un réseau de zombies sur la base de sa zone DNS inverse. Cette fonction peut être utilisée si le serveur SMTP protégé ne sert pas ses propres utilisateurs avec une connexion xDSL ou Dial-up.

- Technologie SPF (Sender Policy Framework). Technologie qui permet de confirmer l'authenticité du domaine de l'expéditeur. À l'aide de la technologie SPF, les domaines reçoivent le droit d'envoyer du courrier en leur nom à des ordinateurs déterminés. Si l'expéditeur du message ne figure pas dans la liste des expéditeurs autorisés, le classement de courrier indésirable du message augmente.

# PRESENTATION DE LA LUTTE CONTRE LES TENTATIVES DE PHISHING

Kaspersky Security permet de rechercher la présence éventuelle de liens de phishing et de liens malveillants dans les messages.

Les liens de phishing mènent à des sites d'escroquerie dont le but est de voler les données personnelles des utilisateurs, par exemple un numéro de compte bancaire. L'exemple type de ce genre d'attaque est la reproduction d'un message qui aurait pu être envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse authentique du site s'affiche ; mais dans la majorité des cas, il s'agit d'un site fictif. Toutes vos actions sur ce site sont suivies et pourraient servir au vol de vos données personnelles.

Les liens malveillants renvoient vers des ressources Web destinées à diffuser un logiciel malveillant.

Pour protéger le serveur Microsoft Exchange contre le phishing et les liens malveillants, l'application utilise des bases de données d'URL que les experts de Kaspersky Lab ont identifiées comme URL de phishing ou comme URL malveillantes. Les bases sont actualisées régulièrement et elles sont livrées avec Kaspersky Security.

Dans le cadre de la recherche d'éléments de phishing ou de liens malveillants, l'application analyse non seulement les URL, mais également les en-têtes des messages, le contenu des messages, les pièces jointes, la mise en page et d'autres caractéristiques. L'analyse repose également sur l'utilisation d'algorithmes heuristiques et de requêtes envoyées au service dans le nuage Kaspersky Security Network (cf. section « Présentation de la participation au Kaspersky Security Network » à la page 61) (KSN), si l'utilisation du KSN pour l'Anti-spam est activée (cf. section « Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing » à la page 78). KSN permet à l'application d'obtenir des informations actualisées sur les URL de phishing et les URL malveillantes qui n'ont pas encore été ajoutées aux bases anti-phishing de Kaspersky Lab.

Si l'application découvre des éléments de phishing ou des liens malveillants dans un message, elle lui attribue l'état *Phishing*. Vous pouvez sélectionner les actions que l'application va exécuter sur les messages portant ce statut. Vous avez le choix entre les actions suivantes :

- **Ignorer**. Le message sera remis au destinataire sans aucune modification.
- **Rejeter**. Le serveur expéditeur reçoit un message d'erreur lors de l'envoi du message (code d'erreur 500) et le message n'est pas remis au destinataire.
- **Supprimer**. Le serveur expéditeur du message reçoit une notification sur l'envoi du message (code 250), mais ce message n'est pas remis au destinataire.
- **Ajouter un classement SCL et PCL**. Les messages se verront attribuer un coefficient de probabilité de courrier indésirable (SCL) égal à 9, et un coefficient de probabilité de phishing (PCL) égal à 8. Les messages dont l'évaluation PCL est élevée (supérieure à 3) seront automatiquement classés dans le dossier **Courrier indésirable** (**Junk E-Mail**) lorsqu'ils arriveront dans l'infrastructure de messagerie Microsoft Exchange et tous les liens qu'ils contiennent seront désactivés.
- **Ajouter une note à l'en-tête du message**. L' objet des messages qui reçoivent le statut *Phishing* est modifié par l'ajout de la note [!!Phishing]. Vous pouvez modifier le contenu de cette note (cf. section « Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing » à la page 78).

# ACTIVATION ET DESACTIVATION DE LA PROTECTION DU SERVEUR CONTRE LE COURRIER INDESIRABLE

La désactivation de la protection contre le courrier indésirable augmente sensiblement le risque de recevoir des messages non sollicités. Il est déconseillé de désactiver la protection contre le courrier indésirable sans raison.

*Pour activer ou désactiver la protection du serveur Microsoft Exchange contre le courrier indésirable, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez activer ou désactiver la protection contre le courrier indésirable pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;
   - si vous souhaitez activer ou désactiver la protection contre le courrier indésirable pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer la protection contre le courrier indésirable.
2. Sélectionnez le nœud **Protection du serveur**.
3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, dans le groupe **Paramètres d'analyse de l'Anti-Spam**, réalisez une des opérations suivantes :
   - Si vous souhaitez activer la protection contre le courrier indésirable, cochez la case **Activer le contrôle de la messagerie contre le courrier indésirable**.
   - Si vous souhaitez désactiver la protection contre le courrier indésirable, décochez la case **Activer le contrôle de la messagerie contre le courrier indésirable**.

4. Cliquez sur le bouton **Enregistrer**.

# ACTIVATION ET DESACTIVATION DE LA RECHERCHE D'ELEMENTS DE PHISHING DANS LES MESSAGES

Vous pouvez activer la recherche des éléments de phishing uniquement si la protection du serveur contre le courrier indésirable est activée. La recherche d'éléments de phishing active également la recherche de liens malveillants.

*Pour activer ou désactiver la recherche d'éléments de phishing, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez activer ou désactiver la recherche d'éléments de phishing pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez activer ou désactiver la recherche d'éléments de phishing pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer la recherche d'éléments de phishing.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, dans le groupe **Paramètres d'analyse de l'Anti-Spam**, réalisez une des opérations suivantes :

   - Si vous souhaitez activer la recherche d'éléments de phishing dans les messages, cochez la case **Activer le contrôle de la messagerie contre les tentatives de phishing**.

   - Si vous souhaitez désactiver la recherche d'éléments de phishing dans les messages, décochez la case **Activer le contrôle de la messagerie contre les tentatives de phishing**.

4. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES PARAMETRES DE RECHERCHE DE COURRIER INDESIRABLE ET D'ELEMENTS DE PHISHING

*Pour configurer les paramètres de recherche de courrier indésirable et d'éléments de phishing, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres de recherche de courrier indésirable et d'éléments de phishing pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les paramètres de recherche de courrier indésirable et d'éléments de phishing pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres de la recherche.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres d'analyse de l'Anti-Spam**.

4. Cochez la case **Activer le contrôle de la messagerie contre le courrier indésirable** si vous souhaitez que l'application analyse le courrier entrant à l'aide du module Anti-Spam.

5. Le curseur **Niveau d'analyse** permet de définir le niveau d'agressivité de la recherche de courrier indésirable (cf. section "Présentation de la protection contre le courrier indésirable" à la page 73) : **maximal**, **élevé**, **faible**, **minimal**.

6. Dans la liste déroulante **Action** du groupe **Paramètres de traitement du courrier indésirable**, sélectionnez l'action que l'application doit exécuter sur les messages en fonction de leur état (*Courrier indésirable*, *Courrier indésirable potentiel*, *Envois massifs*, *Notification formelle*, *Ajouté à la liste noire*) :

   - **Ignorer**. Le message sera remis au destinataire sans aucune modification.

   - **Rejeter**. Le serveur expéditeur reçoit un message d'erreur lors de l'envoi du message (code d'erreur 500) et le message n'est pas remis au destinataire.

   - **Supprimer**. Le serveur expéditeur reçoit une notification sur l'envoi du message (code 250), mais ce message n'est pas remis au destinataire.

7. Sélectionnez, dans le groupe **Paramètres de traitement du courrier indésirable**, les actions complémentaires que l'application doit exécuter sur les messages électroniques en fonction de son état. Cochez les cases en regard des options souhaitées :

   - **Ajouter un classement SCL**. Un classement de probabilité de courrier indésirable sera ajouté au message (évaluation SCL). L'évaluation SCL donne un résultat qui peut être compris entre 1 et 9. Un résultat SCL élevé indique une probabilité élevée que le message soit non sollicité. L'évaluation SCL attribuée aux messages est prise en compte lors du traitement ultérieur des messages par l'infrastructure Microsoft Exchange.

   - **Enregistrer une copie**. Une copie du message sera enregistrée dans la sauvegarde.

   - **Ajouter une note à l'en-tête du message**. Les messages qui reçoivent l'état *Courrier indésirable*, *Courrier indésirable potentiel* et *Ajouté à la liste noire* sont signalés par une note spéciale dans l'objet du message : [!!SPAM], [!!Probable Spam] [!!Mass Mail] et [!!Blacklisted] respectivement. Au besoin, modifiez le texte de ces notes dans les champs correspondant aux états.

8. Cochez la case **Activer le contrôle de la messagerie contre les tentatives de phishing** si vous souhaitez que l'application analyse le courrier entrant à l'aide du module Anti-Spam.

9. Dans le groupe de paramètres **Paramètres de traitement du courrier indésirable** sous la case **Activer le contrôle de la messagerie contre les tentatives de phishing** dans la liste déroulante **Action**, sélectionnez l'action que l'application doit exécuter sur les messages dont l'état est *Phishing*:

   - **Ignorer**. Le message sera remis au destinataire sans aucune modification.

   - **Rejeter**. Le serveur expéditeur reçoit un message d'erreur lors de l'envoi du message (code d'erreur 500) et le message n'est pas remis au destinataire.

   - **Supprimer**. Le serveur expéditeur reçoit une notification sur l'envoi du message (code 250), mais ce message n'est pas remis au destinataire.

10. Dans le groupe de paramètres **Paramètres de traitement du courrier indésirable** sous la case **Activer le contrôle de la messagerie contre les tentatives de phishing** , désignez les actions complémentaires que l'application doit exécuter sur les messages dont l'état est *Phishing*: Cochez les cases en regard des options souhaitées :

    - **Ajouter un classement SCL et PCL**. Les messages recevront une évaluation sur la probabilité de courrier indésirable (SCL) égale à 9 et une évaluation sur la probabilité de phishing (PCL) égale à 8. Les messages dont l'évaluation PCL est élevée (supérieure à 3) seront automatiquement classés dans le dossier **Courrier indésirable** (**Junk E-Mail**) lorsqu'ils arriveront dans l'infrastructure de messagerie Microsoft Exchange et tous les liens qu'ils contiennent seront désactivés.

    - **Enregistrer une copie**. Une copie du message sera enregistrée dans la sauvegarde.

    - **Ajouter une note à l'en-tête du message**. Les messages qui ont reçu l'état *Phishing* sont signalés par une note spéciale dans l'objet : [!!Phishing]. Si vous le souhaitez, modifier le texte de cette note dans le champ à droite.

11. Définissez, dans le groupe **Paramètres de traitement du courrier indésirable** , les paramètres d'utilisation des services complémentaires de recherche de courrier indésirable (cf. section "Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable" à la page 75) :

    - Pour activer KSN lors de la recherche de courrier indésirable et d'éléments de phishing, procédez comme suit :

        a. Cochez la case **Utiliser Kaspersky Security Network (KSN)**.

        b. Le cas échéant, indiquez le délai d'attente maximum pour les requêtes adressées au serveur KSN via le champ **Durée maximale d'attente pour la requête à KSN**.

        La valeur par défaut est de 10 s.

        La case **Utiliser Kaspersky Security Network (KSN)** est accessible si la case **J'accepte les conditions de KSN** dans le groupe **Paramètres KSN** et dans l'entrée **Configuration** est cochée.

    - Si vous souhaitez activer l'utilisation du service Reputation Filtering, cochez la case **Utiliser Reputation Filtering**.

      Pour pouvoir utiliser le service Reputation Filtering, vous devez confirmer votre participation à Kaspersky Security Network (KSN) et acceptez les conditions de l'accord KSN.

    - Si vous souhaitez activer l'utilisation du service de mise à jour rapide des bases de l'Anti-Spam, cochez la case **Utiliser Enforced Anti-Spam Updates Service**.

    - Si vous souhaitez que la connexion aux services KSN et Enforced Anti-Spam Updates Services s'opère via le serveur proxy, cochez la case **Accéder aux services KSN et Enforced Anti-Spam Updates Service via le serveur proxy**.

      Vous pouvez configurer les paramètres du serveur proxy dans le nœud **Configuration** (cf. section « **Configuration des paramètres de connexion à la source des mises à jour** » à la page 56).

12. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES LISTES NOIRE ET BLANCHE DES EXPEDITEURS

Vous pouvez configurer deux types de liste d'expéditeurs :

- Les listes blanches qui reprennent les adresses d'expéditeurs de confiance dont les messages ne doivent pas être soumis à la recherche de courrier indésirable.

- Les listes noires qui reprennent les adresses d'expéditeurs dont l'ensemble des messages est considéré comme non sollicité.

Kaspersky Security permet de configurer des listes blanche et noire d'adresses de messagerie et d'adresses IP.

### Configuration des listes blanche/noire d'adresses de messagerie d'expéditeur

*Pour configurer les listes noire/blanche d'adresses de messageries d'expéditeurs, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

    - si vous souhaitez configurer la liste noire/blanche des adresses de messagerie des expéditeurs pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

- si vous souhaitez configurer la liste noire/blanche des adresses de messagerie des expéditeurs pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité pour lequel vous souhaitez configurer la liste.

2. Sélectionnez le nœud **Protection du serveur**.
3. Dans la fenêtre des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres des listes blanche et noire**.
4. Cochez la case **Ajouter l'adresse de l'expéditeur à la liste blanche/noire**.
5. Ajouter l'adresse de messagerie à la liste. Pour ce faire, procédez comme suit :
   a. Saisissez l'adresse de messagerie dans le champ. Vous pouvez désigner une adresse de messagerie unique ou un modèle du type *@domain.com qui décrit toutes les adresses du domaine de messagerie.
   b. Cliquez sur le bouton  .
6. Pour supprimer une adresse de messagerie de la liste, sélectionnez l'adresse dans la liste, puis cliquez sur le bouton  .
7. Pour enregistrer la liste dans un fichier, cliquez sur le bouton  .
8. Pour importer la liste depuis un fichier, cliquez sur le bouton  .
9. Cliquez sur le bouton **Enregistrer**.

### Configuration de la liste blanche/noire d'adresses IP d'expéditeurs

*Pour configurer les listes noire/blanche d'adresses IP d'expéditeurs, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer la liste noire/blanche des adresses IP des expéditeurs pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;
   - si vous souhaitez configurer la liste noire/blanche des adresses IP des expéditeurs pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité pour lequel vous souhaitez configurer la liste.
2. Sélectionnez le nœud **Protection du serveur**.
3. Dans la fenêtre des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres des listes blanche et noire**.
4. Cochez la case **Ajouter l'adresse de l'expéditeur à la liste blanche/noire des adresses IP**.
5. Pour ajouter une adresse IP à la liste, procédez comme suit :
   a. Saisissez l'adresse IP dans le champ. Vous pouvez indiquer une adresse IP unique ou unE plage d'adresses IP en notation CIDR (du genre XXX.XXX.XXX.XXX/YY).
   b. Cliquez sur le bouton  .
6. Pour supprimer une adresse IP de la liste, sélectionnez l'adresse dans la liste, puis cliquez sur le bouton  .
7. Pour enregistrer la liste dans un fichier, cliquez sur le bouton  .

8. Pour importer la liste depuis un fichier, cliquez sur le bouton .

9. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DE LA LISTE BLANCHE DES DESTINATAIRES

Vous pouvez configurer la *liste blanche* des destinataires en ajoutant à la liste des adresses de destinataires ou en supprimant. Les messages destinés aux personnes reprises dans cette liste ne seront pas soumis à la recherche de courrier indésirable. Par défaut, la liste blanche est vide.

Vous pouvez ajouter des adresses de destinataires à la liste blanche sous la forme des entrées suivantes :

- Objets Active Directory :
  - Simples utilisateurs (User).
  - Contacts (Contact).
  - Groupes de diffusion (Distribution Group).
  - Groupes de sécurité (Security Group).

  Il est conseillé d'ajouter les adresses à la liste blanche sous la forme d'objets de ce type.
- Adresses SMTP au format mailbox@domain.com. Les entrées de ce type doivent être ajoutées si l'adresse à exclure ne figure pas dans Active Directory.

  Pour exclure un dossier public (Public Folder) de la recherche de courrier indésirable, il faut ajouter toutes les adresses SMTM (s'il y en a plusieurs) à la liste. Si certaines adresses SMTP du dossier public manquent à la liste, il se peut que les messages qui arrivent dans le dossier public soient analysés.

Les adresses des destinataires définies sous la forme d'objets Active Directory sont exclues de la recherche de courrier indésirable selon les règles suivantes :

- Si l'adresse du destinataire est définie sous la forme d'un simple utilisateur ou d'un contact, les messages qui lui sont destinés sont exclus de l'analyse.
- Si l'adresse est définie sous la forme d'un groupe de diffusion, les messages destinés à ce groupe sont exclus de l'analyse. Toutefois, les messages adressés personnellement aux membres du groupe ne sont pas exclus de l'analyse si ces adresses n'ont pas été ajoutées séparément à la liste.
- Si l'adresse est définie en tant que groupe de sécurité, les messages destinés à ce groupe et aux membres de ce groupe sont exclus de l'analyse. Toutefois, si un membre du groupe est un groupe de sécurité intégré, les messages destinés à ses membres ne sont pas exclus de l'analyse si ces adresses n'ont pas été ajoutées séparément à la liste.

L'application actualise automatiquement les adresses des destinataires obtenues via Active Directory après la modification des entrées correspondantes dans Active Directory (par exemple, en cas de modification de l'adresse électronique de l'utilisateur ou en cas d'ajout d'un nouveau membre au groupe de sécurité). L'actualisation s'opère une fois par jour.

➡ *Pour configurer la liste blanche des destinataires, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer la liste blanche des destinataires pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

- si vous souhaitez configurer la liste blanche des destinataires pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer la liste blanche des destinataires.

2. Sélectionnez le nœud **Protection du serveur**.
3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, développez le groupe **Paramètres des listes blanche et noire de l'Anti-Spam**.
4. Cochez la case **Ajouter l'adresse du destinataire à la liste blanche**.
5. Ajoutez l'adresse de l'expéditeur à la liste blanche des expéditeurs. Pour ce faire, procédez comme suit :
   - Pour ajouter un enregistrement d'Active Directory à la liste, procédez comme suit :
     a. Cliquez sur le bouton  ;
     b. Dans la fenêtre qui s'ouvre, localisez l'enregistrement requis d'Active Directory, puis cliquez sur **OK**.

     Les adresses sélectionnées dans Active Directory sont désignées par les icônes suivantes dans la liste :
     -  – utilisateurs simples, contacts, groupes de diffusion ;
     -  – groupes de sécurité.
   - Pour ajouter l'adresse SMTP à la liste ou le dossier partagé, procédez comme suit :
     - Pour ajouter une adresse SMTP, saisissez-la dans le champ, puis cliquez sur le bouton  .
     - Pour ajouter un dossier partagé, saisissez le chemin d'accès au dossier et cliquez sur le bouton  .

     Les adresses ajoutées de cette manière sont accompagnées de l'icône  .

     Les adresses ajoutées de cette manière ne sont pas soumises au contrôle de leur existence dans Active Directory.
6. Pour supprimer une adresse de la liste, sélectionnez l'entrée, puis cliquez sur le bouton  .
7. Pour enregistrer la liste dans un fichier, cliquez sur le bouton  .
8. Pour importer la liste depuis un fichier, cliquez sur le bouton  .
9. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DE L'AUGMENTATION DU CLASSEMENT DE COURRIER INDESIRABLE D'UN MESSAGE`

Vous pouvez configurer les paramètres de l'Anti-Spam qui déterminent les caractéristiques spéciales des messages : le classement de courrier indésirable. Ces paramètres permettent de configurer l'augmentation du classement de courrier indésirable des messages sur la base des résultats de l'analyse de l'adresse de messagerie électronique de l'expéditeur et de l'objet du message, ainsi que lorsque le message est en langue étrangère.

*Pour configurer l'augmentation du classement de courrier indésirable d'un message sur la base des résultats de l'analyse de l'adresse de l'expéditeur, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer l'augmentation du classement de courrier indésirable.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres de définition du classement de courrier indésirable**.

4. Dans le groupe de paramètres **Augmenter le classement de courrier indésirable si**, cochez les cases des paramètres suivants en fonction de vos besoins :

   - **Le champ " À " ne contient aucune adresse**. Si le champ « À » est vide, le classement de courrier indésirable du message sera augmenté.

   - **L'adresse de l'expéditeur du message contient des chiffres**. Si l'adresse de l'expéditeur contient des chiffres, le classement de courrier indésirable du message augmente.

   - **L'adresse de l'expéditeur (dans le corps du message) ne contient pas de domaine**. Si l'adresse de l'expéditeur ne contient pas le nom de domaine, le classement de courrier indésirable du message sera augmenté.

5. Cliquez sur le bouton **Enregistrer**.

*Pour configurer l'augmentation du classement de courrier indésirable des messages sur la base des résultats de l'analyse de l'objet du message, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer l'augmentation du classement de courrier indésirable.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres de définition du classement de courrier indésirable**.

4. Dans le groupe de paramètres **Augmenter le classement de courrier indésirable si l'objet du message contient**, cochez les cases des paramètres suivants en fonction de vos besoins :

   - **Plus de 250 caractères**. Si l'objet du message compte plus de 250 caractères, le classement de courrier indésirable du message augmente.

   - **Beaucoup d'espaces et/ou de points**. Si l'objet du message contient beaucoup d'espaces et/ou de points, le classement de courrier indésirable du message augmente.

   - **Horodatage**. Si l'objet du message contient un identifiant numérique ou une balise d'horodatage, le classement de courrier indésirable du message augmente.

5. Cliquez sur le bouton **Enregistrer**.

*Pour configurer l'augmentation du classement de courrier indésirable des messages sur la base des résultats de l'analyse de la langue de rédaction du message, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer l'augmentation du classement de courrier indésirable des messages pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer l'augmentation du classement de courrier indésirable.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres de définition du classement de courrier indésirable**.

4. Dans le groupe de paramètres **Augmenter le classement de courrier indésirable si le message est en**, cochez les cases des langues de rédaction des messages que vous ne comptez pas recevoir :

   - **Chinois** si vous ne vous attendez pas à recevoir des messages rédigés en chinois.

   - **Coréen** si vous ne vous attendez pas à recevoir des messages rédigés en coréen.

   - **Thaï** si vous ne vous attendez pas à recevoir des messages rédigés en thaï.

   - **Japonais** si vous ne vous attendez pas à recevoir des messages rédigés en japonais.

5. Cliquez sur le bouton **Enregistrer**.

# RECOURS A DES SERVICES EXTERNES POUR LA DETECTION DU COURRIER INDESIRABLE

Pour obtenir un filtrage plus précis des messages non sollicités, vous pouvez utiliser des services externes (cf. section "Présentation des services, des fonctions et des technologies complémentaires de protection contre le courrier indésirable" à la page 75).

*Pour activer l'utilisation de services externes d'analyse des adresses IP et des URL à la recherche de courrier indésirable, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres d'utilisation de services d'analyse antispam externes pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer les paramètres d'utilisation de services d'analyse antispam externes pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer l'utilisation des services externes.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe de paramètres **Utilisation de services externes de l'Anti-Spam**.

4. Si vous souhaitez que l'application tienne compte, lors de la recherche de courrier indésirable, des résultats de services externes de vérification d'adresses IP et d'URL, cochez la case **Utiliser des services externes de recherche de courrier indésirable**.

5. Si vous souhaitez que l'application recherche la présence éventuelle de messages non sollicités dans le courrier sur la base d'une liste noire DNSBL définie par défaut, cochez la case **Utiliser la liste noire du service DNSBL installée par défaut** dans le groupe de paramètres **Paramètres du service DNSBL**.

6. Si vous souhaitez utiliser votre propre liste de serveurs DNS et leur attribuer d'autres coefficients de pondération, cochez la case **Utiliser une autre liste de la sélection de listes noires du service DNSBL**. Une fois que vous avez coché cette case, vous devez composer une liste. Pour ce faire, procédez comme suit :

   - Pour ajouter une entrée à la liste définie par l'utilisateur, indiquez le nom DNS du serveur et le coefficient pondéré dans les champs correspondants, puis cliquez sur  .
   - Pour supprimer l'entrée de la liste définie par l'utilisateur, cliquez sur le bouton  .
   - Pour importer une liste définie par l'utilisateur, cliquez sur le bouton  .
   - Pour exporter une liste définie par l'utilisateur, cliquez sur le bouton  .

7. Si vous souhaitez que l'application recherche la présence éventuelle de messages non sollicités dans le courrier sur la base de la liste noire SURBL définie par défaut, cochez la case **Utiliser la liste noire du service SURBL installée par défaut** dans le groupe de paramètres **Paramètres du service SURBL**.

8. Si vous souhaitez utiliser votre propre liste de serveurs DNS et leur attribuer d'autres coefficients de pondération, cochez la case **Utiliser une autre liste de la sélection de listes noires du service SURBL**. Une fois que vous avez coché cette case, vous devez composer une liste. Pour ce faire, procédez comme suit :

   - Pour ajouter une entrée à la liste définie par l'utilisateur, indiquez le nom DNS du serveur et le coefficient pondéré dans les champs correspondants, puis cliquez sur  .
   - Pour supprimer une entrée, cliquez sur  .
   - Pour importer une liste définie par l'utilisateur, cliquez sur le bouton  .
   - Pour exporter une liste définie par l'utilisateur, cliquez sur le bouton  .

9. Si vous souhaitez activer la recherche de la présence de l'entrée dans la zone de retour pour l'adresse IP de l'expéditeur dans le DNS, cochez la case **Vérifier la présence de l'adresse IP de l'expéditeur dans les DNS**.

10. Si vous souhaitez activer l'utilisation de la technologie SPF, cochez la case **Utiliser la technologie SPF**.

11. Si vous souhaitez activer la vérification de l'appartenance éventuelle de l'adresse IP de l'expéditeur à un réseau de zombies en fonction de sa zone DNS de retour, cochez la case **Vérifier si l'adresse de l'expéditeur est de type DNS dynamique**.

    Si la réponse est affirmative, le classement de courrier indésirable du message sera augmenté.

12. Dans le champ **Durée maximale d'attente pour la requête DNS**, saisissez le délai d'attente maximum pour la connexion en secondes.

    La valeur par défaut est de 10 s. Une fois le délai d'attente écoulé, l'application recherche la présence éventuelle de messages non sollicités sans recourir à la vérification de l'appartenance de l'adresse IP de l'expéditeur à un DNS dynamique.

# CONFIGURATION DES PARAMETRES AVANCES DE RECHERCHE DE COURRIER INDESIRABLE ET D'ELEMENTS DE PHISHING

Vous pouvez configurer les paramètres avancés de recherche de courrier indésirable et de phishing tels que la restriction de l'analyse des messages en fonction de la durée ou de la taille ou la possibilité d'analyser les fichiers Microsoft Office joints au message.

*Pour définir des restrictions au niveau de la durée de la recherche de courrier indésirable et de phishing et de la taille des messages, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les restrictions d'analyse antispam et antiphishing pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les restrictions d'analyse antispam et antiphishing pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les restrictions de l'analyse.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres avancés de l'Anti-Spam**.

4. Dans le groupe **Restrictions**, définissez la valeur du paramètre **Durée maximale d'analyse des messages** en secondes à l'aide du menu avec défilement.

   Si la durée d'analyse du message dépasse la valeur indiquée, l'analyse antispam et antiphishing sera arrêtée. La valeur par défaut est de 60 s. Si l'ajout d'en-têtes de service est activé, ceux-ci reprendront des informations relatives au dépassement de la durée maximale de l'analyse.

5. Dans le groupe **Restrictions**, définissez la valeur du paramètre **Taille maximale de l'objet à analyser** en kilo-octets à l'aide du menu avec défilement.

   Si la taille du message avec toutes ses pièces jointes dépasse la valeur indiquée, l'analyse antispam et antiphishing n'aura pas lieu et le message sera remis au destinataire. La valeur par défaut est de 1536 Ko (1,5 Mo). La valeur maximale est de 20 Mo et la valeur minimale est égale à 1 Ko. Si l'ajout d'en-têtes de service est activé, ceux-ci reprendront des informations relatives au dépassement de la taille maximale de l'objet analysé.

6. Cliquez sur **Enregistrer** pour enregistrer les modifications.

*Pour configurer les paramètres de recherche de courrier indésirable et d'éléments de phishing dans des fichiers Microsoft Office, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres d'analyse antispam et antiphishing des fichiers Microsoft Office pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer les paramètres d'analyse antispam et antiphishing des fichiers Microsoft Office pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les restrictions de l'analyse.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres avancés de l'Anti-Spam**.

4. Dans le groupe de paramètres **Paramètres d'analyse des fichiers Microsoft Office**, réalisez les opérations suivantes :

   - Si vous souhaitez que l'application recherche la présence éventuelle de courrier indésirable et de phishing dans les documents Microsoft Word, cochez la case **Analyser les fichiers DOC**.

   - Si vous souhaitez que l'application recherche la présence éventuelle de courrier indésirable et de phishing dans les documents RTF, cochez la case **Analyser les fichiers RTF**.

5. Cliquez sur **Enregistrer** pour enregistrer les modifications.

*Pour configurer l'utilisation des paramètres avancés de recherche de courrier indésirable et de phishing, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer l'utilisation des paramètres avancés d'analyse antispam et antiphishing pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez configurer l'utilisation des paramètres avancés d'analyse antispam et antiphishing pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres d'analyse avancés.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub**, déployez le groupe **Paramètres avancés de l'Anti-Spam**.

4. Si vous souhaitez que les images jointes aux messages soient analysées selon la technologie de traitement des images, cochez la case **Utiliser la technologie d'analyse des images**.

   Cette technologie permet de vérifier si les images présentent des caractéristiques similaires à celles de modèles figurant dans la base de l'Anti-Spam. Si une équivalence est confirmée, le classement de courrier indésirable du message augmente.

5. Si vous souhaitez que l'application ajoute au message les en-têtes X d'information contenant des données relatives au résultat de l'analyse, cochez la case **Inclure les en-têtes de résultats d'analyse (X-Headers) au message**.

6. Cochez la case **Analyser les connexions autorisées** afin d'activer l'analyse antispam et antiphishing des messages reçus via des connexions de confiance (Trusted Connection).

7. Cochez la case **Ne pas analyser les messages destinés à Postmaster** pour désactiver l'analyse antispam et antiphishing des messages reçus à l'adresse Postmaster.

8. Cliquez sur **Enregistrer** pour enregistrer les modifications.

# SAUVEGARDE

Cette section décrit la sauvegarde et son utilisation.

### DANS CETTE SECTION DE L'AIDE


Présentation de la sauvegarde ..... 89

Consultation du contenu de la Sauvegarde ..... 90

Consultation des propriétés des objets placés dans la sauvegarde ..... 91

Configuration des filtres de la sauvegarde ..... 93

Enregistrement sur le disque d'un objet de la sauvegarde ..... 93

Envoi d'un objet de la sauvegarde à des destinataires ..... 94

Suppression des objets de la sauvegarde ..... 94

Configuration des paramètres de la sauvegarde ..... 95

Sélection de la base de données de la sauvegarde pour consulter son contenu depuis le profil ..... 96


# A PROPOS DE LA SAUVEGARDE

L'application Kaspersky Security place dans la *sauvegarde* les copies des messages avant leur traitement par l'application. Les copies des messages sont placées dans la sauvegarde avec toutes les pièces jointes.

Kaspersky Security place des copies des messages dans la sauvegarde dans les cas suivants :

- après l'analyse des messages par l'Antivirus et avant de le modifier à l'aide des actions Supprimer le message ou Supprimer l'objet, à condition que le placement des copies des messages dans la sauvegarde lors de l'analyse antivirus a été configurée (cf. section «Configuration des paramètres de traitement des objets» à la page. 64).

- après la recherche d'éventuels messages non sollicités et de phishing et avant l'exécution de l'action Supprimer ou Rejeter, à condition que le placement des copies des messages dans la sauvegarde pendant l'analyse antispam a été configuré (cf. section "Configuration des paramètres de recherche de courrier indésirable et d'éléments de phishing" à la page 78).

Vous pouvez réaliser les opérations suivantes sur les copies des messages dans la sauvegarde :

- Consulter le contenu de la sauvegarde (cf. section « Consultation du contenu de la sauvegarde » à la page 90) ;

- Obtenir des informations sur les messages dans la sauvegarde (cf. section « Consultation des propriétés des objets placés dans la sauvegarde » à la page 91) ;

- Filtrer les informations sur les messages dans la sauvegarde afin de simplifier la consultation et la recherche d'informations relatives aux messages (cf. section « Configuration des filtres de la sauvegarde » à la page 93).

- Enregistrer les messages de la sauvegarde sur le disque dans le but d'obtenir les informations contenues dans les messages (cf. section « Enregistrement sur le disque d'un objet de la sauvegarde » à la page 93). Vous pouvez également tenter d'analyser à nouveau le message à l'aide de l'Anti-Virus et d'une version mise à jour des bases.

- Transmettre les messages depuis la sauvegarde aux destinataires (cf. section « Envoi d'un objet de la Sauvegarde à des destinataires » à la page 94). Les objets enregistrés seront accessibles aux destinataires.

- Supprimer les copies des messages de la sauvegarde (cf. section « Suppression des objets de la sauvegarde » à la page 94).

Les données relatives aux objets de la sauvegarde sont conservées dans une base de données SQL désignée lors de l'installation de l'application (pour les détails, reportez-vous à *Guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Server*s). Si plusieurs serveurs de sécurité utilisent une base de données SQL (par exemple, dans la configuration de serveurs avec un DAG), les messages reçus de chacun de ces serveurs de sécurité seront conservés dans la Sauvegarde.

Les copies des messages enregistrées dans la sauvegarde sont chiffrées, ce qui évite tout risque d'infection et qui accélère le fonctionnement de l'Antivirus (les fichiers au format de la sauvegarde ne sont pas considérés comme infectés).

La sauvegarde peut contenir un million de fichiers. Vous pouvez également définir des restrictions au niveau de la taille de la sauvegarde et de la durée de conservation des objets qu'elle contient (cf. section « Configuration des paramètres de la sauvegarde » à la page 95).

Le respect des restrictions est contrôlé toutes les minutes. Sur la base des résultats de l'analyse, l'application peut exécuter les actions suivantes :

- quand le nombre maximum de messages est dépassé, l'application supprime le nombre requis de messages parmi les plus anciens ;

- si la limite a été définie au niveau de la taille de la banque en mégaoctets et que l'ajout d'un nouveau message entraîne le dépassement de cette limite, l'application crée l'espace nécessaire en supprimant les objets les plus anciens ;

- si la limite a été définie au niveau de la durée de conservation des messages, l'application supprime les messages arrivés à l'échéance de cette durée.

# CONSULTATION DU CONTENU DE LA SAUVEGARDE

Vous pouvez consulter les informations relatives à tous les objets placés dans la sauvegarde (messages et pièces jointes).

➧ *Pour consulter le contenu de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.

2. Choisissez le nœud **Sauvegarde**.

   Le panneau des résultats affiche un tableau qui reprend les informations relatives aux objets enregistrés dans la sauvegarde (cf. ill. ci-après).

   La partie inférieure du panneau des résultats sous le tableau reprend les informations relatives au nombre d'objets dans la sauvegarde et l'espace qu'ils occupent, ainsi que le nombre d'objets filtrés, en cas d'application du filtre.

   Par défaut, vous pouvez consulter les informations suivantes pour chaque objet repris dans la sauvegarde :

   - **De**. Adresse de l'expéditeur du message.

   - **À**. Adresse du destinataire du message.

   - **Objet**. Objet du message.

   - **Etat**. État d'analyse des objets (*Infecté, Potentiellement infecté, Réparé, Courrier indésirable, Envoi massif, Courrier potentiellement indésirable, Phishing, Ajouté à la liste noire, Notification formelle, De confiance,*

*Protégé, Pas d'accès, Introuvable, Durée d'analyse écoulée, L'analyse n'est pas terminée, Erreur d'analyse*).

- **Heure de réception**. Heure exacte de l'arrivée du message sur le serveur Microsoft Exchange.

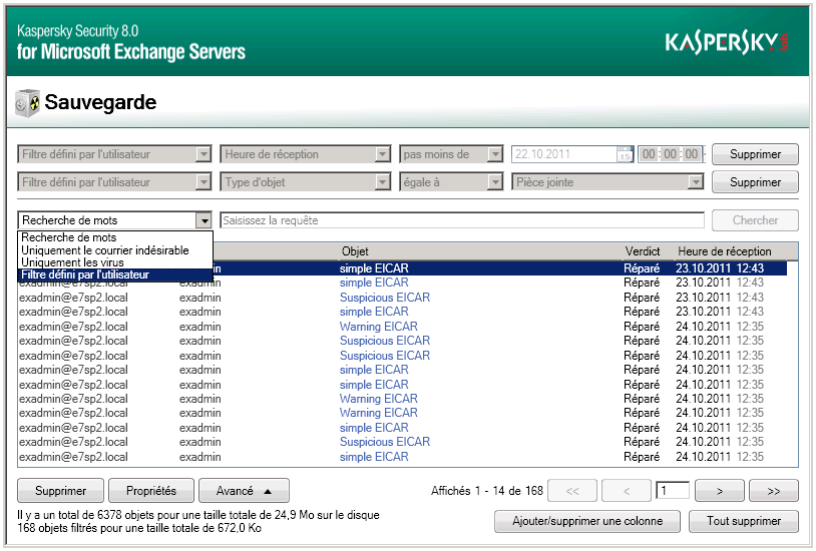


*Figure 2. Consultation du contenu de la Sauvegarde*

Vous pouvez configurer l'aspect du panneau des résultats en modifiant la sélection et l'ordre des colonnes du tableau.

➧ *Pour configurer l'aspect du panneau des résultats, procédez comme suit :*

1. Cliquez sur **Sélectionner les colonnes** afin d'ajouter ou de supprimer des colonnes du tableau.
2. Exécutez les actions suivantes dans la fenêtre qui s'ouvre :
   - Cochez la case en regard des colonnes du tableau que vous souhaitez voir dans le panneau des résultats.
   - Décochez la case en regard des colonnes du tableau que vous ne souhaitez pas consulter.

Vous pouvez trier les informations du tableau selon le contenu de n'importe laquelle des colonnes en cliquant sur le nom de la colonne souhaitée, par exemple **De**, **A**, **Objet**.

Le panneau des résultats affiche un nombre limité d'objets simultanés. Pour afficher le reste des objets, utilisez les touches de navigation située dans le coin inférieur droit du panneau des résultats. Le numéro de la fenêtre actuelle apparaît entre les deux boutons. Pour passer à la fenêtre suivante, cliquez sur le bouton **>**. Pour revenir à la fenêtre précédente, cliquez sur le bouton **<**. Pour accéder à la dernière fenêtre, cliquez sur le bouton **>>**. Pour revenir à la toute première fenêtre, cliquez sur le bouton **<<**.

# CONSULTATION DES PROPRIETES DES OBJETS PLACES DANS LA SAUVEGARDE

➧ *Pour consulter les propriétés d'un objet placé de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Choisissez le nœud **Sauvegarde**.
3. Dans le tableau reprenant la liste des objets de la sauvegarde qui apparaît dans le panneau des résultats, sélectionnez l'objet (message ou pièce jointe) que vous souhaitez consulter.

4. Cliquez sur le bouton **Propriétés** situé dans la partie supérieure du panneau des résultats au-dessus de la liste des objets.

La fenêtre **Propriétés du message** s'ouvre. Cette fenêtre propose les informations suivantes :

- **Virus**. Si le message est infecté par un virus, le nom de ce dernier apparaîtra dans ce champ.
- **Type d'objet**. Type d'objet : message, corps du message ou pièce jointe.
- **De**. Adresse de l'expéditeur.
- **À**. Adresse du destinataire du message.
- **Copie**. Adresse du destinataire de la copie du message.
- **Nom de l'objet**. Nom du fichier du message ou de la pièce jointe.
- **Taille sur le disque**. Espace que le message occupe sur le disque.
- **Objet**. Objet du message.
- **Chemin d'accès**. Chemin d'enregistrement du message.
- **Nom du serveur**. Nom du serveur qui a placé l'objet dans la Sauvegarde.
- **Nom du serveur virtuel**. Nom du serveur virtuel (uniquement pour les configurations en cluster de Microsoft Exchange).
- **Nom du cluster**. Nom du cluster (uniquement pour les configurations en cluster de Microsoft Exchange).
- **Heure de réception**. Moment exact de la remise du message (jour, mois, année, heures, minutes).
- **Date de création**. Moment exact de la création du message (jour, mois, année, heures, minutes).
- **Heure d'édition des bases**. Heure d'édition des bases.
- **Etat**. Etat attribué au message par l'application.
- **Taille**. Taille de l'objet (message ou pièce jointe) en octets.

Vous pouvez sélectionner plusieurs objets et consulter les informations relatives à leur état.

*Pour consulter les propriétés de plusieurs objets placés dans la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Choisissez le nœud **Sauvegarde**.
3. Dans le tableau reprenant la liste des objets de la sauvegarde qui apparaît sur le panneau des résultats, sélectionnez les objets dont vous souhaitez consulter les propriétés.
4. Cliquez sur le bouton **Propriétés** situé dans la partie supérieure du panneau des résultats au-dessus de la liste des objets.

La fenêtre **Propriétés des objets sélectionnés** s'ouvre. Cette fenêtre permet de consulter les états de tous les objets sélectionnés.

# CONFIGURATION DES FILTRES DE LA SAUVEGARDE

Les filtres simplifient la recherche et la consultation d'informations sur les objets dans la sauvegarde. Par exemple, vous pouvez utiliser un filtre afin de sélectionner les objets que vous voulez enregistrer sur le disque.

*Pour configurer le filtre de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Choisissez le nœud **Sauvegarde**.
3. Dans la partie supérieure du panneau des résultats, sélectionnez un des critères suivants dans la liste déroulante afin de filtrer les objets dans la sauvegarde :
   - **Phishing uniquement**. Le panneau des résultats affiche uniquement les messages porteurs de l'état *Phishing*.
   - **Uniquement le courrier indésirable**. Le panneau des résultats affiche uniquement les messages porteurs de l'état *Courrier indésirable*.
   - **Uniquement les virus**. Le panneau des résultats affiche uniquement les messages infectés par des virus ou qui contiennent des virus dans les pièces jointes.
   - **Recherche de mots**. Si vous choisissez cette option, saisissez les mots clés selon lesquels l'application devra rechercher les messages. L'application effectue une recherche dans les colonnes **De**, **A** et **Objet**.
   - **Filtre défini par l'utilisateur**. Si vous avez choisi cette option, procédez comme suit :
     - Dans la liste déroulante, sélectionnez le critère de filtrage.
     - Choisissez la condition d'équivalence au critère sélectionné (**égale à**, **pas égale à**, **supérieure à**, **pas moins de**, **inférieure à**, **pas plus de** ou **entre**).
     - Définissez la valeur du filtre. Pour les critères **Date de création du message**, **Heure de réception** et **Heure d'édition des bases**, définissez les valeurs à l'aide du calendrier. Pour le critère **Etat**, sélectionnez une option dans la liste déroulante. Pour les autres critères, saisissez les valeurs manuellement dans le champ.
4. Cliquez sur le bouton **Chercher**.

   Le filtre appliqué apparaît dans la partie supérieure du panneau des résultats. Le tableau du panneau des résultats reprend les objets qui répondent aux critères de la recherche.
5. Pour supprimer le filtre, cliquez sur le bouton **Supprimer** à droite du filtre.

Après avoir appliqué les filtres, vous pouvez également trier les informations dans le tableau par ordre croissant ou décroissant selon les données de n'importe quelle colonne. Pour ce faire, cliquez sur le nom de la colonne requise, par exemple **De**, **A** ou **Objet**.

# ENREGISTREMENT SUR LE DISQUE D'UN OBJET DE LA SAUVEGARDE

L'enregistrement d'un objet de la sauvegarde sur le disque peut entraîner l'infection de votre ordinateur.

*Pour enregistrer un objet de la sauvegarde sur le disque, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.

2. Choisissez le nœud **Sauvegarde**.

3. Dans le tableau reprenant la liste des objets de la sauvegarde qui apparaît sur le panneau des résultats, sélectionnez l'objet que vous souhaitez enregistrer.

4. Cliquez sur le bouton **Enregistrer sur le disque** situé dans la partie supérieure du panneau des résultats au-dessus de la liste des objets.

5. Dans la fenêtre qui s'ouvre, indiquez le dossier dans lequel vous souhaitez enregistrer l'objet et, le cas échéant, saisissez un nom pour l'objet ou modifiez le nom existant.

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

L'objet sélectionné est décrypté et sa copie est enregistrée dans le dossier indiqué sous le nom spécifié. L'objet enregistré possède un format identique au format qu'il avait lorsqu'il a été traité par l'application. Une fois que l'objet a été enregistré, l'application affiche le message suivant : « L'objet sélectionné a été enregistré sur le disque ».

# ENVOI D'UN OBJET DE LA SAUVEGARDE A DES DESTINATAIRES

Vous pouvez envoyer une copie du message enregistré dans la Sauvegarde au destinataire original.

*Pour envoyer un message depuis la Sauvegarde au destinataire, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez le nœud du serveur Microsoft Exchange.

2. Choisissez le nœud **Sauvegarde**.

3. Dans le tableau contenant la liste des objets de la sauvegarde qui apparaît dans le panneau des résultats, sélectionnez le message que vous souhaitez envoyer aux destinataires.

4. Cliquez sur le bouton **Envoyer aux destinataires** situé dans la partie supérieure du panneau des résultats au-dessus de la liste des objets.

L'application envoie l'objet sélectionné aux destinataires du message d'origine.

# SUPPRESSION DES OBJETS DE LA SAUVEGARDE

L'application supprime automatiquement les objets suivants de la sauvegarde :

- L'objet le plus ancien si l'ajout d'un nouvel objet va entraîner le dépassement de la restriction du nombre d'objets dans la sauvegarde (pour rappel, le nombre d'objets est limité à un million).

- L'objet le plus ancien quand une restriction sur la taille de la sauvegarde a été définie et que l'ajout d'un nouvel objet entraîne le dépassement de cette limite.

- Les objets arrivés à la fin de leur durée de conservation, pour autant qu'une telle limite ait été définie.

Il est possible également de supprimer manuellement les objets de la sauvegarde. Ceci peut être utile pour supprimer des objets enregistrés sur le disque ou pour gagner de la place dans la sauvegarde.

*Pour supprimer des objets de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez le nœud du serveur Microsoft Exchange.

2. Choisissez le nœud **Sauvegarde**.

3. Dans le tableau reprenant la liste des objets de la sauvegarde qui apparaît dans le panneau des résultats, sélectionnez le ou les objets que vous souhaitez supprimer. Pour rechercher des objets, vous pouvez utiliser un filtre (cf. section « Configuration des filtres de la sauvegarde » à la page 93).

4. Cliquez sur le bouton **Supprimer** dans la partie inférieur du panneau des résultats.

   Une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Oui**.

L'application supprime les objets sélectionnés de la sauvegarde.

*Pour supprimer tous les objets de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez le nœud du serveur Microsoft Exchange.

2. Choisissez le nœud **Sauvegarde**.

3. Cliquez sur le bouton **Tout supprimer** dans le panneau des résultats.

   Une fenêtre de confirmation s'ouvre.

4. Cliquez sur **Oui**.

Si vous aviez appliqué un filtre à la sauvegarde, seuls les objets qui satisfont aux critères du filtre sont supprimés de la sauvegarde. Si vous n'aviez appliqué aucun filtre à la sauvegarde, l'application supprime tous les fichiers de la sauvegarde.

# CONFIGURATION DES PARAMETRES DE LA SAUVEGARDE

La sauvegarde est créée lors de l'installation du serveur de sécurité. Les paramètres de la sauvegarde prennent des valeurs par défaut, mais celles-ci peuvent être modifiées par l'administrateur.

*Pour modifier les paramètres de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, sélectionnez le nœud du serveur Microsoft Exchange.

2. Sélectionnez le nœud **Configuration**.

3. Si vous souhaitez limiter le volume de la sauvegarde, procédez comme suit :

   - Dans le panneau des résultats, dans le groupe **Enregistrement des données**, cochez la case **Limiter la taille de la Sauvegarde**.

   - Dans le champ avec défilement **La taille de la sauvegarde ne peut être supérieure à**, indiquez la taille maximale de la sauvegarde.

     Par défaut, la taille maximale de la sauvegarde est égale à 5 120 Mo.

4. Si vous souhaitez limiter la durée de conservation des objets dans la sauvegarde, procédez comme suit :

   - Dans le groupe de paramètres **Enregistrement des données** du panneau de configuration, cochez la case **Limiter la durée de conservation des objets dans la sauvegarde** ;

   - Dans le champ avec défilement **Ne pas conserver les objets plus de**, indiquez le nombre requis de jours.

     Par défaut, la durée de conservation des objets dans la Sauvegarde est de 30 jours.

5. Cliquez sur le bouton **Enregistrer**.

Si aucune des cases du groupe de paramètres **Enregistrement des données** n'est cochée, la seule restriction active est celle portant sur le nombre total d'objets dans la sauvegarde (doit être inférieur à 1 million d'objets).

Quelle que soit la configuration de l'application (serveur unique, cluster de serveurs ou DAG), la sauvegarde doit être configurée individuellement pour chaque serveur physique.

# SELECTION DE LA BASE DE DONNEES DE LA SAUVEGARDE POUR CONSULTER SON CONTENU DEPUIS LE PROFIL

Les données relatives aux objets de la sauvegarde sont conservées dans une base de données SQL désignée lors de l'installation de l'application (pour les détails, reportez-vous à *Guide d'installation de Kaspersky Security 8.0 for Microsoft Exchange Servers*).

En cas d'ajout de plusieurs serveurs de sécurité à un profil, le nœud du profil affiche par défaut le nœud de la sauvegarde dont le nom du serveur SQL avec la base de données est en tête de liste par ordre alphabétique selon le format <nom serveur SQL>\<exemplaire>.

Vous pouvez sélectionner dans le profil la base de données SQL contenant les données relatives aux objets de la sauvegarde dont vous souhaitez consulter le contenu.

- *Pour sélectionner la base de données de la sauvegarde dans le profil afin de pouvoir consulter son contenu, procédez comme suit :*

1. Dans l'arborescence de la console, développez le nœud **Profils**.
2. Développez le nœud du profil contenant le serveur de sécurité qui utilise la base de données SQL requise.
3. Choisissez le nœud **Sauvegarde**.
4. Cliquez sur le bouton **Sélectionner** dans le panneau des résultats.

   La fenêtre **Base de données** qui contient toutes les bases de données SQL utilisées par au moins un des serveurs de sécurité du profil s'ouvre.
5. Dans la fenêtre **Base de données**, sélectionnez le serveur de sécurité sur lequel se trouve la base de données SQL de la sauvegarde requise.
6. Cliquez sur **OK**.

En cas e connexion à distance à la base de données sur le serveur SQL, assurez-vous que ce serveur SQL prend en charge le protocole client TCP/IP.

# NOTIFICATIONS

Cette section décrit les notifications et leur configuration.

### DANS CETTE SECTION DE L'AIDE

Présentation des notifications ..... 97

Configuration des paramètres de notification ..... 97

Configuration des paramètres d'envoi des notifications ..... 98

## PRESENTATION DES NOTIFICATIONS

Kaspersky Security propose une fonction de notifications relatives aux objets infectés, protégés et endommagés détectés lors de l'analyse. Vous pouvez configurer l'envoi des notifications relatives aux objets infectés, protégés et endommagés à l'adresse de messagerie de l'expéditeur du message, du destinataire du message, de l'administrateur ou à d'autres adresses comme celles d'employés du service de sécurité.

La notification peut être communiquée de différentes manières :

- Via la diffusion d'un message par courrier électronique. Dans ce cas, il faut configurer les paramètres d'envoi des notifications (cf. section «Configuration des paramètres d'envoi des notifications» à la page 98).
- Via la consignation de l'événement dans le journal système Microsoft Windows de l'ordinateur sur lequel le serveur de sécurité est installé. Dans ce cas, la consultation des informations s'opère via l'outil standard de consultation et d'administration des journaux Windows : **Observateur d'événements.**

## CONFIGURATION DES PARAMETRES DE NOTIFICATION

*Pour configurer les paramètres des notifications, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez configurer les paramètres de notification pour un serveur de sécurité non réparti, développez le nœud du serveur de sécurité souhaité ;
   - si vous souhaitez configurer les paramètres des notifications pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres d'envoi des notifications.
2. Sélectionnez le nœud **Notifications**.
3. Dans le panneau des résultats, développez le groupe de paramètres requis pour configurer les notifications de chaque type :
   - **Signaler les objets infectés**.
   - **Signaler les objets endommagés**.
   - **Signaler les objets protégés**.
   - **Signaler les erreurs système**.

L'envoi à l'expéditeur et au destinataire relatives de notifications à des erreurs système n'est pas prévu.

4. Pour chaque type de notification, désignez son destinataire dans la rubrique **Signaler par courrier électronique**.

   - Si vous souhaitez que l'application envoie la notification à l'adresse de messagerie de l'administrateur, cochez la case **Administrateur**.

   - Si vous souhaitez que l'application envoie la notification à l'expéditeur du message dans lequel l'objet a été détecté, cochez la case **Expéditeur**.

     Vous ne pouvez pas désigner l'expéditeur dans le groupe de paramètres **Signaler les erreurs système**.

   - Si vous souhaitez que l'application envoie la notification au destinataire du message dans lequel l'objet a été détecté, cochez la case **Destinataire**.

     Vous ne pouvez pas désigner le destinataire dans le groupe de paramètres **Signaler les erreurs système**.

   - Si vous souhaitez que l'application envoie la notification à l'adresse de messagerie que vous avez renseignée, cochez la case **Destinataires suivants**. Saisissez dans le champ la ou les adresses de messagerie auxquelles vous souhaitez envoyer les notifications.

5. Lors de la configuration des notifications sur les erreurs système, vous pouvez sélectionner les erreurs au sujet desquelles vous souhaitez envoyer des notifications dans le groupe de paramètres **Signaler les erreurs système**. Pour ce faire, cochez les cases requises :

   - **Signaler que les bases sont dépassées**.

   - **Signaler les erreurs de licence**.

6. Si vous souhaitez que l'application consigne l'événement dans le journal système Microsoft Windows, cochez la case **Consigner dans le journal des événements Microsoft Windows**.

7. Cliquez sur le bouton **Enregistrer**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres de notification configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres de notification sur les autres serveurs du DAG.

# CONFIGURATION DES PARAMETRES D'ENVOI DES NOTIFICATIONS

*Pour configurer les paramètres d'envoi des notifications, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres d'envoi de notifications pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer les paramètres d'envoi de notifications pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres d'envoi des notifications.

2. Sélectionnez le nœud **Notifications** ou le nœud **Configuration**.

3. En fonction du nœud sélectionné, procédez comme suit :

   - si vous avez choisi le nœud **Notifications**, le lien **Paramètres d'envoi des notifications** dans la partie inférieure du panneau des résultats ouvre la fenêtre **Paramètres d'envoi des notifications** ;

   - si vous avez choisi le nœud **Configuration**, développez le groupe de paramètres **Configuration des paramètres de notification**.

4. Dans le champ **Adresse du service Web**, indiquez l'adresse du service Web d'envoi des messages électroniques via le serveur Microsoft Exchange. L'adresse suivante est utilisée par défaut dans le serveur Microsoft Exchange : https://<nom_du_serveur_d'accès_client>/ews/exchange.asmx

5. Saisissez dans le champ **Compte utilisateur** n'importe quel compte utilisateur tiré des boîtes aux lettres enregistrées sur le serveur Microsoft Exchange ou cliquez sur le bouton **...** et sélectionnez le compte dans la fenêtre ouverte.

6. Saisissez le mot de passe du compte choisi dans le champ **Mot de passe**.

7. Dans le champ **Adresse de l'administrateur**, indiquez l'adresse électronique du destinataire des notifications.

8. Si vous configurez les paramètres de notification pour un Serveur de sécurité non réparti, vous pouvez envoyer un message d'essai en cliquant sur le bouton **Test**.

   L'envoi d'un message d'essai pour les Serveurs de sécurité du profil n'est pas pris en charge.

9. Cliquez sur **OK**.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres de notification configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres d'envoi des notifications sur les autres serveurs du DAG.

# RAPPORTS

Cette section décrit les rapports sur le fonctionnement de l'application et leur configuration.

### DANS CETTE SECTION DE L'AIDE


Présentation des rapports sur le fonctionnement de l'application ..... 100

Création d'un rapport rapide ..... 101

Création de la tâche de composition des rapports ..... 102

Modification des paramètres de la tâche de composition des rapports ..... 103

Lancement de la tâche de composition des rapports ..... 103

Suppression de la tâche de composition des rapports ..... 104

Consultation des tâches de composition des rapports ..... 104

Consultation des rapports prêts ..... 105

Enregistrement du rapport ..... 108

Suppression du rapport ..... 108


# PRESENTATION DES RAPPORTS SUR LE FONCTIONNEMENT DE L'APPLICATION

Kaspersky Security permet de créer et de consulter des rapports sur le fonctionnement des modules Antivirus et Anti-Spam. Un rapport de fonctionnement couvrant une période d'un jour est créé pour chaque module séparément.

Vous pouvez créer des *rapports rapides* manuellement ou créer une *tâche de composition de rapports* automatique selon une programmation. Il est également possible de lancer manuellement la tâche de composition des rapports.

L'application prévoit des rapports standards et des rapports détaillés. Les rapports standards contiennent des informations sur les objets traités au cours de la période, sans indication de la période pendant laquelle l'événement a eu lieu. Les rapports détaillés indiquent les intervalles de temps précis pendant lesquels les événements ont eu lieu.

Ces intervalles dépendent de la période couverte par le rapport :

- Si la période est égale à un jour, l'intervalle minimum pour chaque événement sera égal à une heure.
- Si la période est comprise entre 2 et 7 jours, l'intervalle minimum pour chaque événement est égal à 6 heures.
- Si la période est supérieure à 8 jours, l'intervalle minimum pour chaque événement est égal à un jour.

Le rapport peut être consulté dans l'application ou vous pouvez le recevoir par courrier électronique. Les rapports envoyés par courrier électronique sont présentés dans un fichier en pièce jointe. Le message contient le texte explicatif suivant :

Le fichier joint contient le rapport sur le fonctionnement de Kaspersky Security 8.0 for Microsoft Exchange Servers.

# CREATION DE RAPPORTS RAPIDES

*Pour créer un rapport rapide, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - Si vous souhaitez créer un rapport pour un serveur de sécurité non réparti, développez le nœud du serveur de sécurité souhaité ;

   - Si vous souhaitez créer un rapport pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour les Serveurs de sécurité duquel vous souhaitez créer un rapport.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats, dans le groupe **Rapports disponibles**, cliquez sur le bouton **Créer un rapport**.

4. Dans la fenêtre **Paramètres de création d'un rapport rapide** qui s'ouvre, sélectionnez une des options suivantes dans la liste **Type de rapport** :

   - **Antivirus pour le rôle serveur de boîtes aux lettres** si vous souhaitez créer un rapport sur le fonctionnement de l'Antivirus pour le rôle serveur de boîtes aux lettres.

   - **Antivirus pour le rôle de serveur de transport hub** si vous souhaitez créer un rapport sur le fonctionnement de l'Antivirus pour le rôle serveur de transport hub.

   - **Anti-Spam** si vous souhaitez créer un rapport sur le fonctionnement de l'Anti-Spam.

5. Dans la liste déroulante **Niveau de détail**, sélectionnez une des options suivantes :

   - Si vous souhaitez créer un rapport contenant des informations restreintes sur les objets traités tout au long de la période du rapport sans indication de l'intervalle de temps au cours duquel l'événement s'est produit, choisissez l'option **Standard** dans la liste.

   - Si vous souhaitez créer un rapport détaillé dans lequel figure l'intervalle de temps pour chaque événement, choisissez l'option **Détaillé**.

     L'ampleur de l'intervalle dépend de la période couverte par le rapport.

6. Les champs **de** et **à** permettent de définir manuellement les dates de début et de fin de la période couverte par le rapport. Il est possible également de choisir les dates dans le calendrier.

7. Si vous créez un rapport pour les Serveurs de sécurité du profil, réalisez les opérations suivantes dans le groupe de paramètres **Créer un rapport selon les statistiques** :

   - Choisissez l'option **Tous les serveurs du profil** si vous souhaitez créer un rapport contenant des informations relatives à l'ensemble des Serveurs de sécurité repris dans le profil. Dans la liste déroulante à droite, sélectionnez le serveur sur lequel le rapport va être créé.

   - Choisissez l'option **Un serveur** si vous souhaitez créer un rapport contenant les informations relatives à un Serveur de sécurité du profil. Dans la liste déroulante de droite, sélectionnez le serveur pour lequel vous souhaitez créer le rapport.

8. Cliquez sur le bouton **OK** afin de créer le rapport rapide sur la base des paramètres définis.

L'application ouvre la fenêtre du rapport dans le navigateur directement après qu'il a été créé et elle affiche les informations relatives au rapport dans le groupe **Rapports disponibles**.

# CREATION DE LA TACHE DE COMPOSITION DES RAPPORTS

*Pour créer une tâche de composition de rapports, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez créer une tâche de composition de rapport pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez créer une tâche de composition de rapport pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez créer la tâche de composition de rapports.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats, dans le groupe **Tâches de création de rapports**, cliquez sur le bouton **Ajouter une tâche**.

4. Dans la fenêtre **Tâche de création de rapports programmée** qui s'ouvre, saisissez le nom de la tâche créée dans le champ **Nom**.

5. Sous l'onglet **Paramètres de création du rapport** dans la liste déroulante **Type de rapport**, sélectionnez une des options suivantes :

   - **Antivirus pour le rôle serveur de boîtes aux lettres** si vous souhaitez créer des rapports sur le fonctionnement de l'Antivirus pour le rôle serveur de boîtes aux lettres.

   - **Antivirus pour le rôle de serveur de transport hub** si vous souhaitez créer des rapports sur le fonctionnement de l'Antivirus pour le rôle serveur de transport hub.

   - **Anti-Spam** si vous souhaitez créer des rapports sur le fonctionnement de l'Anti-Spam.

6. Dans la liste déroulante **Niveau de détail**, sélectionnez un des niveaux de détail proposés pour le rapport :

   - Si vous souhaitez créer des rapports contenant des informations sur les objets traités tout au long de la période du rapport sans indication de l'intervalle de temps au cours duquel l'événement s'est produit, choisissez le niveau **Standard** dans la liste.

   - Si vous souhaitez créer des rapports détaillés dans lequel figure l'intervalle de temps pour chaque événement, choisissez le niveau **Détaillé**.

7. Si vous souhaitez que l'application envoie les rapports à l'adresse de messagerie de l'administrateur, cochez la case **Envoyer à l'administrateur**.

8. Si vous souhaitez que l'application envoie le rapport à l'adresse de messagerie que vous avez renseignée, cochez la case **Envoyer aux destinataires**. Saisissez dans le champ les adresses de messagerie auxquelles vous souhaitez envoyer les rapports.

9. Si vous créez un rapport pour les Serveurs de sécurité du profil, réalisez les opérations suivantes dans le groupe de paramètres **Créer un rapport selon les statistiques** :

   - Sélectionnez l'option **Tous les serveurs du profil** si vous souhaitez créer des rapports contenant des informations relatives à l'ensemble des Serveurs de sécurité repris dans le profil. Dans la liste déroulante à droite, sélectionnez le serveur sur lequel le rapport va être créé.

   - Sélectionnez l'option **Un serveur** si vous souhaitez créer des rapports contenant des informations relatives à un Serveur de sécurité du profil. Dans la liste déroulante de droite, sélectionnez le serveur sur les données duquel doit porter le rapport.

10. Sous l'onglet **Programmation**, cochez la case **Créer un rapport selon une programmation** si vous souhaitez que les rapports soient créés selon un horaire défini.

11. Si vous avez cochez la case **Créer un rapport selon une programmation**, sélectionnez la fréquence de création des rapports selon une programmation :

    - **Tous les X jours**. Indiquez dans le champ **tous les X jours** l'intervalle en jours de création des rapports. Dans le champ **Heure de lancement**, saisissez l'heure de création du rapport.

    - **Chaque semaine**. Dans le groupe **Jour de lancement**, sélectionnez les jours de la semaine quand l'application doit créer les rapports. Dans le champ **Heure de lancement**, saisissez l'heure de création du rapport.

    - **mensuel**. Dans le champ **Jour du mois**, indiquez le jour du mois quand l'application doit créer les rapports. Dans le champ **Heure de lancement**, saisissez l'heure de création du rapport.

12. Cliquez sur **OK**.

    L'application affiche la tâche créée de composition des rapports dans le groupe **Tâches de création de rapports**.

# MODIFICATION DES PARAMETRES DE LA TACHE DE COMPOSITION DES RAPPORTS

*Pour modifier les paramètres de la tâche de composition des rapports, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

    - si vous souhaitez modifier les paramètres de la tâche de création des rapports pour le Serveur de sécurité non répartir, développez le nœud du Serveur de sécurité requis ;

    - si vous souhaitez modifier les paramètres de la tâche de création des rapports pour le Serveur de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour lequel vous souhaitez modifier les paramètres de la tâche de composition des rapports pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le volet des résultats du groupe **Tâches de création de rapports**, sélectionnez dans le tableau la tâche dont vous souhaitez modifier les paramètres.

4. Cliquez sur le bouton **Modifier** au-dessus du tableau des tâches.

5. Dans la fenêtre **Tâche de création de rapports programmée** qui s'ouvre, modifiez les paramètres requis.

6. Cliquez sur **OK**.

# LANCEMENT DE LA TACHE DE COMPOSITION DES RAPPORTS

*Pour lancer la tâche de composition des rapports, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

    - si vous souhaitez une tâche de composition des rapports pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

    - si vous souhaitez lancer une tâche de composition de rapports pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour lequel vous souhaitez lancer la tâche de composition des rapports pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats, dans le groupe **Tâches de création de rapports**, cliquez sur le bouton **Lancer la tâche**.

L'application ouvre la fenêtre du rapport dans le navigateur directement après qu'il a été créé et elle affiche les informations relatives au rapport dans le groupe **Rapports disponibles**.

# SUPPRESSION DE LA TACHE DE COMPOSITION DES RAPPORTS

*Pour supprimer une tâche de composition de rapports, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez supprimer la tâche de composition des rapports pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez supprimer la tâche de composition des rapports pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil pour lequel vous souhaitez supprimer la tâche de composition des rapports pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats, dans le groupe **Tâches de création de rapports**, sélectionnez dans le tableau la tâche que vous souhaitez modifier.

4. Cliquez sur le bouton **Supprimer** au-dessus de la table des tâches.

   Une fenêtre de confirmation s'ouvre.

5. Cliquez sur **Oui**.

La tâche sélectionnez sera supprimée du tableau des tâches dans le groupe **Tâches de création de rapports**.

# CONSULTATION DES TACHES DE COMPOSITION DES RAPPORTS

*Pour consulter la tâche de composition de rapports, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez consulter la tâche de composition de rapports pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez consulter la tâche de composition des rapports pour les Serveurs de sécurité du profil, développez le nœud **Profils** , puis développez le nœud du profil pour lequel vous souhaitez consulter la tâche de composition des rapports pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats de la **Tâche de création de rapport**, toutes les tâches créées apparaissent dans le tableau. Les informations suivantes sont proposées pour chaque tâche :

   - **Nom de la tâche**. Nom de la tâche de composition de rapports créés.

- **Type**. Type de rapportscréés : Anti-Spam, Antivirus pour le rôle serveur de boîte aux lettres ou Antivirus pour le rôle serveur de transport Hub.
- **Niveau de détail**. Niveau de détail du rapport créé : détaillé ou standard.
- **Zone d'action**. Profil/serveur ou cluster dont les données apparaissent dans les rapports composés.
- **Programmation**. Programmation de la composition des rapports.
- **Heure de la dernière modification**. Heure de la dernière modification de la tâche de composition des rapports.
- **Prochain lancement**. Prochain lancement programmé de la tâche de composition de rapports.
- **Lancement automatique**. Informations sur la programmation du lancement de la tâche.
- **Serveur de création**. Serveur sur lequel les rapports sont créés.

# CONSULTATION DES RAPPORTS PRETS

*Pour consulter les rapports sur le fonctionnement de l'Antivirus et de l'Anti-Spam, procédez comme suit.*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :
   - si vous souhaitez consulter le rapport pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité ;
   - si vous souhaitez consulter le rapport pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis le nœud du profil dont vous souhaitez consulter les rapports pour les Serveurs de sécurité.
2. Sélectionnez le nœud **Rapports**.
3. Dans le panneau des résultats, dans le groupe **Rapports disponibles**, tous les rapports créés apparaissent dans le tableau Les informations suivantes sont proposées pour chaque rapport :
   - **Nom**. Nom du rapport par défaut.
   - **Date de création**. Date et heure de création du rapport.

     Cette colonne affiche l'heure, selon les paramètres régionaux de l'ordinateur sur lequel la console d'administration est exécutée.
   - **Fréquence**. Période pour laquelle les données sont affichées dans le rapport.
   - **Source des données**. Nom du serveur, du profil, du DAG ou du cluster de serveurs (uniquement pour le rapport de l'Antivirus pour le rôle de serveur de boîte aux lettres) dont les données figurent dans le rapport.
   - **Type**. Type de rapport : Anti-Spam, Antivirus pour le rôle serveur de boîte aux lettres ou Antivirus pour le rôle serveur de transport Hub.
   - **Niveau de détail**. Niveau de détail du rapport : détaillé ou standard.
   - **Serveur de création**. Serveur sur lequel le rapport est créé.
4. Pour consulter un rapport, sélectionnez-le dans la liste, puis cliquez sur le bouton **Afficher**.

   Le rapport sélectionné sera ouvert dans la fenêtre du navigateur par défaut.

### Consultation du rapport de l'Antivirus

Le rapport de l'Antivirus contient les données suivantes dans l'en-tête :

- type de rapport ;
- nom du serveur, du cluster ou du DAG pour lequel le rapport a été créé ;
- période pour laquelle le rapport est créé ;
- jour, mois, année et heure de création du rapport (heure locale de l'ordinateur sur lequel la création du rapport a été exécutée).

Le tableau du rapport standard de l'Antivirus reprend les informations suivantes :

- **Etat**. Etat de l'objet après le traitement par l'Antivirus.
- **Nombre d'objets**. Nombre d'objets portant cet état.
- **Taux de répartition**. Part d'objets portant cet état sur le total d'objets.
- **Taille**. Taille des objets (messages, leurs parties ou les pièces jointes) en mégaoctets.

Le tableau du rapport détaillé de l'Antivirus reprend les informations suivantes :

- **Période**. Intervalle de temps pendant lequel le ou les objets ont été découverts.
- **Objets non infectés**. Nombre d'objets sains.
- **Objets réparés**. Nombre d'objets qui ont pu être réparés.
- **Objets non réparés** :
  - **Objets infectés**. Nombre d'objets infectés par des virus ou leurs modifications.
  - **Objets potentiellement infectés**. Nombre d'objets qui peuvent contenir un virus inconnu.
  - **Objets protégés**. Nombre d'objets protégés par un mot de passe, par exemple des archives.
  - **Objets endommagés**. Nombre d'objets qui ne peuvent être réparés car ils sont endommagés.
- **Objets non traités** :
  - **Problèmes de licence**. Nombre d'objets qui n'ont pas été analysés en raison de problèmes avec la licence de Kaspersky Security.
  - **Erreur de bases de l'Antivirus**. Nombre d'objets qui n'ont pas été analysés en raison d'erreurs survenues à cause de bases de l'Antivirus endommagées ou manquantes.
  - **Erreur de traitement**. Nombre d'objets pendant l'analyse desquels une erreur est survenue.
- **Nombre total d'objets**. Nombre total d'objets soumis à l'analyse.

La ligne **Pour toute la période** indique le total des objets pour chaque colonne pour l'ensemble de la période couverte par le rapport.

### Consultation du rapport de l'Anti-Spam

Le rapport standard de l'Anti-Spam contient les données suivantes dans l'en-tête :

- jour, mois, année et heure de création du rapport (heure locale de l'ordinateur sur lequel la création du rapport a été lancée).
- type de rapport ;
- nom du serveur pour lequel le rapport est créé ;
- période pour laquelle le rapport est créé ;
- serveurs sur les données duquel porte la création du rapport (si le rapport a été créé pour un profil ou un DAG).

Le tableau du rapport standard de l'Anti-Spam reprend les informations suivantes :

- **Etat**. Etat du message après le traitement par l'Anti-Spam.
- **Nombre de messages**. Nombre de messages portant l'état indiqué.
- **Taux de répartition**. Part de messages portant l'état indiqué sur le total des messages.
- **Taille**. Taille des messages en mégaoctets.

Le tableau du rapport détaillé de l'Anti-Spam reprend les informations suivantes :

- **Période**. Période pendant laquelle les messages ont été traités.
- **Sains**. Nombre de messages qui ne contiennent pas de courrier indésirable ou de liens de phishing ainsi que leur taille en Mo.
- **De confiance**. Nombre de messages en provenance d'expéditeurs de confiance ainsi que leur taille en Mo.
- **Courrier indésirable**. Nombre de messages qui appartiennent au courrier indésirable ainsi que leur taille en Mo.
- **Courrier indésirable potentiel**. Nombre de messages qui appartiennent au courrier indésirable potentiel ainsi que leur taille en Mo.
- **Envoi massif**. Nombre de messages envoyés par publipostage qui ne sont pas des courriers indésirables ainsi que leur taille en Mo.
- **Notifications formelles**. Nombre de messages contenant des informations relatives à la remise du message et autres messages de service ainsi que leur taille en Mo.
- **Ajoutés à la liste noire**. Nombre de messages d'expéditeurs dont l'adresse a été ajoutée à la liste noire ainsi que leur taille en Mo.
- **Phishing**. Nombre de messages contenant des liens de phishing.
- **Non vérifié**. Nombre de messages qui n'ont pas été vérifiés par l'Anti-Spam, ainsi que leur taille en Mo.

La ligne **Pour toute la période** reprend le total de message pour chaque colonne sur l'ensemble de la période couverte par le rapport ainsi que leur taille en Mo.

# ENREGISTREMENT DU RAPPORT

*Pour enregistrer les rapports sur le fonctionnement de l'Antivirus et de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez enregistrer un rapport pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité requis ;

   - si vous souhaitez enregistrer le rapport pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil dont vous souhaitez enregistrer le rapport pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le groupe **Rapports disponibles** du panneau des résultats, sélectionnez dans le tableau le rapport que vous souhaitez enregistré, puis cliquez sur **Enregistrer**.

4. Dans la fenêtre **Enregistrer sous** qui s'ouvre, indiquez le dossier dans lequel vous souhaitez enregistrer l'objet et, le cas échéant, saisissez un nom pour l'objet ou modifiez le nom existant.

5. Cliquez sur le bouton **Enregistrer**.

# SUPPRESSION DU RAPPORT

*Pour supprimer les rapports sur le fonctionnement de l'Anti-Virus et de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez supprimer un rapport pour un Serveur de sécurité non réparti, développez le nœud du Serveur en question.

   - Si vous souhaitez supprimer un rapport pour les Serveurs de sécurité du profil, développez le nœud **Profils**, puis développez le nœud du profil dont vous souhaitez supprimer le rapport pour les Serveurs de sécurité.

2. Sélectionnez le nœud **Rapports**.

3. Dans le groupe **Rapports disponibles** du panneau des résultats, sélectionnez dans le tableau le rapport que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   Une fenêtre de confirmation s'ouvre.

4. Cliquez sur **Oui**.

Le rapport sélectionné sera supprimé depuis le tableau des rapports.

# JOURNAUX DE L'APPLICATION

Cette section décrit les journaux de l'application et leur configuration.

### DANS CETTE SECTION DE L'AIDE

Présentation des journaux de l'application ..... 109

Configuration des paramètres des journaux..... 110

Configuration du niveau de diagnostic ..... 110

## PRESENTATION DES JOURNAUX DE L'APPLICATION

Kaspersky Security permet de consigner les événements survenus pendant l'utilisation de l'application dans le journal des applications du système d'exploitation Microsoft Windows et dans ses propres journaux.

L'exhaustivité des informations enregistrées dans les journaux dépend du niveau de diagnostic défini dans les paramètres de l'application (cf. section « Configuration du niveau de diagnostic » à la page 110).

La consultation des événements enregistrés dans le journal des applications Microsoft Windows s'opère à l'aide du composant Microsoft Windows standard Observateur d'événements. L'application désigne les événements de Kaspersky Security à l'aide de l'abréviation KSCM8 dans la colonne **Source** du journal des applications Microsoft Windows afin de les distinguer des autres événements consignés dans le journal des applications.

Les journaux de Kaspersky Security sont tenus dans deux formats et la structure du nom dépend de ce format :

- kselog.aaaajjmm[N].log : journal principal de l'application où N désigne le numéro du fichier du journal. Le numéro du journal est indiqué si plusieurs fichiers de journal ont été créés au cours de la période de fonctionnement de l'application.
- Updateaaaajjmm.log – journal de la mise à jour des bases.
- AntivirusScanneraaaajjmm[N].log – journal de l'analyse de l'Antivirus où N désigne le numéro de traitement de l'Antivirus.

L'application crée par défaut un journal chaque jour à 00:00. L'application consigne les informations à la fin du journal de l'application le plus récent. Par défaut, la taille du journal est limitée à 100 Mo. Cette valeur peut être modifiée. Quand un journal atteint sa taille maximale, il est archivé et un autre journal est créé.

La consultation des journaux de l'application s'opère à l'aide d'une application standard d'édition de fichiers texte (par exemple, le Bloc-Notes).

Les journaux sont conservés localement dans le dossier Logs. Ce dossier se trouve sur le serveur dans le dossier d'installation de l'application dont le chemin d'accès est défini pendant l'installation.

Un journal est créé pour chaque serveur de sécurité, quelle que soit la variante de déploiement de l'application.

# CONFIGURATION DES PARAMETRES DES JOURNAUX

*Pour configurer les paramètres des journaux, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer les paramètres des journaux pour un Serveur de sécurité non réparti, développez le nœud du serveur de sécurité souhaité ;

   - si vous souhaitez configurer les paramètres des journaux pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer les paramètres des journaux.

2. Sélectionnez le nœud **Configuration**.

3. Dans le groupe de paramètres **Diagnostic** du panneau des résultats, sélectionnez une des valeurs suivantes dans la liste déroulante **Enregistrer un nouveau fichier de journal** :

   - **Chaque jour**. Un fichier journal sera créé chaque jour.

   - **Chaque semaine**. Un fichier journal sera créé chaque semaine.

   - **Chaque mois**. Un fichier journal sera créé chaque mois.

   - **Si le fichier dépasse la taille maximale**. Un fichier journal sera créé si la taille maximale du fichier journal est dépassée.

4. Dans le champ avec défilement **Taille maximale du fichier**, indiquez la taille maximale du fichier journal.

   Par défaut, la taille maximale du fichier est de 100 Mo.

5. Cochez la case **Notifier les erreurs par courrier électronique** si vous souhaitez que l'administrateur reçoive des notifications relatives à ces erreurs par courrier électronique (cf. section « Configuration des paramètres de notification » à la page 97) au moment de leur consignation.

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

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, les paramètres des journaux configurés sur un des serveurs sont appliqués automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer les paramètres des journaux sur les autres serveurs du DAG.

# CONFIGURATION DU NIVEAU DE DIAGNOSTIC

Le niveau de détail et l'exhaustivité des informations consignées dans les journaux dépendent du niveau de diagnostic défini.

*Pour configurer le niveau de diagnostic, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, réalisez les actions suivantes :

   - si vous souhaitez configurer le niveau de diagnostic des journaux pour un Serveur de sécurité non réparti, développez le nœud du Serveur de sécurité en question ;

   - si vous souhaitez configurer le niveau de diagnostic des journaux pour les Serveurs de sécurité du profil, développez le nœud **Profils** et développez le nœud du profil pour les Serveurs de sécurité pour lesquels vous souhaitez configurer le niveau de diagnostic des journaux.

2. Sélectionnez le nœud **Configuration**.

3. Dans le groupe de paramètres **Diagnostic** du panneau des résultats, sélectionnez une des options suivantes dans la liste **Niveau de détail** :

   - **Minimal** si vous souhaitez que les journaux contiennent un minimum d'informations.
   - **Personnalisé** si vous souhaitez configurer la consignation détaillée des événements qui vous intéressent pour l'analyse des bogues et leur suppression.

   La tenue de tels journaux peut considérablement ralentir l'application. Outre cela, les corps des messages peuvent être enregistrés dans les journaux détaillés.

4. Si vous avez choisi l'option **Personnalisé**, procédez comme suit :

   a. Cliquez sur le bouton **Configuration**.

   b. Dans la fenêtre **Paramètres du diagnostic** qui s'ouvre, cochez les cases en regard des modules et des événements pour lesquels vous souhaitez activer la journalisation détaillée.

   c. Cliquez sur **OK** dans la fenêtre **Paramètres du diagnostic**.

5. Cliquez sur le bouton **Enregistrer** dans le panneau des résultats.

Si l'application fonctionne sur un DAG de serveurs Microsoft Exchange, le niveau de diagnostic configuré sur un des serveurs est appliqué automatiquement aux autres serveurs du DAG. Il n'est pas nécessaire de configurer le niveau de diagnostic sur les autres serveurs du DAG.

# ADMINISTRATION DES CONFIGURATIONS

Cette section contient des informations sur la manière d'exporter la configuration de l'application dans un fichier et de l'importer depuis un fichier. Le fichier de configuration est un fichier au format XML.

### DANS CETTE SECTION DE L'AIDE

Exportation de la configuration ..... 112

Importation de la configuration ..... 113

## EXPORTATION DE LA CONFIGURATION

*Pour exporter la configuration de l'application dans un fichier, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez le nœud **Configuration**.
3. Dans le groupe de paramètres **Administration de la configuration** du panneau des résultats, cliquez sur le bouton **Exporter**.
4. Dans la fenêtre **Sélection des paramètres de configuration** qui s'ouvre, cochez les cases des groupes de paramètres que vous souhaitez exporter :
   - **Tous les paramètres**. Tous les paramètres qui constituent la configuration de l'application.
   - **Protection pour le rôle serveur de transport Hub.** Groupe de paramètres en rapport avec le module de protection pour le rôle serveur de transport Hub.
   - **Protection pour le rôle serveur de boîte aux lettres** Groupe de paramètres en rapport avec le module de protection pour le rôle serveur de boîte aux lettres.
   - **Paramètres complémentaires de l'Antivirus**. Les paramètres complémentaires de l'Antivirus tels que les paramètres KSN, les paramètres d'analyse des archives et des coffres-forts et les exclusions de l'analyse de l'Antivirus.
   - **Mises à jour**. Les paramètres de mise à jour des bases de l'application.
   - **Connexion**. Paramètres des diagnostics et des journaux des événements de l'application.
   - **Rapports**. Paramètres des rapports.
   - **Notifications**. Paramètres des notifications.
   - **Infrastructure**. Groupe de paramètres reprenant les paramètres suivants :
     - paramètres de connexion à Microsoft SQL Server : nom du serveur et nom de la base de données ;
     - paramètres de connexion au serveur proxy.
5. Cliquez sur **OK**.
6. Dans la fenêtre **Enregistrer sous** qui s'ouvre, saisissez le nom du fichier, sélectionnez le dossier cible, puis cliquez sur le bouton **Enregistrer**.

L'application enregistre les paramètres sélectionnés pour la configuration dans un fichier portant l'extension kseconfig.

# IMPORTATION DE LA CONFIGURATION

*Pour importer la configuration de l'application depuis un fichier, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du serveur de sécurité.
2. Sélectionnez le nœud **Configuration**.
3. Dans le groupe de paramètres **Administration de la configuration** du panneau des résultats, cliquez sur le bouton **Importer**.
4. Dans la fenêtre **Ouvrir** qui s'ouvre, sélectionnez le fichier de configuration de l'application, puis cliquez sur le bouton **Ouvrir**.

   Vous ne pouvez sélectionner que les fichiers portant l'extension .kseconfig.

L'application importe la configuration depuis le fichier sélectionné. Les valeurs des paramètres téléchargés depuis le fichier remplacent les valeurs actuelles des paramètres de l'application sans demande de confirmation.

# VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION

Cette section explique comment vérifier le fonctionnement de l'application, à savoir confirmer que l'application détecte les fichiers et leur modification et qu'elle exécute sur ceux-ci les actions configurées.

### DANS CETTE SECTION DE L'AIDE


Présentation du fichier d'essai EICAR ..... 114

Présentation des types de fichier d'essai EICAR ..... 114

Vérification du fonctionnement de l'application à l'aide du fichier d'essai EICAR ..... 116


## PRESENTATION DU FICHIER D'ESSAI EICAR

Vous pouvez confirmer la détection des virus et la réparation des fichiers infectés à l'aide du *fichier d'essai EICAR*. Ce fichier d'essai a été développé spécialement par l'European Institute for Computer Antivirus Research afin de tester les logiciels antivirus.

Le fichier d'essai EICAR n'est pas un virus. Le fichier d'essai EICAR ne contient aucun code informatique capable de nuire à l'ordinateur. Mais la majorité des logiciels antivirus identifie le fichier d'essai EICAR en tant que virus.

Le fichier d'essai EICAR n'est pas prévu pour tester le fonctionnement de l'analyse heuristique ou la recherche de programmes malveillants au niveau du système (outils de dissimulation d'activité).

N'utilisez en aucun cas de véritables virus afin de tester le fonctionnement des logiciels antivirus ! Cela pourrait nuire à votre ordinateur.

N'oubliez pas de rétablir la protection antivirus du trafic Internet et des fichiers après avoir utilisé le fichier d'essai EICAR.

## PRESENTATION DES TYPES DE FICHIER D'ESSAI EICAR

Vous pouvez vérifier les fonctions de l'application en créant divers types du fichier d'essai EICAR. L'application détecte le fichier d'essai EICAR (son type) et lui attribue un statut en fonction des résultats de l'analyse. L'application exécute sur le fichier d'essai EICAR les actions configurées dans les paramètres du composant qui a détecté le fichier d'essai EICAR.

La première colonne du tableau (cf. tableau ci-après) contient les préfixes que vous pouvez utiliser pour créer des types du fichier d'essai EICAR. La deuxième colonne reprend toutes les valeurs possibles de l'état attribué au fichier par application à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux fichiers de l'état indiqué.

*Table 5. Types du fichier d'essai EICAR*

| Préfixe | Etat du fichier | Informations sur le traitement du fichier |
|---|---|---|
| Pas de préfixe, virus d'essai standard. | **Infecté**.<br>Le fichier contient le code d'un virus connu. La réparation du fichier est impossible. | L'application identifie ce fichier comme un fichier contenant un virus qui ne peut être réparé.<br>La tentative de réparation du fichier s'opère selon l'action définie pour les fichiers infectés. Par défaut, l'application affiche un message qui indique que la réparation du fichier infecté est impossible. |
| CURE- | **Infecté**.<br>Le fichier contient le code d'un virus connu. La réparation du fichier est possible. | Le fichier contient un virus qui peut être réparé ou supprimé. L'application répare le fichier et le texte du corps du virus est remplacé par CURE.<br>L'application affiche un message qui signale la découverte d'un fichier infecté. |
| DELE- | **Infecté**.<br>Le fichier contient le code d'un virus connu. La réparation du fichier est impossible. | L'application identifie ce fichier comme un virus qui ne peut être réparé et le supprime.<br>L'application affiche un message qui signale la suppression d'un fichier infecté. |
| WARN- | **Potentiellement infecté**.<br>Le fichier contient le code d'un virus inconnu. La réparation du fichier est impossible. | Le fichier est considéré comme potentiellement infecté.<br>L'application exécute l'action définie pour les fichiers potentiellement infectés. Par défaut, l'application affiche une notification sur la détection d'un fichier potentiellement infecté. |
| SUSP- | **Potentiellement infecté.**<br>Le fichier contient le code modifié d'un virus connu. La réparation du fichier est impossible. | L'application a découvert une équivalence partielle entre un extrait du code du fichier et un extrait du code d'un virus connu. Au moment de cette découverte du fichier potentiellement infecté, les bases de l'application ne contenaient pas la description du code complet de ce virus.<br>L'application exécute l'action définie pour les fichiers potentiellement infectés. Par défaut, l'application affiche une notification sur la détection d'un fichier potentiellement infecté. |
| CORR- | **Corrompu**. | L'application n'analyse pas le fichier de ce type car sa structure est endommagée (par exemple, format de fichier non correct). Les informations relatives au traitement du fichier figurent dans le rapport sur le fonctionnement de l'application. |
| ERRO- | **Erreur d'analyse**. | Une erreur s'est produite lors de l'analyse du fichier. L'application ne peut accéder au fichier car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers le fichier (lorsque le fichier se trouve sur une ressource de réseau). Les informations relatives au traitement du fichier figurent dans le rapport sur le fonctionnement de l'application. |

# VERIFICATION DU FONCTIONNEMENT DE L'APPLICATION A L'AIDE DU FICHIER D'ESSAI EICAR

Une fois que vous aurez installé et configuré Kaspersky Security, il est conseillé de vérifier l'exactitude de la configuration et le bon fonctionnement de l'application à l'aide du « virus » d'essai EICAR.

Vous pouvez télécharger le fichier d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

Il est vivement recommander d'activer la protection antivirus du serveur après avoir utilisé le fichier d'essai EICAR. La désactivation de la protection antivirus du serveur augmente sensiblement le risque de pénétration d'un programme malveillant via le système de messagerie.

### Vérification du fonctionnement de l'Antivirus

- *Pour envoyer le message avec le fichier d'essai, procédez comme suit :*

1. Créez un message avec le fichier d'essai EICAR en pièce jointe.
2. Envoyez le message via le serveur Microsoft Exchange sur lequel est installée l'application Kaspersky Security avec le serveur de sécurité activé (cf. rubrique « Connexion de la Console d'administration au Serveur de sécurité » à la page 43).
3. Confirmez que le message remis ne contient aucun virus.

En cas de détection d'un virus sur un serveur de boîte aux lettres, le virus supprimé est remplacé par un fichier texte. En cas de détection d'un virus sur un serveur déployé dans le rôle de transport Hub, le préfixe Malicious object deleted est ajouté à l'objet du message.

Une fois le virus découvert, une notification sera envoyée à l'adresse électronique indiquée dans les paramètres des notifications (cf. rubrique « Configuration des paramètres des notifications » à la page 97).

- *Pour consulter le rapport sur le virus détecté dans l'application, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du Serveur de sécurité via lequel le message contenant le fichier de test EICAR avait été envoyé.
2. Sélectionnez le nœud **Rapports**.
3. Réalisez les opérations suivantes dans le groupe déroulant **Rapports rapides** du panneau des résultats :
   a. Sélectionnez, dans la liste déroulante **Type**, le type de rapport **Antivirus pour le rôle serveur de boîtes aux lettres** ou **Antivirus pour le rôle de serveur de transport hub** (en fonction de la configuration en vigueur).
   b. Cliquez sur le bouton **Créer un rapport**.
4. Consultez le rapport dans le groupe déroulant **Rapports disponibles** après l'avoir sélectionné dans la liste et cliquez sur le bouton **Afficher**.

   Si le rapport contient des informations sur une infection par le virus EICAR, cela signifie que la configuration de l'application est correcte.

- *Pour configurer l'envoi des rapports à l'adresse de messagerie de l'administrateur, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du Serveur de sécurité via lequel le message contenant le fichier de test EICAR avait été envoyé.

2. Sélectionnez le nœud **Rapports**.

3. Dans le panneau des résultats, dans les groupes déroulant des paramètres **Rapport de l'antivirus pour le rôle Boîte aux lettres** et **Rapport de l'Antivirus pour le rôle Transport Hub**, cochez la case **Administrateur** dans le groupe **Envoyer le rapport à l'adresse électronique** afin d'envoyer les notifications à l'adresse de messagerie de l'administrateur reprise dans les paramètres d'envoi des notifications (cf. section "Configuration des paramètres d'envoi des notifications" à la page 98).

4. Pour confirmer que les rapports seront bien remis à l'adresse indiquée, cliquez sur le bouton **Test** afin d'envoyer un message d'essai.

Par défaut, l'application conserve une copie de l'objet infecté dans la sauvegarde.

*Pour voir si la copie de l'objet infecté a été enregistrée dans la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du Serveur de sécurité via lequel le message contenant le fichier de test EICAR avait été envoyé.

2. Choisissez le nœud **Sauvegarde**.

3. Assurez-vous que l'objet infecté (message avec fichier d'essai EICAR en pièce-jointe) apparaît dans la fenêtre des résultats.

## Vérification du fonctionnement de l'Anti-Spam

*Pour vérifier le fonctionnement de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console d'administration, développez le nœud du Serveur de sécurité via lequel le message contenant le fichier de test EICAR sera envoyé.

2. Sélectionnez le nœud **Protection du serveur**.

3. Dans le panneau des résultats, sous l'onglet **Protection pour le rôle serveur de transport Hub** cochez la case **Ajouter l'adresse de l'expéditeur à la liste noire** dans le groupe déroulant de paramètres **Paramètres des listes blanche et noire de l'Anti-Spam**.

4. Saisissez dans le champ l'adresse électronique de n'importe quelle boîte aux lettres à laquelle vous avez accès.

5. Cliquez sur le bouton  situé à droite du champ.

6. Sous l'onglet **Protection pour le rôle serveur de transport Hub** dans le bloc déroulant de paramètres **Paramètres d'analyse de l'Anti-Spam**, dans le groupe de paramètres **Paramètres de traitement du courrier indésirable** pour l'état **Ajouté à la liste noire**, choisissez l'option **Ignorer** et cochez la case **Ajouter un intitulé**.

7. Envoyez le message d'essai depuis la boîte aux lettres indiquée à l'adresse de l'administrateur via le serveur de messagerie protégé.

Si l'objet du message reçu contient la note [Blacklisted], l'Anti-Spam fonctionne correctement.

# CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

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

### DANS CETTE SECTION DE L'AIDE

Modes d'obtention de l'assistance technique ..... 118

Assistance technique par téléphone..... 118

Obtention de l'assistance technique via Kaspersky Company Account ..... 119

Utilisation du fichier de traçage et du script AVZ..... 120

## MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous ne trouvez pas la solution à votre problème dans la documentation ou dans une des sources d'informations à son sujet (cf. section « Sources d'informations sur l'application » à la page 11), nous vous conseillons de contacter le service d'assistance technique de Kaspersky Lab. Les opérateurs du service d'assistance technique répondront à vos questions concernant l'installation et l'utilisation de l'application.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

Vous pouvez contacter les experts du service d'assistance technique de l'une des méthodes suivantes :

- Par téléphone. Cette méthode permet de contacter les opérateurs du service d'assistance technique russophone ou international.
- Via Mon espace personnel sur le site du service d'assistance technique. Cette méthode permet de contacter les experts du service d'assistance technique via le formulaire de requête.

L'assistance technique est uniquement proposée aux utilisateurs qui ont acheté une licence pour l'application. L'assistance technique n'est pas proposée aux utilisateurs des versions d'évaluation.

## ASSISTANCE TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support technique français et international (http://support.kaspersky.com/fr/support/international).

Avant de vous adresser au Support technique, veuillez prendre connaissance des règles applicables (http://support.kaspersky.com/fr/support). Nos experts pourront ainsi vous venir en aide plus rapidement.

# ASSISTANCE TECHNIQUE VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.fr/) est un service en ligne qui permet d'envoyer des requêtes à Kaspersky Lab et d'en suivre le traitement par les experts de Kaspersky Lab.

Vous devez vous enregistrer pour accéder à Kaspersky CompanyAccount. Vous pouvez vous inscrire sur la page d'enregistrement (https://support.kaspersky.fr/companyaccount/registration). Vous pouvez également être enregistré par un utilisateur doté des autorisations d'administration du compte de votre entreprise dans Kaspersky CompanyAccount.

Le compte de votre entreprise dans Kaspersky CompanyAccoount est créé lors du premier enregistrement de la licence que votre société a achetée dans Kaspersky CompanyAccount. Par la suite, tous les employés de votre société qui s'enregistrent dans Kaspersky CompanyAccount sont associés à ce compte.

Si un nouveau compte utilisateur pour votre société est créé lors de l'enregistrement dans Kaspersky CompanyAccount, vous ne recevez pas défaut les autorisations d'administration de ce compte, à savoir les autorisations pour exécuter toutes les opérations possibles à l'aide de ce compte. Si, lors de l'enregistrement, vous vous associez au compte existant de votre société, vous recevez par défaut des autorisations réduites.

Les détails relatifs au Kaspersky CompanyAccount et aux actions que vous pouvez réaliser à l'aide de Kaspersky CompanyAccount figurent sur la page (http://support.kaspersky.fr/faq/companyaccount_help) du site du Service de Support Technique.

### Envoi d'une demande au service d'assistance technique par voie électronique

Vous pouvez envoyer vos demandes au service d'assistance technique en russe, en anglais et dans d'autres langues.

Il faut remplir les champs suivants dans le formulaire de requête en ligne :

- Le type de requête.
- Le nom et le numéro de version de l'application.
- Le texte du message.

Le cas échéant, vous pouvez joindre des fichiers au formulaire de demande en ligne.

L'expert du Support Technique répond via le système Kaspersky CompanyAccount en envoyant un message électronique à l'adresse indiquée lors de l'enregistrement.

### Requête adressée au laboratoire des virus

Certaines requêtes ne doivent pas être envoyées au service d'assistance technique, mais au laboratoire des virus.

Vous pouvez envoyer des requêtes au laboratoire des virus dans les cas suivants :

- si vous soupçonnez que le fichier ou l'URL contient un virus mais que Kaspersky Security n'a détecté aucune menace. Les experts du laboratoire des virus analysent le fichier ou l'URL envoyé et s'ils détectent un virus inconnu jusqu'à présent, ils ajoutent sa définition à la base des données qui sera accessible lors de la mise à jour des applications de Kaspersky Lab.
- si Kaspersky Security considère qu'un fichier ou une URL contient un virus, mais que vous êtes convaincu que le fichier ou l'URL ne présente aucune menace.

Vous pouvez également envoyer une demande au Laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.fr/virlab/helpdesk.html?LANG=fr) sans vous enregistrer dans Kaspersky CompanyAccount.

# UTILISATION DU FICHIER DE TRAÇAGE ET DU SCRIPT AVZ

Après avoir signalé le problème aux experts du Support Technique, ceux-ci peuvent vous demander de composer un rapport reprenant les informations relatives au système d'exploitation et de l'envoyer au Support Technique. Les experts du Support Technique peuvent vous demander également de créer un *fichier de traçage*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

L'analyse des données que vous envoyez permet aux experts du Support Technique de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet d'analyser les processus exécutés à la recherche de code malveillant, de rechercher la présence de code malveillant dans le système, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

# APPLICATION. SCRIPT D'ENVOI D'UN MESSAGE NON SOLLICITE POUR EXAMEN

Cette section contient des informations sur le script d'envoi d'un message non sollicité aux experts de Kaspersky Lab pour examen et sur la configuration de ses paramètres.

### DANS CETTE SECTION DE L'AIDE


Présentation du script d'envoi d'un message non sollicité pour examen ..... 121

Mode de fonctionnement du script ..... 122

Paramètres de lancement du script ..... 123

Configuration des paramètres du fichier de configuration du script ..... 124

Journal de fonctionnement du script ..... 125


## PRESENTATION DU SCRIPT D'ENVOI D'UN MESSAGE NON SOLLICITE POUR EXAMEN

Le module Anti-Spam bloque les messages non sollicités qui présentent des caractéristiques connues à ce moment des diffusions de messages non sollicités. Si l'utilisateur de la boîte aux lettres reçoit des messages non sollicités que le module Anti-Spam ne connaît pas encore, le destinataire peut transférer ces exemples de messages non sollicités non filtrés aux experts de Kaspersky Lab qui les traiteront. C'est une manière efficace d'enrichir la base de données de l'Anti-Spam et de bloquer plus vite la diffusion des messages non sollicités, empêchant ainsi la propagation.

Les utilisateurs peuvent transmettre les exemples de messages non sollicités à Kaspersky Lab en les plaçant dans le dossier **Courrier indésirable** (**Junk E-Mail**). La recherche des messages dans le dossier **Courrier indésirable** des boîtes de réception des utilisateurs indiqués et le transfert de ces messages à l'adresse renseignée s'opère à l'aide de ce que l'on appelle le *script d'envoi des messages non sollicités pour examen* (ci-après, le *script*). Le script transfère uniquement les messages qui ont été ajoutés au dossier **Courrier indésirable** depuis le nombre de jours indiqués et qui n'ont pas été traités par d'autres systèmes de protection contre le courrier indésirable.

Le script envoie à Kaspersky Lab les messages du dossier **Courrier indésirable** et tout ce qu'ils contiennent. Il faut signaler aux utilisateurs des boîtes de réception qu'en plaçant les messages dans le dossier **Courrier indésirable**, ils confirment qu'ils ne contiennent pas d'informations confidentielles.

Le script est exécuté au nom du compte utilisateur dont l'adresse de messagerie appartient à l'infrastructure Microsoft Exchange de l'organisation et qui a accès à Exchange Web Services. Ce compte utilisateur doit pouvoir modifier le dossier **Courrier indésirable** de toutes les boîtes aux lettres traitées.

Pour pouvoir créer le journal de fonctionnement du script et manipuler le fichier de configuration des paramètres du script, le compte utilisateur sous lequel le script est exécuté doit pouvoir accéder en écriture au dossier dans lequel ils se trouvent (<Dossier d'installation de l'application\SpamForwarder>).

*Pour ouvrir un dossier avec un script,*

sélectionnez **Démarrer → Programmes → Kaspersky Security 8.0 for Microsoft Exchange Servers → Script d'envoi d'un message non sollicité pour examen**

Pour que le script fonctionne, l'interface Microsoft Exchange Web Services Managed API 2.0 doit être installée. Le module de cette interface doit être téléchargé en cliquant sur le lien http://www.microsoft.com/fr-fr/download/default.aspx et enregistré dans le sous-dossier bin du dossier contenant le script.

# MODE DE FONCTIONNEMENT DU SCRIPT

Il existe deux modes de fonctionnement du script :

- mode de définition des autorisations ;
- mode de fonctionnement normal.

### Mode de définition des autorisations

Dans le mode de définition des autorisations, le script attribue des autorisations pour les boîtes aux lettres traitées pour l'utilisateur au nom duquel le script va être exécuté. Il faut lancer le script dans ce mode avant de commencer et chaque fois que de nouvelles boîtes aux lettres sont ajoutées au fichier de configuration.

Les boîtes aux lettres dont les autorisations ont déjà été définies sont accompagnées d'un attribut spécial dans le fichier de configuration et ces boîtes aux lettres ne sont pas traitées par le script lors de la prochaine exécution de celui-ci dans ce mode.

Vous pouvez remettre les autorisations octroyées par le script à leur valeur d'origine manuellement.

*Pour ce faire, procédez comme suit :*

1. Ouvrez la boîte aux lettres de l'utilisateur dans MS Office Outlook.
2. Ouvrez le menu contextuel du dossier **Courrier indésirable**.
3. Choisissez l'option **Propriétés**.
4. Sous l'onglet **Autorisation** de la boîte de dialogue des propriétés du dossier **Courrier indésirable**, supprimez l'enregistrement lié au compte utilisateur sous le nom duquel le script est exécuté.
5. Cliquez sur **OK**.
6. Ouvrez le fichier de configuration du script (cf section "Configuration des paramètres du fichier de configuration du script" à la page. 124).
7. Dans le groupe <users>, supprimer l'enregistrement qui concerne la boîte aux lettres de l'utilisateur.

Si vous avez l'intention de poursuivre le traitement des messages non sollicités pour cette boîte aux lettres, il suffit de retirer l'attribut rightsAssigned de l'enregistrement dans le fichier de configuration. Cette opération suspend le traitement de la boîte aux lettres jusqu'à la prochaine exécution du script en mode de définition des autorisations ou jusqu'à ce que l'attribut rightsAssigned retrouve sa forme d'origine.

En mode de définition des autorisations, le script est exécuté dans Exchange Management Shell au nom de l'utilisateur autorisé à modifier les autorisations dans les boîtes aux lettres des utilisateurs.

Le fonctionnement du script requiert PowerShell version 2.0 et suivantes.

### Mode de fonctionnement normal du script

Dans ce mode, le script sélectionne les messages non sollicités dans le dossier **Courrier indésirable** des boîtes aux lettres des utilisateurs repris dans le groupe <users> du fichier de configuration et qui possèdent les autorisations correspondantes.

Les critères de sélection suivants sont appliqués :

- le message n'est pas un rapport de remise impossible du message (NDR) ;
- l'âge du message n'est pas antérieur au nombre de jours indiqué dans le paramètre <oldMessages> du fichier de configuration ;
- le champ "Objet" ne contient aucune des notes reprises dans le groupe <subjectMarks> du fichier de configuration.

Les messages non sollicités qui répondent aux critères sont ajoutés en tant que pièce jointe à un message sans que la structure interne du message sollicité ne soit modifiée et ce message est envoyé à l'adresse de messagerie définie par le paramètre <recipientEmail> du fichier de configuration. Ensuite, une note qui a l'attribut default dans le fichier de configuration est ajoutée au champ "Objet" du message.

Cette procédure est suivie pour toutes les boîtes aux lettres définies dans le groupe <users> du fichier de configuration.

Pour garantir le fonctionnement permanent du script, vous devez créer via votre système d'exploitation une tâche programmée.

# PARAMETRES DE LANCEMENT DU SCRIPT

Quel que soit le mode d'exécution du script, il doit s'exécuter avec le paramètre -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab. Ce paramètre permet au script de passer en mode actif. Si le script est lancé sans ce paramètre, il ne s'exécute pas et un texte avertissant qu'une exception s'est produite apparaît dans la console PowerShell.

Vous pouvez utiliser les paramètres d'entrée suivants pour le lancement du script :

- workFolder ; chemin d'accès au dossier contenant le script. Par défaut, il s'agit du dossier actif. Ce paramètre permet de lancer le script selon son mode de fonctionnement normal.

**Exemple d'exécution du script en mode normal** :

.\spamForwarder.ps1 –workFolder c:\temp\spamForwarder -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab

- grantPermissions : paramètre qui permet de lancer le script dans le mode de désignation d'autorisations.

**Exemple d'exécution du script en mode de définition des autorisations** :

.\spamForwarder.ps1 –grantPermissions -IWantToForwardEmailFromJunkEmailFolderToKasperskyLab

# CONFIGURATION DES PARAMETRES DU FICHIER DE CONFIGURATION DU SCRIPT

Le fichier de configuration config.xml du script permet de configurer les paramètres de fonctionnement du script. Il possède la structure suivante :

```
<config>
    <senderEmail>administrator@company.com</senderEmail>
    <recipientEmail>Probable_KSEspam@spam.kaspersky.com</recipientEmail>
    <exchangeVersion>Exchange2007_SP1</exchangeVersion>
    <envelopeSubject>Example of SPAM Message</envelopeSubject>
    <envelopeBody>This message contains SPAM sample in attachment</envelopeBody>
    <logSize>10</logSize>
    <oldMessages>3</oldMessages>
    <ews>https://kseserver.company.com/EWS/Exchange.asmx</ews>
    <users>
        <user rightsAssigned="True">user@company.com</user>
        <user>user1@company.com</user>
        <user>user2@company.com</user>
        </users>
    <subjectMarks>
        <mark>[KL SPAM]</mark>
        <mark default="True">[!! SPAM]</mark>
        <mark>[!!SPAM]</mark>
        <mark>[!!Spam]</mark>
        <mark>[!!Probable Spam]</mark>
        <mark>[!!Blacklisted]</mark>
    </subjectMarks>
</config>
```

Vous pouvez configurer les paramètres suivants du fichier de configuration.

- senderEmail – adresse e-mail de laquelle sont envoyés les messages contenant les modèles de courrier indésirable qui seront examinés par Kaspersky Lab ;

  Le compte utilisateur à partir duquel le script est exécuté doit pouvoir accéder en lecture et en écriture aux boîtes aux lettres d'où sont envoyés les messages destinés à Kaspersky Lab.

- recipientEmail : adresse de messagerie du destinataire des exemples de messages non sollicités. Par défaut, Probable_KSEspam@spam.kaspersky.com;

- exchangeVersion : paramètre qui désigne la version de MS Exchange pour l'initialisation d'EWS API. Ce paramètre peut prendre une des valeurs suivantes (sélectionnez celle qui vous convient le mieux) :

  - Exchange2007_SP1 ;
  - Exchange2010 ;
  - Exchange2010_SP1 ;

  - Exchange2013.

- envelopeSubject : objet du message dans lequel sont placés les exemples de messages non sollicités qui vont être envoyés. Il est déconseillé de modifier cette valeur.

- envelopeBody : corps du message dans lequel sont placés les exemples de messages non sollicités qui vont être envoyés. Il est déconseillé de modifier cette valeur.

- logSize : taille maximale du fichier journal (en mégaoctets). La rotation a lieu dès que le fichier atteint cette taille. Vous pouvez saisir n'importe quelle valeur.

- oldMessages : ancienneté des messages (en jours) que le script sélectionne pour l'envoi. La valeur par défaut est de 3 jours. Il est déconseillé de modifier cette valeur.

- ews : adresse du service EWS. Si ce paramètre figure dans le fichier de configuration, le script n'utilise pas la fonction de définition automatique du serveur CA. Il est déconseillé d'utiliser ce paramètre.

- users : groupe contenant les adresses de messagerie des utilisateurs dont les boîtes aux lettres sont traitées par le script. Ce groupe peut contenir un nombre indéterminé d'enregistrements de différentes boîtes aux lettres.

- user : enregistrement contenant l'adresse de messagerie de la boîte aux lettres soumise au traitement par le script. L'attribut rightsAssigned est proposé automatiquement à l'étape de l'ajout des autorisations. Il est déconseillé de modifier cette valeur, sauf lorsqu'il faut à nouveau définir les autorisations pour la boîte aux lettres de l'utilisateur. Les enregistrements pour lesquels cet attribut n'est pas défini ne sont pas repris dans le processus de traitement des boîtes aux lettres par le script.

- subjectMarks : groupe reprenant les notes qui peuvent être ajoutées par le système de protection contre le courrier indésirable à l'objet du message. Ce groupe peut contenir un nombre indéterminé d'enregistrement, mais le nombre de notes peut avoir une influence sur la vitesse de la recherche des messages dans les boîtes aux lettres des utilisateurs.

- mark : enregistrement contenant un enregistrement distinct sur la note. L'attribut default désigne l'enregistrement utilisé par le script pour marquer les messages envoyés pour l'analyse. Il est déconseillé de donner l'attribut default à plusieurs notes car cela nuirait au fonctionnement du script.

# JOURNAL DE FONCTIONNEMENT DU SCRIPT

Les résultats du fonctionnement du script sont consignés dans un journal enregistré dans le sous-dossier log du dossier du script.

La taille du journal est évaluée à chaque lancement du script. Si la taille du journal est supérieure à la valeur définie par <logSize> dans le fichier de configuration, le journal est archivé à l'aide de GZIP. Cette étape vérifie également s'il existe des archives du journal de plus de deux mois. Ces archives sont supprimées.

# GLOSSAIRE

## A

### ANALYSE DES BANQUES

Analyse antivirus des messages stockés sur le serveur de messagerie et du contenu des dossiers à l'aide des versions les plus récentes des bases. L'analyse a lieu en arrière-plan et peut être lancée manuellement ou selon une programmation définie. Tous les dossiers partagés et les banques de messagerie sont analysés. De nouveaux virus, dont la définition n'était pas reprise dans les bases utilisées pour les analyses antérieures, peuvent être ainsi découverts.

## B

### BASES 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 permettent de détecter le code malveillant dans les objets analysés. Les bases sont composées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

## C

### CLÉ ACTIVE

Clé utilisée actuellement par l'application.

### CLÉ COMPLÉMENTAIRE

Clé qui confirme le droit d'utilisation de l'application, mais qui n'est pas utilisée actuellement.

### CONSOLE D'ADMINISTRATION

Composant de l'application Kaspersky Security. Constitue l'interface utilisateur pour les services d'administration de l'application et permet de configurer et de gérer le serveur en partie. Le module de gestion se présente sous la forme d'une extension à la Microsoft Management Console (MMC).

### COURRIER INDÉSIRABLE

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

### COURRIER POTENTIELLEMENT INDÉSIRABLE

Message qui ne peut être considéré comme courrier indésirable de manière certaine mais qui possède certaines caractéristiques du courrier indésirable (par exemple, certains types d'envois et de messages publicitaires).

## D

### DNS BLACK LIST (DNSBL)

Serveurs contenant en libre accès des listes d'adresses IP utilisées dans la diffusion de courrier indésirable.

### DURÉE DE VALIDITÉ DE LA LICENCE

La durée de validité de la licence est la période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires. Le volume des fonctions et des services complémentaires disponibles dépend du type de licence.

## E

### ENFORCED ANTI-SPAM UPDATES SERVICE

Service de mises à jour rapide des bases de l'Anti-Spam qui permet d'accélérer la réaction du module face aux nouvelles diffusions. Enforced Anti-Spam Updates Service requiert une connexion à Internet permanent.

## K

### KASPERSKY SECURITY NETWORK (KSN)

Infrastructure de services en ligne qui donne accès à la base de données de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et des applications L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

## L

### LIENS MALVEILLANTS

URL renvoyant vers des ressources malveillantes, c'est-à-dire des sites destinés à diffuser des logiciels malveillants.

### LISTE NOIRE DES CLÉS

Base de données contenant des informations relatives aux clés Kaspersky Lab bloquées. Le contenu du fichier de la liste noire est mis à jour en même temps que les bases.

## M

### MASQUE DE FICHIER

Représentation du nom d'un fichier par des caractères génériques. Les caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de n'importe quel caractère et ? représente un caractère unique).

### MISE À JOUR DES BASES

Fonction de l'application de Kaspersky Lab qui permet de maintenir la protection de l'ordinateur à jour. Pendant la mise à jour, l'application copie la mise à jour des bases et des modules de l'application depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et les installe et les applique automatiquement.

## N

### NOTIFICATION FORMELLE

Message automatique diffusé par les clients de messagerie ou des robots (par exemple, message sur l'impossibilité de remettre un message ou confirmation de l'inscription de l'utilisateur sur un site Internet quelconque).

## O

### OBJET CONTENEUR

Objet contenant plusieurs objets, par exemple, une archive un message avec un message joint. Cf. également « objet simple ».

### OBJET INFECTÉ

Objet dont un segment de code correspond parfaitement à un segment de code d'un programme dangereux connu. Les experts de Kaspersky Lab déconseillent de manipuler de tels objets.

### OBJET POTENTIELLEMENT INFECTÉS

Objet dont le code contient un extrait modifié de code d'un programme dangereux connu ou un objet dont le comportement évoque un tel programme.

### OBJET SIMPLE

Corps du message ou pièce jointe simple, par exemple un fichier exécutable. Voir également Objet-conteneur.

## P

### PHISHING

Type d'escroquerie sur Internet qui consiste à envoyer aux victimes potentielles des messages électroniques, prétendument envoyés en général par une banque, dans le but d'obtenir des informations confidentielles.

### PROFIL

Sélection de paramètres appliqués simultanément à plusieurs Serveurs de sécurité.

## R

### RÉPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Certains objets infectés ne peuvent pas être réparés.

## S

### SAUVEGARDE

Banque spéciale prévue pour la conservation des copies de sauvegarde des objets avant la réparation, la suppression ou le remplacement. Il s'agit d'un dossier de service et il est créé dans le dossier de conservation des données de l'application lors de l'installation du serveur de sécurité.

### SERVEUR DE SÉCURITÉ

Composant serveur de Kaspersky Security. Réalise l'analyse antivirus et antispam du trafic de messagerie, met à jour les bases, maintient son intégrité, conserve les données statistiques et offre des services administratifs pour l'administration à distance et la configuration. Le composant contient un ou plusieurs intercepteurs.

### SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoi une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peuvent être modifiées par le serveur proxy à des fins déterminées.

### SERVEURS DE MISE À JOUR DE KASPERSKY LAB

Serveurs HTTP ou FTP de Kaspersky Lab sur lesquelles les applications de Kaspersky Lab récupèrent les mises à jour des bases et des modules de l'application.

### SPAM URI REALTIME BLOCK LISTS (SURBL)

Les listes accessibles à tous des liens qui mènent vers les ressources, publiées par les expéditeurs du courrier indésirable.

### SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique qui se caractérise par la suppression physique du message. Cette méthode est recommandée lorsqu'il ne fait aucun doute que le message est indésirable ou qu'il contient un objet

malveillant. Une copie du message est conservée dans le dossier de sauvegarde avant la suppression (pour autant que cette fonctionnalité ne soit pas désactivée).

### SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet qui implique sa suppression définitive de l'emplacement où il a été détecté par l'application. Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

## V

### VIRUS

Le programme qui infecte d'autres programmes : y ajoute son propre code pour obtenir l'administration lors du lancement des fichiers infectés. Cette définition simple permet de révéler l'action principale exécutée par le virus - l'infection.

### VIRUS INCONNU

Nouveau virus au sujet duquel aucune information ne figure dans les bases. En général, l'application détecte les virus inconnus dans les objets à l'aide de l'analyse heuristique. Ces objets obtiennent l'état potentiellement infecté.

## Z

### ZETA SHIELD

Technologie de détection des vulnérabilités et des logiciels malveillants contre lesquels aucun mécanisme de défense n'existe pour l'instant. La technologie ZETA Shield permet de détecter efficacement les attaques ciblées sur le réseau local d'une entreprise et est utilisée en complément des bases antivirus.

## É

### ÉVALUATION PCL

Le Phishing Confidence Level est une note particulière utilisée par les serveurs de messagerie Microsoft Exchange pour déterminer la probabilité qu'un message contienne des éléments de phishing. Sa valeur peut être comprise entre 0 et 8. Le serveur de messagerie considère qu'un message dont l'évaluation CPL est égale ou inférieure à 3 ne contient pas d'éléments de phishing. Les messages ayant obtenu une note de 4 ou plus sont considérés comme contenant des éléments de phishing. La valeur de l'évaluation PCL d'un message peut être modifiée par Kaspersky Security en fonction des résultats de l'analyse.

### ÉVALUATION SCL

Le Spam Confidence Level est une note particulière utilisée par les serveurs de messagerie Microsoft Exchange pour déterminer la probabilité qu'un message soit un courrier indésirable. La valeur de l'évaluation SCL peut être comprise entre 0 (faible probabilité de courrier indésirable) et 9 (le message est très probablement un courrier indésirable). La valeur de l'évaluation SCL d'un message peut être modifiée par Kaspersky Security en fonction des résultats de l'analyse.

# KASPERSKY LAB ZAO

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 logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'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 antivirus 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 (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

**Réalisations**. 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.fr |
| Encyclopédie des virus | http://www.securelist.com/fr/ |
| Laboratoire d'étude des virus : | newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive) |
| | http://support.kaspersky.com/fr/virlab/helpdesk.html?LANG=fr |
| | (pour les questions aux experts antivirus) |
| Forum Internet de Kaspersky Lab : | http://forum.kaspersky.com |

# INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

# AVIS SUR LES MARQUES

Les marques déposées et les marques de service appartiennent à leurs détenteurs respectifs.

Active Directory, Microsoft, SQL Server, Window, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

Intel et Pentium sont des marques d'Intel Corporation, déposées aux Etats-Unis et dans d'autres pays.

# INDEX

## A


Actions à exécuter sur les objets....64
Actions à réaliser sur le courrier indésirable....78
Ajout d'un serveur....43
Analyse des messages....73, 76
Analyse en arrière-plan....70
Anti-Phishing....76
Anti-Spam....73
Arborescence de la console....21


## B


Barre d'outils....20
Bases
  mise à jour manuelle....53
Bases
  mise à jour automatique....53
Bases
  mise à jour programmée....53
Bases de données de la Sauvegarde et statistiques....96
Bases de l'application....51, 52


## C


Clé....25
Configuration logicielle....15
Configuration matérielle....15
Console d'administration
  lancement....43
Copie de sauvegarde
  consultation des données de la copie de sauvegarde....91
  purge de la sauvegarde....94


## D


Diagnostic....110
Dossier de sauvegarde
  configuration des paramètres....95


## E


EICAR....114, 116
ETAT DE LA PROTECTION....33
Exclusion
  filtrage de l'activité....66
Exclusion de l'analyse....66
Exclusions....66


## F


Fenêtre principale....20
Fenêtre principale
  Arborescence de la console....20
Fenêtre principale de l'application....20

Fichier de licence ....25
Filtre des appels et SMS ....80

## I

INTERFACE DE L'APPLICATION ....20

## J

Journal des événements ....109
    configuration des paramètres ....110

## K

KASPERSKY ....130
Kaspersky Security Network ....61

## L

Lancement
    Console d'administration ....43
    mise à jour manuelle ....53
Lancement
    composition du rapport ....103
LANCEMENT
    APPLICATION ....32
Le contrat de licence ....24
Licence
    Contrat de licence ....24

## M

Menu contextuel ....23
MISE A JOUR ....51
Mise à jour ....51
    lancement manuel ....53
    planification ....53
    serveur proxy ....56
    source des mises à jour ....54

## N

Notifications ....97

## P

Panneau des résultats ....22
Pièces jointes ....70
Profil ....45
Protection
    activation/désactivation ....61, 77
Protection antivirus ....59
Protection des boîtes aux lettres ....65
Protection des dossiers partagés ....65

## R

Rapports ....100
    création ....101
    enregistrement ....108
    tâches de création ....102
Rapports
    rapports rapides ....101
Rapports

consultation....105

## S

Sauvegarde....89
Sauvegarde
suppression de l'objet....94
Serveur proxy....56
Source des mises à jour....54

## T

Tâche de création du rapport
création....102
Tâche de création du rapport. ....100
Traçages
création d'un fichier de trace....120

## V

Vérification du fonctionnement....116