# Kaspersky Security 8.0 for Microsoft Exchange Servers

## Manuel d'administrateur

VERSION DE L'APPLICATION: 8.0

Chers utilisateurs !

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



Date d'édition du document : le 22/09/2010



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

# TABLE DES MATIERES


PRÉSENTATION DU MANUEL ..... 6
Dans ce document ..... 6
Conventions ..... 7
SOURCES D'INFORMATIONS COMPLEMENTAIRES ..... 9
Sources d'informations pour une recherche indépendante ..... 9
Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne ..... 10
Contacter le groupe de préparation de la documentation ..... 10
KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS ..... 11
Fonctions de base ..... 11
Distribution ..... 12
Services pour les utilisateurs enregistrés ..... 12
Contrat de licence ..... 13
Configurations logicielle et matérielle ..... 13
ARCHITECTURE DE L'APPLICATION ..... 15
Composants de l'application et leurs rôles ..... 15
Architecture du serveur de sécurité ..... 15
SCHEMAS TYPIQUES DE DEPLOIEMENT ..... 17
Rôles de Microsoft Exchange Server et configurations correspondantes de la protection ..... 17
Schéma de déploiement de la protection des serveurs ..... 17
Déploiement de l'application sur un cluster de serveurs ..... 18
INSTALLATION DE L'APPLICATION ..... 19
Préparatifs en vue de l'installation ..... 19
Mise à jour de la version antérieure de l'application. ..... 20
Installation de l'application ..... 20
Etape 1. Installation des composants indispensables ..... 20
Etape 2. Message de bienvenue et contrat de licence ..... 21
Etape 3. Sélection du type d'installation ..... 21
Etape 4. Sélection des composants de l'application ..... 21
Etape 5. Configuration de la connexion à Microsoft SQL Server ..... 22
Etape 6. Copie des fichiers ..... 23
Préparatifs pour l'utilisation. Assistant de configuration de l'application ..... 23
Configuration de la mise à jour ..... 23
Installation d'une licence ..... 23
Configuration des notifications ..... 24
Configuration de la protection du serveur ..... 24
Vérification du fonctionnement de l'application ..... 25
Restauration de l'application ..... 26
Suppression de l'application ..... 27
ADMINISTRATION DES LICENCES DE KASPERSKY SECURITY ..... 28
Obtention d'informations sur les licences installées ..... 29
Installation d'une licence ..... 30
Suppression d'une licence ..... 30
Notification sur l'expiration de la durée de validité de la licence ..... 30

Création de la liste des boîtes aux lettres et des banques protégées....31
INTERFACE DE L'APPLICATION....32
Fenêtre principale....32
Menu contextuel....34
LANCEMENT ET ARRET DE L'APPLICATION....35
ÉTAT DE LA PROTECTION PAR DÉFAUT DE MICROSOFT EXCHANGE SERVER....37
PREMIÈRE UTILISATION....38
Lancement de la console d'administration....38
Création de la liste des serveurs Microsoft Exchange protégés....38
Connexion de la console d'administration au serveur de sécurité....40
MISE À JOUR RÉGULIÈRE DES BASES DE L'ANTIVIRUS ET DE L'ANTI-SPAM....41
Mise à jour manuelle....42
Mise à jour automatique....43
Sélection de la source de la mise à jour....44
Configuration des paramètres de connexion....44
PROTECTION ANTIVIRUS....46
Activation et désactivation de la protection antivirus du serveur....47
Création de règles de traitement des objets....48
Analyse des archives jointes et des conteneurs....49
Création d'exclusions de l'analyse....49
Configuration des paramètres de protection des boîtes aux lettres....50
Analyse en arrière-plan....51
PROTECTION CONTRE LE COURRIER INDÉSIRABLE....52
Configuration des paramètres de recherche de courrier indésirable....54
Création des listes noire et blanche d'expéditeurs....55
Configuration avancée de l'Anti-Spam....57
Utilisation de services externes de traitement du courrier indésirable....58
Utilisation des fonctionnalités avancées de l'Anti-Spam....59
SAUVEGARDE....61
Consultation du dossier de sauvegarde....62
Consultation des propriétés des objets placés dans la sauvegarde....64
Filtrage de la sauvegarde....65
Restauration d'un objet depuis la sauvegarde....66
Envoi d'un objet pour examen....66
Suppression d'un objet de la sauvegarde....67
Configuration des paramètres de la sauvegarde....67
NOTIFICATIONS....69
Configuration des paramètres de notification....69
Configuration des paramètres d'envoi des notifications....70
RAPPORTS....71
Configuration des paramètres des rapports rapides....71
Configuration des paramètres des rapports de l'Antivirus....72
Configuration des paramètres de l'Anti-Spam....73
Consultation des rapports prêts....73
Envoi des rapports par courrier électronique....76

JOURNAUX DES ÉVÉNEMENTS DE L'APPLICATION ....78
Configuration du niveau de diagnostic ....78
Configuration des paramètres des journaux ....79
QUESTIONS FRÉQUEMMENT POSÉES ....80
CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE ....82
INFORMATIONS SUR LE CODE TIERS ....83
Code d'application ....83
BOOST 1.30.0, 1.36 ....84
BZIP2/LIBBZIP2 1.0.5 ....85
EXPAT 1.2, 2.0.1 ....85
FREEBSD LIBC 2.3-2.6 ....85
GECKO SDK 1.8 ....86
ICU 4.0.1 ....92
INFO-ZIP 5.51 ....92
LIBJPEG 6B ....93
LIBNKFM 2.0.5 ....95
LIBPNG 1.2.29 ....95
LIBSPF2 1.2.9 ....95
LIBUNGIF 3.0 ....95
LIBXDR ....96
LOKI 0.1.3 ....96
LZMA SDK 4.43 ....97
MICROSOFT ENTERPRISE LIBRARY 4.1 ....97
MICROSOFT VISUAL STUDIO 2008 (MSVCP80.DLL, MSVCR80.DLL) ....97
OPENSSL 0.9.8D ....97
PCRE 7.4, 7.7 ....100
RFC1321-BASED (RSA-FREE) MD5 LIBRARY ....101
SPRING.NET 1.2.0 ....101
SQLITE 3.6.18 ....103
WPF TOOLKIT 3.5.40128.1 ....104
ZLIB 1.2, 1.2.3 ....104
Autres informations ....104
GLOSSAIRE ....105
KASPERSKY LAB ZAO ....109
CONTRAT DE LICENCE ....110
INDEX ....116

# PRÉSENTATION DU MANUEL

Les experts de Kaspersky Lab, Ltd (ci-après, Kaspersky Lab) vous souhaitent la bienvenue ! Nous espérons que ce Manuel de l'administrateur vous aidera à comprendre les principaux aspects du fonctionnement de Kaspersky Security 8.0 for Microsoft Exchange Servers (ci-après, KS 8.0 for Exchange Servers ou Kaspersky Security). Ce guide s'adresse aux administrateurs de serveurs de messagerie Exchange Server 2007 et 2010 (ci-après, Microsoft Exchange Server ou serveur Microsoft Exchange) qui ont choisi Kaspersky Security pour la protection de leurs serveurs.

Objectif de ce document :

- Aider l'administrateur de Microsoft Exchange Server à installer les composants de l'application sur le serveur, à activer la protection du serveur et à trouver la configuration optimale en fonction des tâches en cours ;
- Offrir un accès rapide aux réponses aux questions liées à l'installation et à l'utilisation de l'application ;
- Présenter les autres sources d'informations sur l'application et les méthodes pour obtenir une assistance technique.

### DANS CETTE SECTION DE L'AIDE

Dans ce document ..... 6

Conventions ..... 7

# DANS CE DOCUMENT

Le manuel de l'administrateur de Kaspersky Security 8.0 for Microsoft Exchange Servers contient les chapitres suivants :

- Présentation du manuel. Le chapitre décrit la structure du manuel de l'administrateur.
- Sources d'informations complémentaires (cf. page 9). Le chapitre décrit les différentes sources d'informations sur l'achat, l'installation ou l'utilisation de Kaspersky Security.
- Kaspersky Security 8.0 for Microsoft Exchange Servers (cf. page 11). Le chapitre décrit les principales fonctionnalités de l'application.
- Architecture de l'application (cf. page 15). Le chapitre décrit les composants de l'application et les modes d'interaction.
- Schémas typiques de déploiement (cf. page 17). Le chapitre décrit les rôles de Microsoft Exchange Server et les schémas de déploiement de la protection des serveurs.
- Installation de l'application (cf. page 19). Le chapitre décrit en détails la procédure d'installation de Kaspersky Security.
- Administration des licences (cf. rubrique " Administration des licences de Kaspersky Security " à la page 28). Le chapitre décrit les types de licence ainsi que la procédure d'installation et de suppression des licences.
- Interface de l'application (cf. page 32). Le chapitre décrit l'interface utilisateur de Kaspersky Security.
- Lancement et arrêt de l'application (cf. page 35). Le chapitre fournit des informations sur l'exécution et l'arrêt de l'application.
- État par défaut de la protection de Microsoft Exchange Server (cf. page 37). Le chapitre présente les particularités du fonctionnement de Kaspersky Security selon les paramètres par défaut.

- Première utilisation (cf. page 38). Le chapitre contient des informations sur l'utilisation de Kaspersky Security, l'activation de la protection du serveur de messagerie et la création des listes de serveurs à protéger.
- Mise à jour des bases de l'Antivirus et de l'Anti-Spam (cf. page 41). Le chapitre explique la configuration des paramètres de la mise à jour des bases de Kaspersky Security.
- Protection antivirus (cf. page 46). Le chapitre est consacré à la configuration de la protection antivirus du serveur de messagerie.
- Protection contre le courrier indésirable (cf. page 52). Le chapitre présente les possibilités de l'application en matière de protection du serveur de messagerie contre le courrier indésirable.
- Sauvegarde (cf. page 61). Le chapitre décrit la fonctionnalité de sauvegarde, les modes de restauration des objets depuis la sauvegarde et la configuration de la sauvegarde.
- Notifications (cf. page. 69). Le chapitre crit les modes de réception de notifications sur les événements de Kaspersky Security.
- Rapports (cf. page 71). Le chapitre présente des informations sur la création et la consultation des rapports dans l'application et la réception de ceux-ci par courrier électronique.
- Journaux des événements (cf. rubrique " Journaux des événements de l'application " à la page 78). Le chapitre décrit la configuration des paramètres des rapports sur le fonctionnement de l'Antivirus et de l'Anti-Spam ainsi que sur d'autres événements de Kaspersky Security.
- Questions fréquemment posées (cf. page 80). Le chapitre propose les réponses aux questions les plus fréquentes des utilisateurs.
- Contacter le service d'assistance technique (cf. page 82). Le chapitre décrit les différentes manières d'obtenir une assistance technique pour l'application.
- Glossaire. Le chapitre présente une brève définition de termes utilisés dans l'application.
- Kaspersky Lab, Ltd (cf. page 109). Le chapitre présente brièvement la société.
- Informations relatives au code tiers (cf. page 83). Le chapitre contient des informations relatives au code logiciel d'éditeurs tiers utilisé dans le développement de cette application.

# CONVENTIONS

Les conventions décrites dans le tableau ci-dessous sont utilisées dans le guide.

*Tableau 1. Conventions*

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| N'oubliez pas que... | Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur. |
| Il est conseillé d'utiliser... | Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance. |
| **Exemple :**<br>... | Les exemples sont présentés sur un fond jaune sous le titre " Exemple ". |

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| La *mise à jour*, c'est ... | Les nouveaux termes sont en italique. |
| **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. |
| **Activer** | Les noms des éléments de l'interface sont en caractères mi-gras : les champs de saisie, les commandes du menu, les boutons. |
| ➧ *Pour planifier une tâche, procédez comme suit :* | Les phrases d'introduction sont en italique. |
| `help` | Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux. |
| <adresse IP de votre ordinateur> | Les variables sont écrites entre chevrons. La valeur correspondant à la variable doit être remplacée par cette variable à chaque fois. Par ailleurs, les chevrons sont omis. |

# SOURCES D'INFORMATIONS COMPLEMENTAIRES

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Security, vous pouvez obtenir la réponse rapidement.

Kaspersky Lab offre diverses sources d'informations sur l'application. Vous pouvez choisir celle 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 ..... 9

Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne ..... 10

Contacter le groupe de préparation de la documentation ..... 10


# SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDÉPENDANTE

Vous pouvez consulter les sources suivantes pour obtenir des informations sur l'application :

- Page de l'application sur le site de Kaspersky Lab ;
- Page de l'application sur le site du Service d'assistance technique (dans la banque de solutions) ;
- Système d'aide électronique ;
- Documentation.

### Page sur le site de Kaspersky Lab

http://www.kaspersky.fr/business_products

Cette page vous propose des informations générales sur Kaspersky Security, ses possibilité et ses particularités.

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

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

Cette page regroupe des articles publiés par les experts du Service d'assistance technique.

Ces articles contiennent des renseignements utiles, des recommandations et des réponses aux questions fréquemment posées sur l'utilisation de Kaspersky Security.

### Système d'aide électronique

L'aide électronique contient des informations sur la manière de configurer les composants de l'application ainsi que des indications et des recommandations sur l'administration de l'application.

Si vous souhaitez consulter l'aide électronique, sélectionnez l'option **Aide** dans le menu **Actions** de la console d'administration.

Si vous avez une question relative à une boîte de dialogue ou à un onglet en particulier dans Kaspersky Security, vous pouvez consulter l'aide contextuelle.

Pour ouvrir l'aide contextuelle, ouvrez la boîte de dialogue ou l'onglet qui vous intéresse, puis appuyez sur la touche **F1**.

### Documentation

Le manuel de l'administrateur de Kaspersky Security contient toutes les informations requises pour l'utilisation de l'application et il fait partie de la distribution.

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

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 y consulter les discussions antérieures, publier des commentaires, créer une nouvelle discussion ou lancer une recherche.

# CONTACTER LE GROUPE DE PRÉPARATION DE LA DOCUMENTATION

Si vous avez des questions sur la documentation, si vous avez découvert des erreurs ou si vous souhaitez envoyer des commentaires sur nos guides, vous pouvez contacter le groupe de rédaction de la documentation technique.

Le lien **Envoyer un commentaire** situé dans le coin supérieur droit de la fenêtre d'aide ouvrira une fenêtre du client de messagerie électronique utilisé par défaut sur votre ordinateur. Le message vide reprendra l'adresse du groupe de rédaction (docfeedback@kaspersky.com) tandis que le texte " Kaspersky Help Feedback: Kaspersky Security " apparaîtra dans l'objet du message. Laissez l'objet tel quel et écrivez votre commentaire, puis envoyez le message.

# 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.

Les programmes malveillants peuvent provoquer de sérieux dégâts : ils sont créés spécialement pour voler des informations, les bloquer, les modifier ou les détruire et pour perturber le fonctionnement des ordinateurs et des réseaux informatiques. Lors d'une diffusion massive, un virus peut rapidement se propager dans le réseau d'une entreprise et mettre hors service non seulement les serveurs opérationnels, mais également les ordinateurs des employés, ce qui entraîne des temps morts et des pertes. De plus, les attaques de virus entraînent des pertes de données, ce qui peut avoir un impact négatif sur votre activité commerciale et sur celle de vos partenaires.

Kaspersky Security offre une protection contre le courrier indésirable au niveau du serveur de messagerie de l'organisation, ce qui ôte aux employés la nécessité de supprimer manuellement le courrier indésirable.

### DANS CETTE SECTION DE L'AIDE


Fonctions de base ..... 11

Distribution ..... 12

Services pour les utilisateurs enregistrés ..... 12

Contrat de licence ..... 13

Configurations logicielle et matérielle ..... 13


## FONCTIONS DE BASE

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

Kaspersky Security permet de réaliser les opérations suivantes :

- Analyser le courrier entrant et sortant ainsi que les messages stockés sur Microsoft Exchange Server (y compris dans les dossiers partagés) 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 courrier. Le composant spécial Anti-Spam analyse le trafic 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.

- Créer dans la sauvegarde des copies de sauvegarde des objets (pièce jointe 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.

- 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 trafic et notamment, définir le délai de connexion 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 mise 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 sera exécutée en arrière-plan et aura une incidence négligeable sur les performances du serveur de messagerie.

- Administrer la protection antivirus au niveau des banques et composer des listes des banques protégées.

- Administrer les licences. Chaque licence est octroyée pour un nombre défini de boîte aux lettres et non pas pour un nombre de comptes.

# DISTRIBUTION

Vous pouvez acheter Kaspersky Security chez nos partenaires ou en ligne (par exemple, http://www.kaspersky.fr, rubrique Boutique en ligne). Kaspersky Security fait partie de Kaspersky Security pour serveurs de messagerie (http://www.kaspersky.fr/kaspersky_security_mail_server), et de Kaspersky Open Space Security (http://www.kaspersky.fr/open_space_security) dans Kaspersky Enterprise Space Security et Kaspersky Total Space Security. Dès que vous aurez acheté la licence pour Kaspersky Security, vous recevrez un courrier électronique reprenant un lien pour le téléchargement de l'application depuis le site de la société ainsi que le fichier de licence pour activer la licence ou vous obtiendrez un cédérom avec la distribution de l'application Avant de décacheter l'enveloppe contenant le CD, lisez attentivement le contrat de licence.

# SERVICES POUR LES UTILISATEURS ENREGISTRÉS

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

En obtenant une licence, vous devenez un utilisateur enregistré et vous pouvez bénéficier des services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et accès aux nouvelles versions de ce logiciel ;

- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;

- Notifications de la sortie de nouveaux logiciels de Kaspersky Lab ou de l'émergence de nouveaux virus. Ce service est offert aux utilisateurs qui se sont abonnés au bulletin d'informations de Kaspersky Lab sur le site du service d'Assistance technique(http://support.kaspersky.com/fr/corporatesubscribe/).

Aucune aide n'est octroyée pour les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, de logiciels tiers ou de diverses technologies.

# 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 que vous venez d'acquérir.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les dispositions du contrat de licence, vous pouvez refuser d'utiliser l'application et vous serez remboursé. Dans ce cas, l'enveloppe contenant le CD ne doit en aucun cas avoir été décachetée.

L'ouverture de l'enveloppe cachetée contenant le CD d'installation implique que vous acceptez tous les termes du contrat de licence.

# CONFIGURATIONS LOGICIELLE ET MATÉRIELLE

### Configuration matérielle

La configuration matérielle requise par Kaspersky Security est identique à la configuration matérielle requise par Microsoft Exchange Server. 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 configuration matérielle pour la console d'administration installée en même temps que l'application est la suivante :

- 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 de Kaspersky Security requiert un des systèmes d'exploitation suivants :

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 R2 Enterprise Edition / Microsoft Windows Server 2008 x64 R2 Standard Edition / Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 1 / Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2 / Microsoft Windows Server 2008 x64 Standard Edition Service Pack 1 / Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2 / 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.

Les composants suivants sont obligatoires pour l'installation :

- Microsoft Exchange Server 2007 x64 Service Pack 1 ou Microsoft Exchange Server 2010, déployé dans un des rôles : hub de transport ou boîte aux lettres ;
- MS SQL Server 2005 Express Edition, MS SQL Server 2005 Standard Edition, MS SQL Server 2005 Enterprise Edition, MS SQL Server 2008 Express Edition, MS SQL Server 2008 Standard Edition, MS SQL Server 2008 Enterprise Edition ;
- Microsoft .NET Framework 3.5 Service Pack 1.

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

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 / Microsoft Windows Server 2003 x64 Service Pack 2 / Microsoft Windows Server 2003 x64 R2 Standard Edition /

Microsoft Windows Server 2003 x64 R2 Enterprise Edition / Microsoft Windows XP x64 Service Pack 2 / Microsoft Windows Vista x64 / Microsoft Windows Server 2003 R2 Standard Edition / Microsoft Windows Server 2003 R2 Enterprise Edition / Microsoft Windows Vista / Microsoft Windows Server 2003 Service Pack 2 / Microsoft Windows XP Service Pack 3 / Windows 7 Enterprise / Windows 7 Ultimate.

Les composants suivants sont obligatoires pour l'installation :

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

# ARCHITECTURE DE L'APPLICATION

Kaspersky Security recherche la présence éventuelle de virus dans tout le courrier entrant et sortant ainsi que dans les messages stockés sur le serveur de messagerie et filtre également le courrier indésirable. Le programme vérifie le corps du message ainsi que les pièces jointes, quel que soit leur format. La recherche des programmes malveillants et du courrier indésirable s'opère selon les enregistrements des bases de Kaspersky Security. Les bases sont actualisées à intervalle régulier par Kaspersky Lab et elles sont diffusées sur les serveurs de mises à jour en ligne.

En outre, l'application utilise un mécanisme d'analyse spécial : l'analyseur heuristique qui permet de découvrir des virus inconnus. La recherche du courrier indésirable est à la charge du composant Anti-Spam qui exploite plusieurs technologies afin d'identifier les messages non sollicités. L'application analyse en temps réel les objets qui arrivent sur le serveur. Les nouveaux messages ne peuvent pas être lus tant qu'ils n'ont pas été analysés. Chaque objet est traité conformément aux actions définies par l'administrateur pour différents types d'objets. Vous pouvez créer des règles de traitement des objets malveillants (cf. rubrique " Création de règles de traitement des objets " à la page 48) et du courrier indésirable (cf. rubrique " Configuration des paramètres d'analyse du courrier indésirable " à la page 54).

Le logiciel peut enregistrer l'objet dans un dossier de sauvegarde spécial avant la modification. Cette copie pourra être restaurée ultérieurement ou envoyée pour examen aux spécialistes de Kaspersky Lab. L'application peut envoyer des notifications sur les événements à l'administrateur de la protection antivirus, au destinataire ou à l'expéditeur du message et elle peut également consigner les informations correspondantes dans les journaux de Kaspersky Security et dans le journal des applications de Microsoft Windows.

### DANS CETTE SECTION DE L'AIDE

Composants de l'application et leurs rôles ..... 15

Architecture du service de sécurité ..... 15

# COMPOSANTS DE L'APPLICATION ET LEURS RÔLES

L'application contient deux composants principaux :

- **Serveur de sécurité**. Il s'installe sur le serveur Microsoft Exchange et il est chargé du filtrage des messages non sollicités dans le trafic de messagerie et de la protection contre les virus. Le serveur de sécurité intercepte les messages qui arrivent sur Microsoft Exchange Server et les soumet à la recherche d'éventuels virus ou messages non sollicités à l'aide des modules intégrés Antivirus et Anti-Spam respectivement. Si le message entrant est infecté par un virus ou s'il s'agit d'un message non sollicité, il peut être enregistré dans la sauvegarde ou supprimé en fonction des paramètres de l'Antivirus ou de l'Anti-Spam.

- La **console d'administration** est un composant enfichable isolé spécial intégré à MMC 3.0. La console d'administration peut être installée sur le serveur Microsoft Exchange ou sur un ordinateur distant pour l'administration à distance de la protection du serveur Microsoft Exchange. La console d'administration permet de composer la liste des serveurs Microsoft Exchange à protéger et d'administrer le serveur de sécurité.

# ARCHITECTURE DU SERVEUR DE SÉCURITÉ

Le côté serveur de l'application, à savoir le serveur de sécurité est composé des principaux sous-systèmes suivants :

- **Intercepteur de courrier**. Il intercepte les objets qui arrivent sur le serveur Microsoft Exchange et les transmet au *sous-système d'analyse antivirus*. Le composant s'intègre aux processus de Microsoft Exchange Server selon la technologie VSAPI 2.6 ou selon la technologie Transport Agents, en fonction du rôle dans lequel Microsoft Exchange Server est déployé.

- **Antivirus** assure la protection des objets contre les virus. Le composant est un moteur antivirus qui fonctionne à l'intérieur du processus **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Il intègre également un

dossier pour les objets temporaires en vue de leur analyse dans la mémoire vive. La banque est le dossier de service Store.

Le dossier Store est créé dans le dossier d'installation de l'application et doit être exclu de l'analyse réalisée par les logiciels antivirus installés dans le réseau de l'entreprise. Dans le cas contraire, l'application risque de ne pas fonctionner correctement.

- **Anti-Spam** filtre le courrier indésirable. Le composant est un moteur antispam qui fonctionne à l'intérieur du processus **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Après qu'un message a été intercepté, il est transmis au moteur de l'Anti-Spam pour le traitement. À l'issue du traitement, le message est soit accepté, soit supprimé en fonction des paramètres définis pour le traitement du courrier indésirable. Les copies des messages supprimés peuvent être conservées dans la Sauvegarde.

- **Module d'administration interne de l'application et de contrôle de l'intégrité**. Ce module, lancé dans un processus séparé, est un service Microsoft Windows. Ce service porte le nom **Kaspersky Security 8.0 for Microsoft Exchange Servers** et il est exécuté indépendamment au passage du premier message, en cas de tentative de connexion de la console d'administration au serveur de sécurité et à la fin de l'Assistant de configuration de l'application. Le service ne dépend pas de l'état de Microsoft Exchange Server (en exécution, à l'arrêt), ce qui permet de configurer l'application même si Microsoft Exchange Server est à l'arrêt.  En mode d'analyse en arrière-plan, l**e** module interne d'administration de l'application reçoit du serveur Microsoft Exchange, conformément aux paramètres, tous les messages situés dans les dossiers partagés 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 composant Antivirus pour traitement. Le traitement des objets en arrière-plan est identique à celui des objets en mode d'analyse du trafic. Pour garantir un fonctionnement adéquat du logiciel, le module d'**administration interne** doit être toujours en exécution. Il n'est pas recommandé d'arrêter le service manuellement.

# SCHEMAS TYPIQUES DE DEPLOIEMENT

L'application Kaspersky Security est installée sur le serveur Microsoft Exchange. La sélection des composants de l'application que vous pouvez installer dépend du rôle dans lequel Microsoft Exchange Server est déployé. Kaspersky Security prévoit également le déploiement sur un cluster de serveurs. Il est conseillé de lire les informations du présent chapitre afin de pouvoir choisir l'option de déploiement la mieux adaptée.

### DANS CETTE SECTION DE L'AIDE


Rôles de Microsoft Exchange Server et configurations correspondantes de la protection ..... 17

Schéma de déploiement de la protection des serveurs ..... 17

Déploiement de l'application sur un cluster de serveurs ..... 18


## RÔLES DE MICROSOFT EXCHANGE SERVER ET CONFIGURATIONS CORRESPONDANTES DE LA PROTECTION

Pour garantir le bon fonctionnement de Kaspersky Security, le serveur Microsoft Exchange protégé doit être déployé dans au moins un des rôles suivants :

- Boîte aux lettres (Mailbox).
- Transport Hub (Hub Transport).
- Transport Edge (Edge Transport).

Si Microsoft Exchange Server est déployé dans le rôle de boîte aux lettres, Kaspersky Security utilise la norme VSAPI 2.6 pour l'union. Dans les autres cas, c'est la technologie des agents de transport qui est utilisée. Dans ce cas, pour le rôle transport Hub, les objets sont d'abord traités par Kaspersky Security, puis par les agents de transport de Microsoft Exchange. Pour le rôle Transport Edge, c'est l'inverse : les objets sont d'abord traités par les agents de transport de Microsoft Exchange, puis par Kaspersky Security.

## SCHÉMA DE DÉPLOIEMENT DE LA PROTECTION DES SERVEURS

La protection des serveurs de messagerie se déploie dans l'ordre suivant :

1. Le composant Serveur de sécurité est installé sur tous les serveurs Microsoft Exchange à protéger du réseau. L'installation doit être réalisée sur chaque serveur individuel à l'aide des fichiers d'installation.
2. Le composant Console d'administration est installé avec le serveur de sécurité. Il offre un accès centralisé à tous les serveurs de sécurité de Kaspersky Security depuis le poste de travail de l'administrateur. Le cas échéant, la console d'administration est installée sur un ordinateur distinct appartenant au réseau de l'entreprise. Toutefois, lorsque plusieurs administrateurs travaillent simultanément, il est possible d'installer la console d'administration sur l'ordinateur de chaque administrateur.
3. La liste des serveurs à administrer (cf. rubrique " Création de la liste des serveurs Microsoft Exchange à protéger " à la page 38) est composée.

4. La console d'administration se connecte au serveur de sécurité (cf. rubrique " Connexion de la console d'administration au serveur de sécurité " à la page 40).

# DÉPLOIEMENT DE L'APPLICATION SUR UN CLUSTER DE SERVEURS

Kaspersky Security prend en charge les clusters suivants :

- Cluster à copie unique (Single Copy Clusters, SCC);
- Réplication continue en cluster (Cluster Continous Replication, CCR).

Lors de l'installation, l'application identifie automatiquement les clusters de serveurs. L'ordre d'installation de l'application sur les noeuds de cluster n'a pas d'importance. La procédure d'installation de Kaspersky Security sur les clusters de serveurs se distingue de l'installation traditionnelle en ceci :

- Avant de terminer l'installation de Kaspersky Security sur tous les noeuds du cluster, il est interdit de déplacer les serveurs de cluster des boîtes aux lettres entre les noeuds.
- Lors de l'installation de Kaspersky Security sur tous les noeuds d'un cluster, il faut utiliser le même dossier d'installation.
- Le compte utilisateur au nom duquel l'installation est réalisée doit disposer des autorisations d'écriture dans la section de configuration d'Active Directory.

Après l'installation sur le cluster de serveurs, presque tous les paramètres de l'application sont conservés dans Active Directory et tous les noeuds du cluster fonctionnent selon ces paramètres. Toutefois, les paramètres en rapport avec le serveur physique sont configurés manuellement pour chaque noeud du cluster. Kaspersky Security définit automatiquement les noeuds de cluster actifs et leur applique la configuration depuis Active Directory. Pour chaque noeud du cluster, les résultats de l'analyse seront affichés uniquement pour les messages transmis par le serveur virtuel Microsoft Exchange sur ce noeud du cluster. Les résultats de l'analyse reprennent :

- le contenu de la sauvegarde ;
- les informations reprises dans les rapports ;
- la sélection d'événements consignés dans les journaux de l'application ;

La procédure de suppression de l'application Kaspersky Security du cluster de serveurs se distingue de la procédure normale en ceci :

- Avant la fin de la suppression, il est interdit de déplacer les serveurs de cluster des boîtes aux lettres (CMS) entre les noeuds.
- Lors de la suppression d'une application depuis un noeud actif du cluster, la ressource de cluster de type Microsoft Exchange Information Store est arrêtée ainsi que toutes les ressources de type Microsoft Exchange Database Instance qui en dépendent. L'état d'origine des ressources de cluster sera restauré après la suppression.

# INSTALLATION DE L'APPLICATION

Kaspersky Security contient deux composants principaux : le serveur de sécurité et la console d'administration. Le serveur de sécurité est toujours installé en même temps que la console d'administration. La console d'administration peut être installée séparément sur un autre ordinateur pour l'administration à distance du serveur de sécurité. Vous avez le choix entre trois modes d'installation en fonction de l'architecture du serveur adoptée par votre entreprise.

- Le serveur de sécurité est installé sur l'ordinateur sur lequel Microsoft Exchange Server est déployé. La console d'administration est installée sur ce même serveur.
- Le serveur de sécurité et la console d'administration sont installés sur l'ordinateur sur lequel Microsoft Exchange Server est déployé. La console d'administration est installée sur n'importe quel ordinateur du réseau de l'entreprise pour l'administration à distance du serveur de sécurité.
- Le serveur de sécurité est installé sur la grappe de serveurs sur laquelle Microsoft Exchange Server est déployé. Dans ce cas, le serveur de sécurité et la console d'administration sont installés ensemble sur chaque nœud de la grappe.

Après l'installation de Kaspersky Security, il convient de redémarrer certains services de Microsoft Exchange Server.

### DANS CETTE SECTION DE L'AIDE


Préparatifs en vue de l'installation ..... 19

Mise à jour de la version antérieure de l'application. ..... 20

Installation de l'application ..... 20

Préparatifs pour l'utilisation. Assistant de configuration de l'application ..... 23

Restauration de l'application ..... 26

Suppression de l'application ..... 27


# PRÉPARATIFS EN VUE DE L'INSTALLATION

L'installation de Kaspersky Security requiert les privilèges d'administrateur de domaine. De plus, il faut une connexion à Internet pour installer les composants obligatoires suivants :

- .Net Framework 3.5 SP1 ;
- Microsoft Management Console 3.0 ;
- Microsoft SQL Server 2005 / 2008 (Standard, Express, Enterprise).

Pour pouvoir créer une base de données sur un serveur SQL, vous devez avoir les autorisations d'accès local au système de l'ordinateur sur lequel Kaspersky Security est installé ainsi que des privilèges d'administrateur sur le serveur SQL. Si le serveur SQL se trouve sur un contrôleur de domaine, vous devez être membre du groupe Administrateurs de la société et/ou Administrateurs du domaine.

# MISE À JOUR DE LA VERSION ANTÉRIEURE DE L'APPLICATION.

Kaspersky Security ne prend pas en charge la mise à jour des versions plus anciennes de l'application. Avant d'installer Kaspersky Security, il faut d'abord supprimer la version plus ancienne de l'application installée. Les données et la configuration des paramètres de la version antérieure ne sont pas conservés.

# INSTALLATION DE L'APPLICATION

Le programme d'installation de Kaspersky Security se présente sous la forme d'un Assistant qui fournit les informations relatives aux actions à exécuter à chaque étape. Les boutons **Précédent** et **Suivant** permettent de naviguer entre les fenêtres (étapes) de l'installation à n'importe quelle étape. Les boutons **Quitter** et **Annuler** permettent de quitter le programme d'installation. Le bouton **Terminer** permet de terminer l'installation. L'installation débute après l'exécution du fichier setup_fr.exe. Examinons en détails les étapes de l'Assistant d'installation.

### DANS CETTE SECTION DE L'AIDE

Etape 1. Installation des composants indispensables ..... 20

Etape 2. Message de bienvenue et contrat de licence ..... 21

Etape 3. Sélection du type d'installation ..... 21

Etape 4. Sélection des composants de l'application ..... 21

Etape 5. Configuration de la connexion à Microsoft SQL Server ..... 22

Etape 6. Copie des fichiers ..... 23

# ETAPE 1. INSTALLATION DES COMPOSANTS INDISPENSABLES

Au cours de cette étape, vous devez confirmer que les composants indispensables suivants sont bien installés sur l'ordinateur.

- .Net Framework 3.5 SP1. Vous pouvez installer le composant en cliquant sur le bouton **Installer .Net Framework 3.5 SP1**. L'ordinateur doit être redémarré après l'installation de .Net Framework 3.5 SP1. La poursuite de l'installation sans le redémarrage de l'ordinateur peut entraîner des échecs pendant l'utilisation de Kaspersky Security.

- Microsoft Windows Installer (MSI) version 4.5. Ce composant est requis pour l'installation de Microsoft SQL Server 2008 Express Edition. Vous pouvez installer le composant en cliquant sur le bouton **Installer Microsoft Windows Installer 4.5**.

- Microsoft SQL Server 2008 Express Edition ou autre server SQL. Pour installer le composant, cliquez sur le bouton **Installer Microsoft SQL Server 2008 Express Edition**. Dans le cadre de l'utilisation de Kaspersky Security, il est conseillé de réinstaller le serveur SQL.

- Microsoft Management Console 3.0 (MMC 3.0). Microsoft Management Console 3.0 (MMC 3.0) fait partie du système d'exploitation Microsoft Windows Server 2003 R2 et ultérieur. Pour installer l'application sur une version plus ancienne de Microsoft Windows Server, il faut réaliser la mise à jour de MMC jusqu'à la version 3.0. Pour ce faire, cliquez sur le bouton **Installer MMC 3.0**.

Pour passer à l'étape suivante de l'installation, cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers**.

De plus, vous pouvez télécharger et installer le guide d'installation en cliquant sur le bouton **Guide d'installation**.

## ETAPE 2. MESSAGE DE BIENVENUE ET CONTRAT DE LICENCE

La fenêtre d'accueil contient des informations sur le début de l'installation de Kaspersky Security sur votre ordinateur. Cliquez sur le bouton **Suivant** pour afficher la fenêtre contenant le texte du contrat de licence.

Le contrat de licence est conclu entre l'utilisateur de l'application et Kaspersky Lab. En cochant la case **J'accepte les dispositions du contrat de licence**, vous indiquez que vous avez lu le contrat de licence et que vous en acceptez les dispositions.

## ETAPE 3. SÉLECTION DU TYPE D'INSTALLATION

La fenêtre de sélection du type d'installation contient deux boutons :

- **Normale**. Si vous cliquez sur ce bouton, l'installation se poursuit avec la sélection standard de composants qui répond aux besoins de la majorité des utilisateurs. Pour la suite, cf. Etape 5.

- **Personnalisée**. Si vous cliquez sur ce bouton, vous pouvez choisir les composants de l'application que vous souhaitez installer. L'installation personnalisée est recommandée pour les utilisateurs expérimentés.

Une fois le type d'installation choisi, l'Assistant d'installation passe à l'étape suivante.

## ETAPE 4. SÉLECTION DES COMPOSANTS DE L'APPLICATION

Si vous avez choisi l'option **Personnalisée** à l'étape suivante, le programme d'installation vous propose de choisir les composants que vous voulez installer. La sélection des composants qui peuvent être installés varie en fonction de la présence de Microsoft Exchange Server sur l'ordinateur et de son rôle. Si Microsoft Exchange Server est déployé simultanément dans un rôle de boîtes aux lettres et de transport Hub, les composants suivants pourront être sélectionnés :

- Console d'administration ;

- Module Anti-Spam de la protection ;

- Antivirus pour le rôle serveur de boîtes aux lettres ;

- Antivirus pour le rôle serveur de transport Hub et transport Edge.

Si Microsoft Exchange Server est déployé uniquement dans un rôle de transport Edge ou de transport Hub, les composants suivants pourront être sélectionnés :

- Console d'administration ;

- Module Anti-Spam de la protection ;

- Antivirus pour le rôle serveur de transport Hub et transport Edge.

Si Microsoft Exchange Server est déployé uniquement dans un rôle de boîte aux lettres, les composants suivants pourront être sélectionnés :

- Console d'administration ;

- Antivirus pour le rôle serveur de boîtes aux lettres.

Dans tous les autres cas, seule la console d'administration pourra être installée.

La partie inférieure de la fenêtre affiche le nom complet du dossier d'installation par défaut. Si vous souhaitez sélectionner un autre dossier, cliquez sur le bouton **Parcourir**. Le nom du dossier de conservation des données apparaît en dessous. Le dossier de conservation des données contient les éléments suivants :

- Bases de l'Antivirus ;
- Bases de l'Anti-Spam ;
- Objets placés en quarantaine.

Si vous pensez que le dossier va prendre plus de place que l'espace disponible sur le disque sélectionné, vous pouvez modifier le chemin d'accès au dossier de conservation en cliquant sur **Parcourir**.

Cliquez sur **Abandon** pour annuler la sélection des composants que vous aviez réalisée et revenir à la sélection par défaut.

Cliquez sur le bouton **Disques** pour ouvrir une boîte de dialogue afin de voir si les disques locaux disposent de l'espace nécessaire pour l'installation des composants sélectionnés.

# ETAPE 5. CONFIGURATION DE LA CONNEXION À MICROSOFT SQL SERVER

Cette étape correspond à la configuration des paramètres de la connexion au serveur SQL. Pour pouvoir créer une base de données sur un serveur SQL, vous devez avoir les autorisations d'accès local au système de l'ordinateur sur lequel Kaspersky Security est installé ainsi que des privilèges d'administrateur sur le serveur SQL. Si le serveur SQL se trouve sur un contrôleur de domaine, vous devez être membre du groupe Administrateurs de la société et/ou Administrateurs du domaine. En cas de connexion à distance au serveur SQL, il convient de confirmer que la prise en charge du protocole TCP/IP est activée dans SQL Server Configuration Manager.

### Configuration de la connexion à Microsoft SQL Server

Dans le champ **Nom du serveur SQL**, indiquez le nom de l'ordinateur (ou l'adresse IP) ou de l'instance du serveur SQL. Si vous cliquez sur le bouton **Parcourir** situé en face du champ, vous pouvez choisir un serveur SQL dans ce segment du réseau.

Pour créer une base de données sur le serveur SQL, il faut sélectionner le compte utilisateur sous lequel la base SQL sera créée. Vous avez le choix entre les options suivantes :

- **Compte utilisateur actuel**. Dans cas, c'est le compte utilisateur actuel qui sera utilisé.
- **Autre compte utilisateur**. Dans ce cas, il faut indiquer le nom et le mot de passe du compte différent du compte actuel. Pour sélectionner le compte, cliquez sur **Parcourir**.

Le service du navigateur du serveur SQL doit être lancé sur l'ordinateur où se trouve le serveur SQL. Dans le cas contraire, vous ne pourrez pas voir l'instance du serveur SQL dont vous avez besoin. Si Kaspersky Security est installé sur un serveur dont le rôle est transport Edge et qu'un serveur SQL se trouve dans le domaine, il sera impossible d'établir la connexion avec le serveur SQL. Dans ce cas, il faut utiliser une instance locale du serveur SQL.

### Sélection du compte utilisateur pour l'utilisation du service.

Dans la fenêtre suivante, vous serez invité à sélectionner le compte utilisateur qui sera utilisé pour la connexion au serveur SQL. La fenêtre propose deux options :

- **Compte utilisateur système (Local System)**. Dans ce cas, la connexion au serveur SQL sera établie sous le compte utilisateur système.
- **Compte utilisateur**. Dans ce cas, saisissez le nom et le mot de passe d'un compte possédant les autorisations suffisantes pour la connexion au serveur SQL et l'exécution du service de l'application.

## ETAPE 6. COPIE DES FICHIERS

Pour poursuivre l'installation, cliquez sur **Installer** dans la fenêtre de l'Assistant d'installation. La procédure de copie des fichiers de l'application sera lancée, ainsi que l'enregistrement des composants dans le système. La base sera créée sur le serveur SQL et certains services de Microsoft Exchange Server seront redémarrés.

# PRÉPARATIFS POUR L'UTILISATION. ASSISTANT DE CONFIGURATION DE L'APPLICATION

Une fois la copie des fichiers et l'enregistrement des composants dans le système terminés, l'Assistant d'installation affiche un message qui indique que l'installation est terminée. Cliquez sur **Suivant** dans l'Assistant d'installation afin d'accéder à l'Assistant de configuration de l'application. L'Assistant de configuration de l'application vous aidera à configurer les paramètres de la mise à jour, à installer la licence, à sélectionner le mode de réception des notifications et à vérifier le fonctionnement de l'application. Pour commencer la configuration à l'aide de l'Assistant de configuration de l'application, cliquez sur **Suivant**.

### DANS CETTE SECTION DE L'AIDE

Configuration de la mise à jour ..... 23

Installation d'une licence ..... 23

Configuration des notifications ..... 24

Configuration de la protection du serveur ..... 24

Vérification du fonctionnement de l'application ..... 25

## CONFIGURATION DE LA MISE À JOUR

Dans la fenêtre **Paramètres de mise à jour** de l'Assistant de configuration de l'application, configurez les paramètres de la mise à jour de Kaspersky Security.

*Pour configurer les paramètres de la mise à jour, procédez comme suit :*

1. Ne décochez pas la case **Activer le mode de mise à jour automatique**, si vous souhaitez **que** la mise à jour de l'application ait lieu selon un horaire défini.
2. Pour réaliser la connexion au serveur de mises à jour de Kaspersky Lab via un serveur proxy, cochez la case **Utiliser le serveur proxy** et saisissez l'adresse du serveur proxy de l'entreprise dans la ligne **Adresse du serveur proxy**.
3. Indiquez le numéro du port du serveur proxy à l'aide du menu déroulant. Le port utilisé par défaut est **8080**.
4. Pour l'authentification sur le serveur Proxy que vous avez indiqué, 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**.
5. Si vous souhaitez que les mises à jour soient téléchargées depuis un serveur local de votre entreprise sans utiliser le serveur proxy, cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.

## INSTALLATION D'UNE LICENCE

La fenêtre **Licences** permet d'installer la licence de Kaspersky Security.

*Pour installer la licence, procédez comme suit :*

1. Cliquez sur le bouton **Ajouter**.

2. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur **Ouvrir**.

   Cette action entraînera l'installation de la licence qui donne droit à l'utilisation de Kaspersky Security pendant la durée indiquée sans restriction sur les fonctionnalités. Durant la période de validité de la licence, vous pouvez télécharger les mises à jour des bases de l'Antivirus et de l'Anti-Spam ou contacter les experts de Kaspersky Lab pour toute question relative à l'utilisation de l'application.

### Suppression d'une licence

Pour supprimer la licence, cliquez sur **Supprimer**.

## CONFIGURATION DES NOTIFICATIONS

La fenêtre **Configuration des notifications** permet de configurer les paramètres des notifications envoyées par courrier électronique. Grâce aux notifications, vous êtes au courant de tous les événements qui se produisent dans Kaspersky Security.

*Pour configurer les paramètres des notifications, procédez comme suit :*

1. Dans le champ **Adresse du service Web**, indiquez l'adresse du service Web d'envoi des messages électroniques via Microsoft Exchange Server.

   Par défaut, dans Microsoft Exchange Server, il s'agit de l'adresse :

   `https://<nom_du_serveur_accès_client>/ews/exchange.asmx`

2. Dans le champ **Compte utilisateur**, indiquez n'importe quel compte parmi les boîtes aux lettres inscrites sur Microsoft Exchange Server.

   Pour ce faire, cliquez sur le bouton **Parcourir** ou saisissez le nom du compte utilisateur manuellement.

3. Saisissez le mot de passe du compte choisi dans le champ **Mot de passe**.

4. Dans le champ **Adresse électronique**, saisissez l'adresse électronique du destinataire des notifications.

5. Cliquez sur le bouton**Test** afin d'envoyer un message d'essai.

   Si le message d'essai arrive dans la boîte aux lettres indiquée, cela signifie que l'envoi des notifications est correctement configuré.

## CONFIGURATION DE LA PROTECTION DU SERVEUR

La **fenêtre Paramètres** de la protection vous permet de configurer les paramètres de protection antivirus et anti-spam. La protection contre le spam et les virus est activée par défaut.

*Pour configurer les paramètres de protection, procédez comme suit :*

1. Ne décochez pas la case **Activer la protection Antivirus** pour lancer la protection antivirus.

2. Ne décochez pas la case **Activer la protection antispam** pour lancer la protection contre le courrier indésirable.

Si vous ne voulez pas que la protection antivirus ou anti-spam commence à fonctionner tout de suite, décochez les cases correspondantes. Vous allez pouvoir activer la protection via la Console d'administration plus tard.

3. Cliquez sur **Suivant** pour terminer la configuration des paramètres de l'application.

4. Cliquez sur le bouton **Terminer** dans la dernière fenêtre de l'Assistant de configuration de l'application afin de quitter l'Assistant.

   Si la case **Lancer la Console d'administration à la fin de l'Assistant de configuration de l'application** est cochée, la console d'administration sera lancée automatiquement.

# VÉRIFICATION DU FONCTIONNEMENT DE L'APPLICATION

Une fois l'installation et la configuration de Kaspersky Security terminée, il est conseillé de vérifier l'exactitude de la configuration des paramètres et le bon fonctionnement de l'application à l'aide d'un virus d'essai et de ses modifications.

Ce virus d'essai a été développé spécialement par l'organisation EICAR (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus. Le virus d'essai n'est pas un programme malveillant et il ne contient pas de code qui pourrait nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

Vous pouvez télécharger le virus d'essai depuis le site officiel de l'organisation EICAR : http://www.eicar.org/anti_virus_test_file.htm.

### Vérification du fonctionnement de l'Antivirus

- *Pour envoyer un message avec le virus d'essai, procédez comme suit :*

  1. Créez un message avec le virus d'essai EICAR en pièce jointe.

  2. Envoyez le message via Microsoft Exchange Server sur lequel Kaspersky Security est installé et auquel le serveur de sécurité est connecté.

  3. Vérifiez que le message remis ne contient pas de virus. En cas de découverte d'un virus sur le rôle Boîte aux lettres, le virus supprimé est remplacé par un fichier texte. En cas de découverte du virus dans le rôle 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 notifications " à la page 24) de l'Assistant de configuration initiale.

- *Pour consulter le rapport relatif au virus découvert dans l'application, procédez comme suit :*

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

  2. Dans l'arborescence de la console située à gauche, sélectionnez le nœud correspondant au serveur via lequel le message avec le virus a été envoyé et déployez-le.

  3. Sélectionnez le nœud **Rapports**.

  4. Dans la fenêtre des résultats à droite, cliquez sur le bouton **Créer un rapport** dans le groupe de paramètres **Rapports rapides** et/ou **Rapport antivirus**.

  5. Dans le groupe de paramètres **Rapports disponibles**, consultez le rapport créé. Pour ce faire, double-cliquez sur le rapport pour l'ouvrir.

     Si le rapport contient les informations relatives à l'infection par le virus EICAR, cela signifie que les paramètres de fonctionnement de l'application ont bien été configurés.

*Pour recevoir le rapport à l'adresse électronique, procédez comme suit :*

1. Dans la fenêtre des résultats, dans le groupe de paramètres **Rapports rapides** et/ou **Rapport antivirus**, cochez la case du paramètre **Administrateur** pour l'envoi des messages à l'adresse saisie dans les paramètres de notification (cf. rubrique " Configuration des notifications " à la page 24) de l'Assistant de configuration de l'application.

   Si vous n'avez pas saisi une adresse électronique dans l'Assistant de configuration de l'application, cliquez sur le lien **Paramètres d'envoi des messages** pour configurer les notifications (cf. rubrique " Configuration des notifications " à la page 24).

2. Pour confirmer que le message arrivera bien à l'adresse saisie, cliquez sur le bouton **Test** afin d'envoyer un message d'essai.

Par défaut, une copie de l'objet infecté est conservée dans la sauvegarde.

*Pour voir si une copie de l'objet infecté a été créée dans la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le **Sauvegarde**.

2. Confirmez que l'objet infecté (message avec virus en pièce jointe) apparaît dans la fenêtre des résultats.

**Vérification du fonctionnement de l'Anti-Spam**

*Pour vérifier que le composant **Anti-Spam** fonctionne correctement, procédez comme suit :*

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

2. Dans l'arborescence de la console située à gauche, sélectionnez le nœud correspondant au serveur via lequel le message d'essai a été envoyé et déployez-le.

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

4. Dans la fenêtre des résultats, choisissez l'onglet **Protection contre le courrier indésirable**.

5. Déployez le groupe **Paramètres des listes blanche et noire**.

6. Cochez la case **Ajouter l'adresse de l'expéditeur à la liste noire**.

7. Saisissez l'adresse de l'expéditeur dans le champ de saisie.

8. Cliquez sur le bouton d'ajout  à droite du champ.

9. Déployez le groupe **Paramètres d'analyse**.

10. Dans le champ **Expéditeur interdit**, choisissez la valeur **Ignorer**.

11. Dans ce même champ, cochez la case **Ajouter un intitulé**.

12. Envoyez le message à l'adresse de l'administrateur via le serveur de messagerie protégé.

    Si le message arrive avec l'intitulé **[Blacklisted]** dans l'en-tête, l'**Anti-Spam** fonctionne correctement.

# RESTAURATION DE L'APPLICATION

En cas d'échec du fonctionnement de l'application (par exemple, les modules binaires sont endommagés), vous pouvez utiliser la fonction de restauration du programme d'installation. Lors de la restauration, le programme d'installation conserve les paramètres sélectionnés, ainsi que la configuration de l'utilisateur, y compris les notifications, le chemin d'accès à la base de la quarantaine, etc.

*Pour restaurer Kaspersky Security, procédez comme suit :*

1. Lancez le fichier setup_fr.exe.
2. Cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers**.
3. Dans la fenêtre d'accueil de l'Assistant d'installation, cliquez sur le bouton **Suivant**.
4. Dans la fenêtre **Modification, restauration ou suppression de l'application**, cliquez sur le bouton **Restaurer**.
5. Dans la fenêtre **Restauration**, cliquez sur le bouton **Réparer**.

Si les fichiers de configuration ont été endommagés, la restauration de l'application n'est pas possible. Il est alors conseillé de supprimer l'application et de l'installer à nouveau.

# SUPPRESSION DE L'APPLICATION

*Pour supprimer Kaspersky Security de l'ordinateur, procédez comme suit :*

1. Lancez le fichier setup_fr.exe.
2. Cliquez sur le lien **Kaspersky Security 8.0 for Microsoft Exchange Servers** pour lancer l'Assistant d'installation, puis cliquez sur **Suivant**.
3. Dans la fenêtre **Modification, restauration ou suppression de l'application**, cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre **Suppression**, cliquez sur le bouton **Supprimer**.

Vous pouvez également supprimer l'application à l'aide des outils standard d'installation et de suppression d'applications de Microsoft Windows.

Lors de la suppression de Kaspersky Security, il faudra redémarrer certains services de Microsoft Exchange Server.

# ADMINISTRATION DES LICENCES DE KASPERSKY SECURITY

Un contrat de licence est conclu entre vous et Kaspersky Lab lorsque vous achetez Kaspersky Security. Ce contrat vous donne le droit d'utiliser l'application pendant une période déterminée afin de protéger un nombre défini de boîtes aux lettres. Les boîtes aux lettres et les dossiers partagés sont soumis à la protection. Il n'est donc pas nécessaire d'obtenir une licence séparée pour la protection des dossiers partagés dans l'environnement Microsoft Exchange Server. En cas d'utilisation de l'application sur un cluster de serveurs, la licence s'applique à tout le cluster.

Les possibilités suivantes vous sont offertes pendant la durée de validité de la licence :

- Utilisation des fonctions antivirus de l'application ;
- Utilisation des fonctions de l'Anti-Spam ;
- Mise à jour régulière des bases de l'Antivirus et de l'Anti-Spam ;
- Réception des nouvelles versions de l'application ;
- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;

L'application détermine l'existence d'un contrat de licence sur la base du fichier de licence qui est une partie incontournable de n'importe quel logiciel de Kaspersky Lab.

Kaspersky Security ne peut fonctionner sans licence !

### Licence active

L'application ne peut avoir qu'une seule licence active. Cette licence contient les limites d'utilisation de Kaspersky Security qui peuvent être vérifiées par des mécanismes spéciaux de l'application. En cas de violation du contrat de licence :

- les fonctionnalités de l'application sont réduites ;
- une note indiquant la violation apparaît dans le journal des événements ;
- si les paramètres de notification ont été configurés, un message électronique signalant la violation est envoyé.

Il est uniquement possible de réglementer le nombre de boîtes aux lettres à protéger en excluant de l'analyse des banques (cf. rubrique " Création de la liste des boîtes aux lettres et des banques protégées " à la page 31) les boîtes aux lettres qui ne seront pas analysées. Il est conseillé d'acheter une licence pour la protection de toutes les boîtes aux lettres car la présence d'une banque non protégée augmente le risque d'infection par un virus et de propagation de celui-ci via le système de messagerie. À l'expiration de la licence commerciale, les fonctionnalités de l'application sont maintenues, à savoir que l'application continue à rechercher la présence éventuelle de virus et de messages non sollicités dans le trafic, mais la récupération des mises à jour des bases et des nouvelles versions de l'application ne sera plus disponible, tout comme la possibilité de contacter le service d'assistance technique. L'application continuera à rechercher la présence éventuelle de virus dans le trafic et à réaliser l'analyse en arrière-plan des banques, mais à l'aide des bases antivirus dépassées. Dans un tel contexte, il est difficile de garantir une protection totale contre les nouveaux virus et le courrier indésirable qui apparaîtraient après la fin de validité de la licence.

Par défaut, 15 jours avant l'expiration de la licence, des notifications apparaissent pendant l'utilisation de l'application. Ces messages reprennent la date d'expiration de la licence installée ainsi que des informations sur la manière de la renouveler. Vous pouvez modifier le délai de réception des notifications (cf. " Message d'alerte relatif à l'expiration de la licence " à la page 30) et saisir l'adresse électronique à laquelle la notification sera envoyée.

### Licence complémentaire

Une fois que vous avez installé la licence commerciale, vous pouvez acheter une licence complémentaire pour l'application (cf. rubrique " Distribution " à la page 12) qui reprend Kaspersky Security et l'installer. Une fois que la licence active expire, la licence complémentaire devient active et l'application continue à fonctionner sans aucune modification. Ainsi, vous pouvez garantir la protection sans interruption des serveurs de messagerie de votre organisation. Kaspersky Security n'accepte qu'une seule licence complémentaire.

### Licence d'évaluation

Vous pouvez utiliser la licence d'évaluation afin d'étudier les avantages offerts par Kaspersky Security. Si vous utilisiez une licence d'évaluation, alors à l'issue de la période de validité de celle-ci, la fonctionnalité de l'application sera suspendue, en plus des restrictions décrites ci-dessus. N'oubliez pas que la durée de validité de la licence d'évaluation commence à partir de l'ajout de la première licence d'évaluation. La durée de validité de toutes les licences d'évaluation suivantes sera adaptée à la durée de validité de la première.

### Restrictions d'utilisation de la licence

Dans certains cas tels que la résiliation du contrat de vente ou la modification des restrictions de la licence, Kaspersky Lab résilie le contrat de licence. Dans ce cas, le numéro de série de la licence est placé dans la liste des licences annulées ; c'est ce qu'on appelle la " liste noire ". S'il s'avère que la licence active figure dans la liste noire, la licence complémentaire ne s'active pas et seuls les services d'administration et de mise à jour des bases seront disponibles parmi toutes les fonctionnalités de l'application. Si votre licence s'est retrouvée par erreur dans la liste noire, il est conseillé de lancer la mise à jour des bases ou de contacter le service d'assistance technique si cette opération ne règle pas le problème.

### DANS CETTE SECTION DE L'AIDE

Obtention d'informations sur les licences installées ..... 29

Installation d'une licence ..... 30

Suppression d'une licence ..... 30

Notification sur l'expiration de la durée de validité de la licence ..... 30

Création de la liste des boîtes aux lettres et des banques protégées ..... 31

# OBTENTION D'INFORMATIONS SUR LES LICENCES INSTALLÉES

*Pour consulter les informations relatives aux licences installées, procédez comme suit :*

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Licences** dans le noeud du serveur qui vous intéresse.

   Dans la fenêtre des résultats, vous pouvez consulter les informations relatives aux licences installées. Les données suivantes sont fournies :

   - **Type**. Décrit le type de clé de licence
   - **Détenteur**. Identifie le détenteur de la licence.
   - **Restrictions**. Détermine le nombre maximum d'utilisateurs autorisé (boîtes aux lettres) par la licence.

- **Date d'expiration**. Affiche la date d'expiration de la licence.
- **Numéro de série**. Affiche le numéro de série de la licence.
- **Etat**. Affiche l'état de la licence active.

# INSTALLATION D'UNE LICENCE

*Pour installer la licence de Kaspersky Security, procédez comme suit :*

1. Dans la console d'administration, choisissez le noeud **Licences**.
2. Dans la fenêtre des résultats, cliquez sur le bouton**Ajouter**.
3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur **Ouvrir**.

Après avoir installé la licence commerciale, vous pouvez installer une licence complémentaire.

*Pour installer la licence complémentaire, procédez comme suit :*

1. Dans la console d'administration, choisissez le noeud **Licence**.
2. Dans la fenêtre des résultats, dans la rubrique **Licence complémentaire**, cliquez sur le bouton **Ajouter**.
3. Dans la fenêtre qui s'ouvre, désignez le fichier de licence dans le champ **Nom du fichier** (fichier avec extension *.key), puis cliquez sur **Ouvrir**.

# SUPPRESSION D'UNE LICENCE

*Pour supprimer la licence de Kaspersky Security, procédez comme suit :*

1. Dans la console d'administration, choisissez le noeud **Licences**.
2. Dans la fenêtre des résultats, dans la rubrique **Licence active** ou **Licence complémentaire**, cliquez sur le bouton **Supprimer**.

# NOTIFICATION SUR L'EXPIRATION DE LA DURÉE DE VALIDITÉ DE LA LICENCE

L'application vérifie les licences après chaque mise à jour des bases. Les résultats de la vérification peuvent être les suivants :

- la licence active arrive à échéance dans quelques jours ;
- la validité de la licence est écoulée ;
- la licence active se trouve dans la liste noire.

Pour tous les cas cités, un enregistrement est ajouté aux journaux de l'application et si les notifications ont été configurées (cf. rubrique " Configuration des notifications " à la page 69), un message est envoyé à l'adresse électronique saisie pendant la configuration. Par défaut, la notification est envoyée 15 jours avant la fin de validité de la licence. Vous pouvez définir un délai plus long ou plus court.

- *Pour configurer les paramètres de notification sur l'expiration de la licence de Kaspersky Security, procédez comme suit :*

  1. Dans la console d'administration, choisissez le noeud **Licences**.

  2. Dans la fenêtre des résultats, pour le champ **Signaler l'expiration de la durée de validité de licence**, définissez, à l'aide du menu déroulant, combien de jours avant l'expiration vous souhaitez recevoir la notification sur l'expiration de la licence.

  3. Cliquez sur le bouton **Enregistrer**.

# CRÉATION DE LA LISTE DES BOÎTES AUX LETTRES ET DES BANQUES PROTÉGÉES

L'application assure la protection du nombre de boîtes aux lettres précisé dans la licence que vous avez acquise. Si le nombre ne suffit pas, vous pouvez sélectionner les boîtes aux lettres à retirer de la protection et transférer les données de la boîte dans les banques qui ne seront pas protégées. Par défaut, tous les dossiers partagés du serveur de messagerie protégé sont soumis à la protection. Vous pouvez désactiver la protection des dossiers partagés si vous estimez que celle-ci n'est pas nécessaire.

- *Pour désactiver la protection des banques des boîtes aux lettres ou des banques des dossiers partagés, procédez comme suit :*

  1. Dans la console d'administration, choisissez le noeud **Protection du serveur**.

  2. Sous l'onglet **Protection antivirus**, ouvrez le groupe de paramètres **Protection des boîtes aux lettres**.

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

  4. Dans la rubrique **Banques de dossiers public à protéger**, cochez les cases des banques des dossiers partagés que vous souhaitez protéger.

  5. Cliquez sur le bouton **Enregistrer** pour que les modifications entrent en vigueur.

Les listes proposées reprennent l'ensemble des banques des boîtes aux lettres et des dossiers partagés du serveur Microsoft Exchange protégé. Par défaut, celles qui existaient déjà au moment de l'installation de l'application et les nouvelles banques sont protégées

# 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 ..... 32

Menu contextuel ..... 34

## FENÊTRE PRINCIPALE

La fenêtre principale de la console d'administration comprend les partie suivantes (cf. ill. ci-après) :

- **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.
- **Menu**. Situé directement au-dessus de la barre d'outils. Le menu remplit les fonctions principales d'administration des fichiers et des fenêtres et offre également l'accès aux fichiers d'aide.
- **Arborescence de la console**. Située dans la partie gauche de la fenêtre principale. L'arborescence de la console permet de voir les serveurs de sécurité connectés ainsi que les paramètres de Kaspersky Security. Les serveurs connectés et les paramètres de Kaspersky Security sont présentés sous la forme de noeuds. Pour déployer un noeud parent, cliquez sur le signe +. Le noeud déployé est accompagné du signe -.
- **Fenêtre des résultats**. Située dans la partie droite de la fenêtre principale. Affiche le contenu du noeud sélectionné dans l'arborescence.

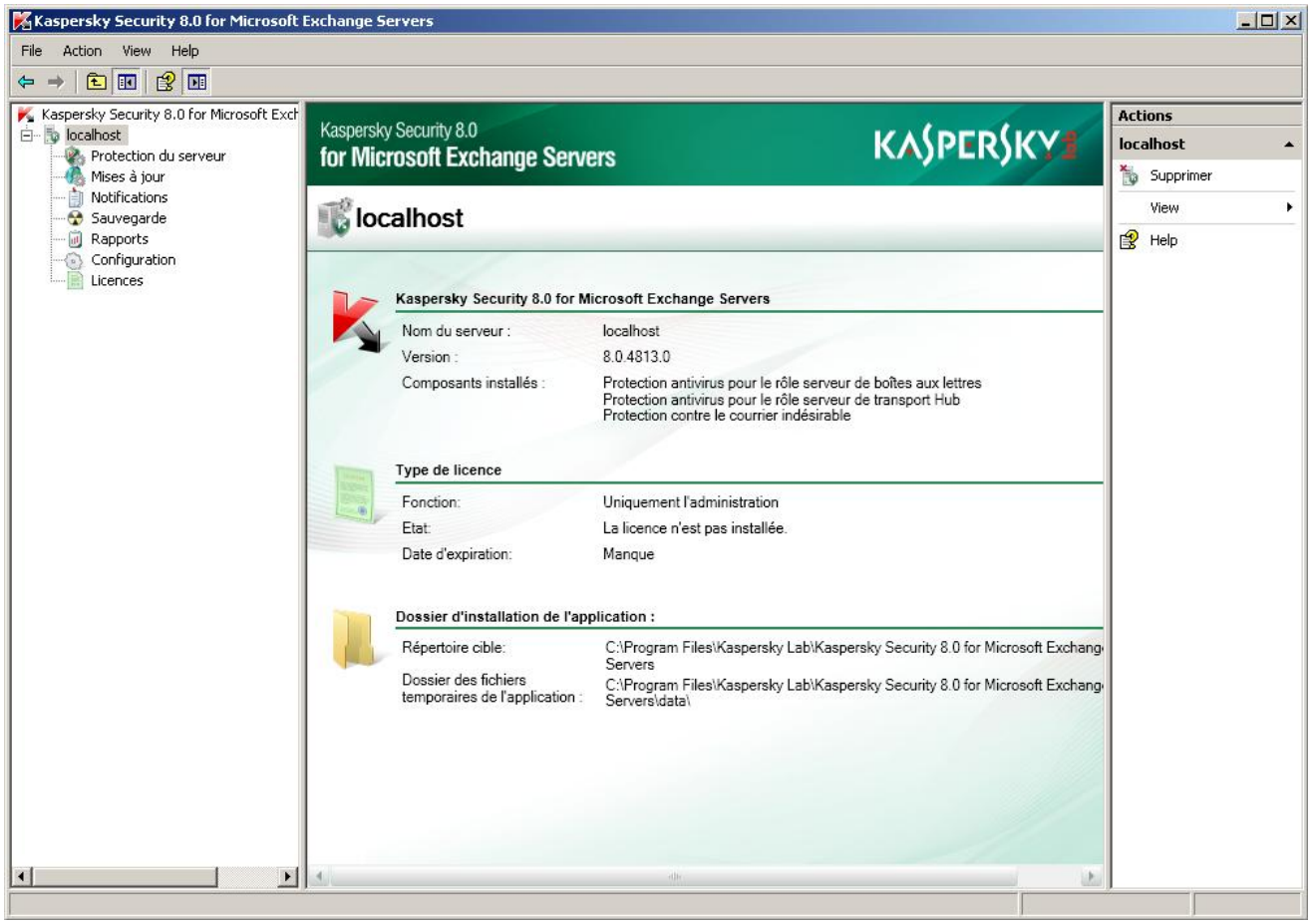


*Illustration 1. Fenêtre principale de l'application*

Le noeud le plus haut dans l'arborescence de la console est **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Si vous double-cliquez sur ce noeud dans l'arborescence de la console, la liste des serveurs connectés et dotés de Kaspersky Security s'affiche. La fenêtre des résultats affiche également les serveurs connectés et le bouton **Ajouter un serveur**. Si vous cliquez avec le bouton droit de la souris sur le noeud du serveur connecté, la fenêtre des résultats affiche des informations générales sur les composants de l'application installés sur le serveur sélectionné, sur le type de licence ou sur le dossier d'installation de l'application. Si vous cliquez sur le signe plus en regard du serveur connecté, la liste des paramètres de Kaspersky Security pour ce serveur apparaît dans l'arborescence de la console. Vous pouvez consulter et configurer les paramètres suivants de Kaspersky Security :

- **Protection du serveur** : consultation et configuration des paramètres de la protection contre les virus et le courrier indésirable.
- **Mises à jour** : consultation et configuration des paramètres de la mise à jour des bases antivirus et des bases de l'Anti-Spam.
- **Notifications** : consultation et configuration des paramètres des notifications par courrier électronique.
- **Sauvegarde** : consultation de la sauvegarde.
- **Rapports** : consultation et configuration des paramètres des rapports sur la protection contre les virus et le courrier indésirable.
- **Configuration** : consultation et configuration des paramètres d'envoi des notifications, de la sauvegarde, des diagnostics, des rapports et des statistiques.
- **Licence** : installation et suppression des licences et consultation des données relatives à la licence en cours.

Pour chaque noeud de l'application sélectionné dans l'arborescence de la console, la fenêtre des résultats affiche les paramètres configurés pour ce noeud.

# MENU CONTEXTUEL

Chaque catégorie d'objet de l'arborescence de la console possède son propre menu contextuel qui s'ouvre d'un clic du bouton droit de la souris. En plus des commandes standard du menu contextuel de MMC, on y retrouve des commandes qui permettent d'exécuter des travaux avec l'objet en question. Le menu contextuel permet de réaliser les opérations suivantes :

- Ajouter un serveur. Dans l'arborescence de la console d'administration, cliquez avec le bouton droit de la souris sur **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Dans le menu contextuel, choisissez l'option **Ajouter un serveur**.

- Activer le diagnostic du composant enfichable. Dans l'arborescence de la console d'administration, cliquez avec le bouton droit de la souris sur **Kaspersky Security 8.0 for Microsoft Exchange Servers**. Dans le menu contextuel, sélectionnez l'option **Activer le diagnostic du composant enfichable**.

- Supprimer le serveur connecté. Dans l'arborescence de la console d'administration, cliquez avec le bouton droit de la souris sur le noeud du serveur connecté. Sélectionnez **Supprimer** dans le menu contextuel.

- Actualiser les bases antivirus et les bases de l'Anti-Spam. Dans l'arborescence de la console d'administration, cliquez avec le bouton droit de la souris sur le noeud **Mettre à jour**. Dans le menu contextuel, sélectionnez l'option **Mettre à jour les bases de l'Antivirus** ou **Mettre à jour les bases de l'Anti-Spam**.

- Configurer les paramètres d'envoi des notifications Dans l'arborescence de la console d'administration, cliquez avec le bouton droit de la souris sur le noeud **Notifications** ou **Rapports**. Dans le menu contextuel, sélectionnez **Paramètres d'envoi des messages**.

# LANCEMENT ET ARRET DE L'APPLICATION

Kaspersky Security est lancé automatiquement au démarrage de Microsoft Exchange Server, au démarrage de Microsoft Windows, lorsqu'un message transite par le serveur Microsoft Exchange et lors de la connexion de la console d'administration au serveur de sécurité. Si la protection antivirus du serveur est activée (cf. ill. ci-après ), elle sera opérationnelle dès le lancement de Microsoft Exchange Server.

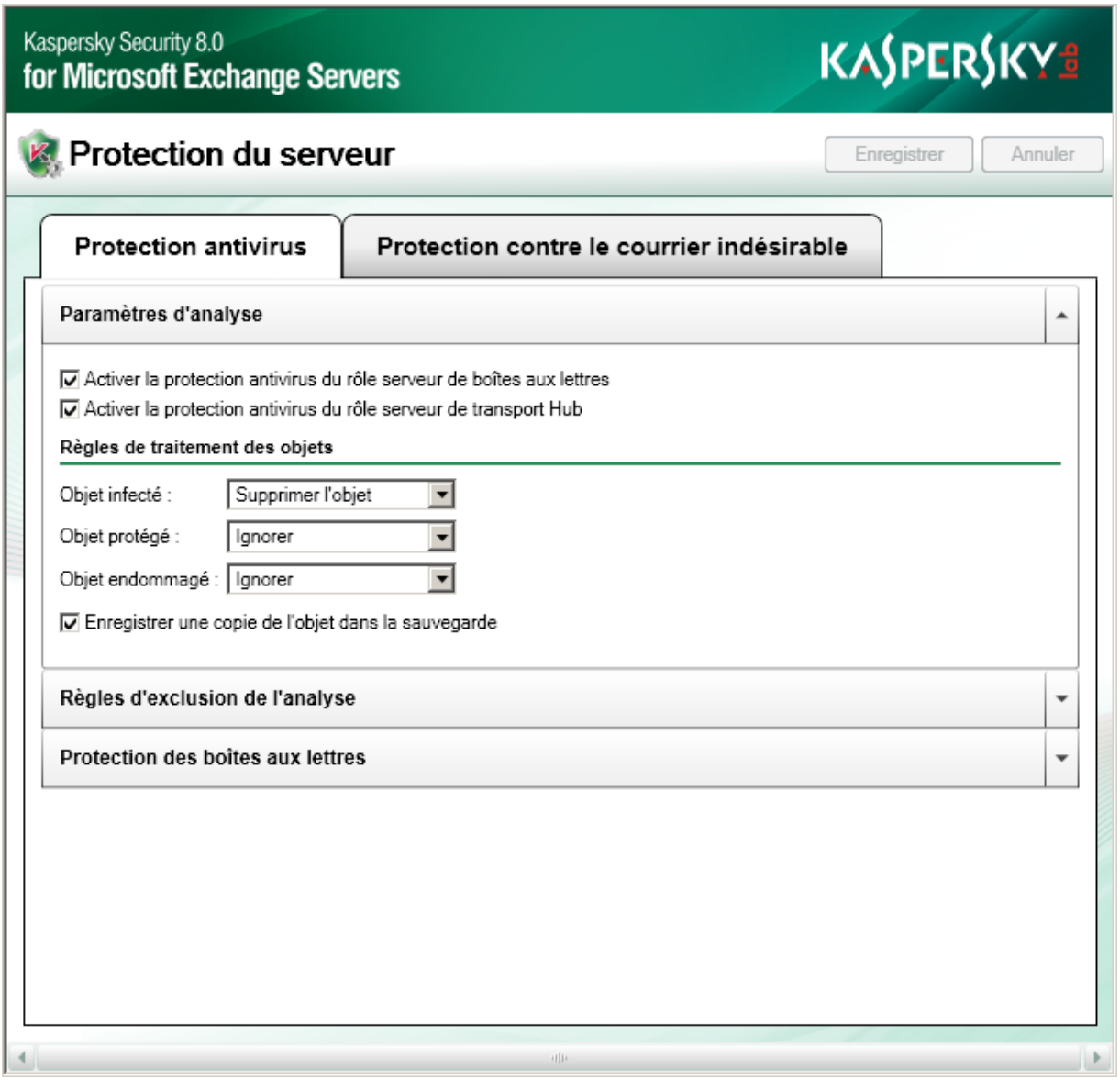


*Illustration 2. Activation de la protection du serveur*

➧ *Pour activer la protection antivirus du serveur Microsoft Exchange connecté, procédez comme suit :*

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

2. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

4. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe **Paramètres d'analyse**.

5. Cochez la case d'activation de la protection antivirus pour tous les rôles de Microsoft Exchange Server.

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

7. Pour désactiver la protection, décochez toutes les cases d'activation de la protection antivirus, puis cliquez sur le bouton **Enregistrer**.

8. Vous pouvez arrêter la protection activée pour des rôles distincts de Microsoft Exchange Server. Pour ce faire, cochez la case d'activation de la protection antivirus pour les rôles de Microsoft Exchange Server que vous avez sélectionnés. Cliquez sur le bouton **Enregistrer**.

*Pour activer la protection du serveur Microsoft Exchange contre le courrier indésirable, procédez comme suit :*

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

2. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

4. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres d'analyse**.

5. Cochez la case **Rechercher la présence de courrier indésirable**.

6. Pour désactiver la protection du serveur contre le courrier indésirable, décochez la case **Rechercher la présence de courrier indésirable**.

7. Cliquez sur le bouton **Enregistrer**.

*Pour arrêter Kaspersky Security, procédez comme suit :*

1. Désactivez la protection antivirus et la protection contre le courrier indésirable via la console d'administration (cf. ci-dessus).

2. Arrêtez le service Kaspersky Security et définissez le type d'exécution **Désactivé**.

*Pour lancer l'application après la désactivation du lancement automatique du service Kaspersky Security, procédez comme suit :*

1. Assurez-vous que le type de lancement de Kaspersky Security a été configuré sur **Automatique**.

2. Activez la protection antivirus et la protection contre le courrier indésirable via la console d'administration (cf. ci-dessus).

# ÉTAT DE LA PROTECTION PAR DÉFAUT DE MICROSOFT EXCHANGE SERVER

Par défaut, la protection du serveur Microsoft Exchange contre les programmes malveillants et le courrier indésirable est active directement après l'installation du composant Serveur de sécurité. Le mode de fonction de l'application suivant se déroule :

- Les objets sont soumis à la recherche de la présence éventuelle de tous les programmes malveillants connus à ce jour :
  - l'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.
  - La durée maximale d'analyse d'un objet est limitée à 180 secondes.
  - La sélection de l'action en cas de découverte d'un objet infecté dépend du rôle de serveur Microsoft Exchange sur lequel l'objet a été découvert. En cas de découverte d'un objet infecté sur 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 le préfixe [Malicious object deleted] est ajouté à l'objet du message. En cas de découverte d'un objet infecté sur le rôle Boîte aux lettres, l'application conserve la copie originale de l'objet (pièce jointe ou corps du message) dans le dossier de sauvegarde et tente de réparer l'objet. Si la réparation est impossible, l'objet est supprimé et remplacé par un fichier texte reprenant des informations au format 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>
    ```

  - Par défaut, l'application ignore tout objet protégé ou endommagé. L'utilisateur peut choisir l'action **Supprimer** pour ces catégories d'objet. Dans ce cas, l'application conserve une copie d'origine du message dans la sauvegarde.
  - Les dossiers partagés et les banques de messages sont soumises à la protection.
- Les messages non sollicités sont filtrés. Par défaut, la recherche des messages non sollicités s'opère selon un niveau d'agressivité faible. Ce niveau offre la combinaison optimale de rapidité et de qualité de l'analyse.
  - L'action " Ignorer " est définie pour tous les messages, mais les messages dont le verdict est " Courrier indésirable " recevront l'intitulé spécial [!!Spam].
  - Le paramètre " Courrier indésirable potentiel " est activé La note [!!Probable Spam] est ajoutée aux messages qui reçoivent ce verdict.
  - Durée maximale d'analyse des messages : 30 s
  - Taille maximale de l'objet à analyser : 300 Ko.
  - Les services externes d'analyse des adresses IP et des URL sont utilisés : DNSBL et SURBL. Ces services permettent de filtrer le courrier indésirable à l'aide de listes noires diffusées d'adresses IP et d'URL.
  - Le service UDS (cf. rubrique " Utilisation de services externes pour le traitement du courrier indésirable " à la page 58) est activé.
- Si la mise à jour des bases de Kaspersky Security a été activée pendant l'installation de l'application, alors cette mise à jour aura lieu à intervalles réguliers depuis les serveurs de mise à jour de Kaspersky Lab selon les paramètres indiqués dans l'Assistant de configuration de l'application.

# PREMIÈRE UTILISATION

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 ..... 38

Création de la liste des serveurs Microsoft Exchange protégés ..... 38

Connexion de la console d'administration au serveur de sécurité ..... 40


## LANCEMENT DE LA CONSOLE D'ADMINISTRATION

*Pour lancer la console d'administration, procédez comme suit :*

1. Dans le menu **Démarrer**, sélectionnez l'option **Programmes**.
2. Dans la liste des programmes, choisissez **Kaspersky Security 8.0 for Microsoft Exchange Servers**.
3. Cliquez avec le bouton gauche de la souris sur l'option **Console d'administration**.

Au lancement de la console d'administration, le composant enfichable Kaspersky Security se connecte à MMC et l'icône de l'application et le noeud **Kaspersky Security 8.0 for Microsoft Exchange Servers** apparaissent dans l'arborescence de la console. De plus, l'arborescence de la console affiche le noeud du serveur de sécurité local (s'il a été installé) connecté à la console.

## CRÉATION DE LA LISTE DES SERVEURS MICROSOFT EXCHANGE PROTÉGÉS

Vous pouvez créer la liste des serveurs Microsoft Exchange protégés. Pour ce faire, le serveur de sécurité doit être installé sur chaque serveur Microsoft Exchange que vous souhaitez protéger. Vous pouvez ajouter un ordinateur local (cf. ill. ci-après) ou n'importe quel serveur Microsoft Exchange protégé parmi ceux installés sur le réseau. Directement après l'ajout d'un serveur, vous pouvez également établir la connexion de la console d'administration avec Kaspersky Security.

*Pour ajouter le serveur de sécurité Kaspersky Security à la liste des serveurs à protéger, procédez comme suit :*

1. Lancez Kaspersky Security via le menu **Démarrer** → **Programmes** → **Kaspersky Security 8.0 for Microsoft Exchange Servers** → **Console d'administration**.
2. Choisissez le nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers** dans l'arborescence de la console.
3. Dans le menu contextuel du noeud, choisissez l'option **Ajouter un serveur** ou sélectionnez l'option du même nom dans le menu **Action**. Vous pouvez également cliquer sur le bouton **Ajouter un serveur** dans la fenêtre des résultats.

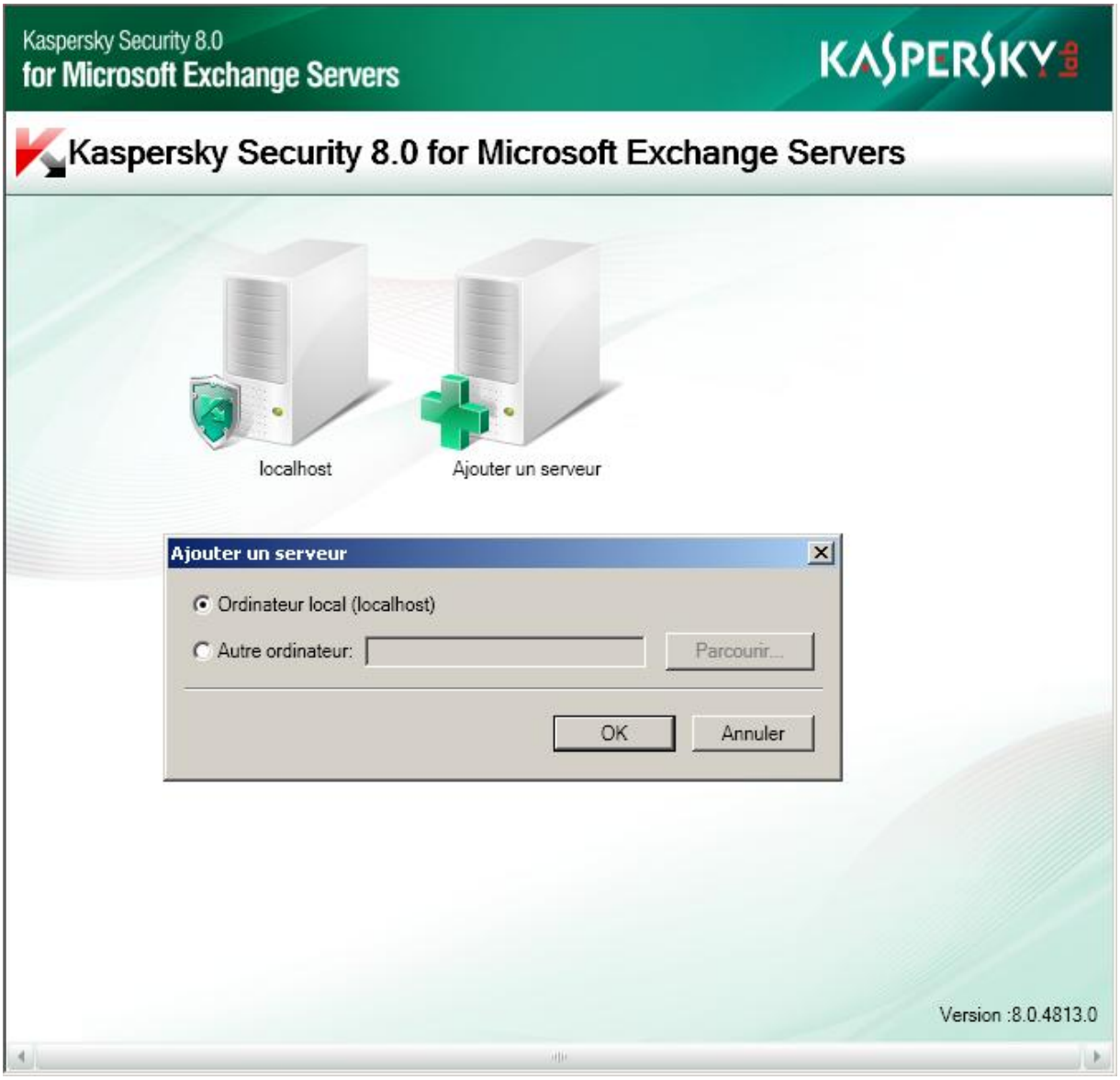


*Illustration 3. Ajout d'un serveur de sécurité*

4. Sélectionnez une des deux options :

   - **Ordinateur local**. Dans ce cas, c'est le serveur de sécurité déployé sur un ordinateur local qui sera ajouté.

   - **Autre ordinateur**. Dans ce cas, vous pouvez connecter le serveur de sécurité installé sur un serveur Microsoft Exchange distant. Pour réaliser la connexion à un serveur de sécurité qui se trouve sur un ordinateur distant, il faut ajouter le service Kaspersky Security à la liste des applications de confiance du pare-feu sur l'ordinateur distant ou autoriser la connexion selon RPC.

5. Si vous avez choisi l'option **Autre ordinateur**, indiquez le nom de l'ordinateur dans le champ. Vous pouvez saisir le nom manuellement en indiquant soit :

   - 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) ;

     ou vous pouvez choisir l'ordinateur dans la liste à l'aide du bouton **Parcourir**.

6. Cliquez sur **OK**.

Vous pouvez réaliser une configuration distincte de Kaspersky Security pour chaque serveur connecté.

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

Après l'installation de Kaspersky Security, la console d'administration se connecte automatiquement au serveur de sécurité local et celui-ci s'affiche dans l'arborescence de la console d'administration. Pour réaliser la connexion à un serveur de sécurité qui se trouve sur un ordinateur distant, il faut ajouter le service Kaspersky Security à la liste des applications de confiance du pare-feu sur l'ordinateur distant ou autoriser la connexion selon RPC.

*Pour connecter un serveur distant, procédez comme suit :*

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

2. Choisissez le nœud **Kaspersky Security 8.0 for Microsoft Exchange Servers** dans l'arborescence de la console.

3. Dans le menu contextuel du noeud, choisissez l'option **Ajouter un serveur** ou sélectionnez l'option du même nom dans le menu **Action**. Vous pouvez également cliquer sur le bouton **Ajouter un serveur** dans la fenêtre des résultats.

4. Dans la fenêtrer qui s'ouvre, choisissez l'option **Autre ordinateur**, puis après avoir cliqué sur le bouton **Parcourir**, saisissez le nom dans le champ. Vous pouvez saisir le nom manuellement. Pour ce faire, vous pouvez indiquer soit :

   - 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).

5. Cliquez sur **OK**.

# MISE À JOUR RÉGULIÈRE DES BASES DE L'ANTIVIRUS ET DE L'ANTI-SPAM

Kaspersky Lab permet à ses utilisateurs de mettre à jour (cf. ill. ci-après) les bases antivirus de Kaspersky Security utilisées pour détecter les programmes malveillants et réparer les objets infectés. Les fichiers des bases contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les méthodes de réparation des objets infectés, sans oublier la description des applications potentiellement dangereuses.

Les bases de l'Anti-Spam sont également mises à jour. Pour que le filtrage du courrier indésirable sur le serveur de messagerie soit le plus efficace possible, il est conseillé de configurer la mise à jour des bases de l'Anti-Spam selon un intervalle de cinq minutes minimum. Il est primordial de maintenir toutes les bases à jour. Il est conseillé de réaliser la mise 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 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 de sélectionner la même fréquence pour la mise à jour automatique (cf. page 43).

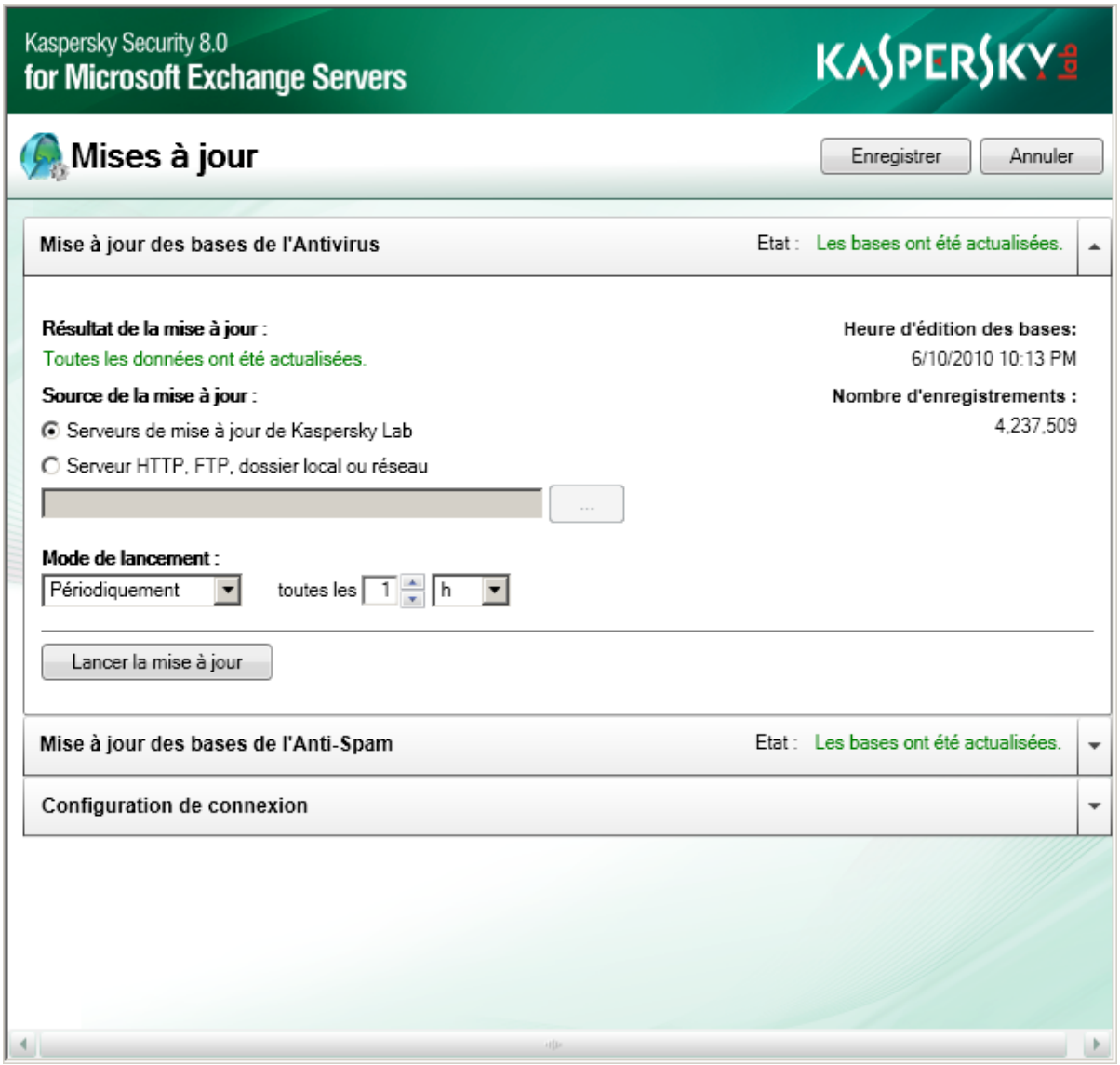


*Illustration 4. Mise à jour des bases antivirus*

La mise à jour des bases peut avoir lieu depuis les sources suivantes :

- les serveurs de mises à jour de Kaspersky Lab en ligne ;
- une source de mise à jour locale (dossier local ou de réseau) ;
- un autre serveur HTTP/FTP (par exemple, votre serveur Intranet).

La mise à jour peut se dérouler manuellement ou selon un horaire défini. Après la copie des fichiers depuis la source de mises à jour définie, l'application utilise automatiquement les bases récupérées et analyse le courrier à l'aide de celles-ci.

### DANS CETTE SECTION DE L'AIDE

Mise à jour manuelle ..... 42

Mise à jour automatique ..... 43

Sélection de la source de la mise à jour ..... 44

Configuration des paramètres de connexion ..... 44

# MISE A JOUR MANUELLE

*Pour consulter les informations relatives à la mise à jour des bases antivirus et actualiser, le cas échéant, les base, procédez comme suit :*

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Déployez le groupe de paramètres **Mise à jour des bases de l'Antivirus**.

   Les informations relatives à la mise à jour des bases contiennent les éléments suivants :

   - **Résultat de la dernière mise à jour**. Informations relatives à l'état de la mise à jour des bases.
   - **Heure d'édition des bases**. Heure d'édition des bases utilisées actuellement par l'application sur le serveur de Kaspersky Lab (UTC).
   - **Nombre d'enregistrements**. Nombre de définitions de virus dans les bases antivirus actuelles.
4. Dans la liste déroulante **Mode de lancement**, sélectionnez l'option **Manuel**.
5. Cliquez sur le bouton **Lancer la mise à jour**.
6. Pour arrêter la mise à jour, cliquez sur **Arrêter**.

*Pour consulter les informations relatives à la mise à jour des bases de l'Anti-Spam et actualiser, le cas échéant, les base, procédez comme suit :*

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Déployez le groupe de paramètres **Mise à jour des bases de l'Anti-Spam**.

Les informations relatives à la mise à jour des bases contiennent les éléments suivants :

- **Résultat de la dernière mise à jour**. Informations relatives à l'état de la mise à jour des bases.
- **Heure d'édition des bases**. Heure d'édition des bases utilisées actuellement par l'application sur le serveur de Kaspersky Lab (UTC).

4. Dans la liste déroulante **Mode de lancement**, sélectionnez l'option **Manuel**.
5. Cliquez sur le bouton **Lancer la mise à jour**.
6. Pour arrêter la mise à jour, cliquez sur **Arrêter**.

# MISE A JOUR AUTOMATIQUE

*Pour réaliser la mise à jour des bases de l'Anti-Virus automatiquement, procédez comme suit :*

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Dans la fenêtre 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 menu déroulant, définissez la valeur du champ **toutes les N minutes, heures, jours** pour la fréquence d'exécution de la mise à jour.
   - **Chaque jour**. Indiquez l'heure exacte dans le champ **au format HH**:**MM** (UTC).
   - **Le jour sélectionné**. Cochez la case en regard des jours de la semaine quand vous souhaitez réaliser la mise à jour des bases. Indiquez également l'heure de la mise à jour.
5. Cliquez sur le bouton **Enregistrer**.
6. Pour arrêter la mise à jour, cliquez sur **Arrêter**. Vous pouvez arrêter uniquement la mise à jour en cours. La mise à jour suivante aura lieu selon la programmation.

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

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Dans la fenêtre 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 menu déroulant, définissez la valeur du champ **toutes les N minutes, heures, jours** pour la fréquence d'exécution de la mise à jour.
   - **Chaque jour**. Indiquez l'heure exacte dans le champ **au format HH**:**MM** (UTC).
   - **Le jour sélectionné**. Cochez la case en regard des jours de la semaine quand vous souhaitez réaliser la mise à jour des bases. Indiquez également l'heure de la mise à jour.
5. Cliquez sur le bouton **Enregistrer**.

6. Pour arrêter la mise à jour, cliquez sur **Arrêter**. Vous pouvez arrêter uniquement la mise à jour en cours. La mise à jour suivante aura lieu selon la programmation.

# SÉLECTION DE LA SOURCE DE LA MISE À JOUR

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

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Dans la fenêtre des résultats, déployez le groupe de paramètres **Mise à jour des bases de l'Antivirus**, puis choisissez une des options suivantes :
   - **Serveurs de mises à jour de Kaspersky Lab** si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab.
   - **Serveur HTTP, FTP, dossier local ou réseau** si vous souhaitez télécharger les mises à jour depuis une des sources de mises à jour citées.
4. Saisissez dans le champ l'adresse du serveur, du dossier local ou du dossier de réseau.
5. Cliquez sur le bouton **Enregistrer**.

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

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Dans la fenêtre des résultats, déployez le groupe de paramètres **Mise à jour des bases de l'Anti-Spam**, puis choisissez une des options suivantes :
   - **Serveurs de mises à jour de Kaspersky Lab** si vous souhaitez télécharger les mises à jour depuis les serveurs de Kaspersky Lab.
   - **Serveur HTTP, FTP, dossier local ou réseau** si vous souhaitez télécharger les mises à jour depuis une des sources de mises à jour citées.
4. Saisissez dans le champ l'adresse du serveur, du dossier local ou du dossier de réseau.
5. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES PARAMETRES DE CONNEXION

*Pour consulter ou modifier les paramètres de la connexion de réseau, procédez comme suit :*

1. Lancez la console d'administration de l'application.
2. Dans l'arborescence de la console d'administration, sélectionnez le noeud **Mises à jour** dans le noeud du serveur qui vous intéresse.
3. Dans la fenêtre 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** et définissez les paramètres de connexion : adresse du serveur proxy et numéro du port pour la connexion. Le numéro du port du serveur proxy est **8080** par défaut.

5. Si l'accès au serveur proxy requiert un mot de passe, définissez les paramètres d'authentification de l'utilisateur. Pour ce faire, cochez la case **Utiliser l'authentification** et remplissez les champs **Compte utilisateur** et **Mot de passe**.

6. Si vous ne souhaitez pas télécharger les mises à jour depuis des adresses locales via le serveur proxy, cochez la case **Ne pas utiliser le serveur proxy pour les adresses locales**.

7. Définissez le délai d'attente de la connexion dans le champ **Délai d'attente de la connexion**. Par défaut, le délai d'attente de la connexion est de **60** s.

# PROTECTION ANTIVIRUS

Une des principales tâches de Kaspersky Security consiste à rechercher la présence éventuelle de virus dans le trafic de messagerie, les messages dans les boîtes aux lettres et les dossiers partagés ainsi qu'à réparer les objets infectés à l'aide des informations de la version actuelle (la plus récente) des bases de Kaspersky Security.

Tous les messages qui arrivent sur le serveur Microsoft Exchange sont analysés en temps réel. Le trafic entrant et sortant est traité, ainsi que le trafic des messages en transit. Vous pouvez réaliser les opérations 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.

En cas de suppression d'un message dans un rôle Boîte aux lettres, l'objet supprimé est remplacé par un fichier texte qui contient le nom de l'objet malveillant, la date d'édition des bases qui ont détecté l'objet et le nom du serveur Microsoft Exchange sur lequel l'objet a été découvert.

Si l'objet malveillant a été découvert sur un transport Hub, le préfixe `Malicious object deleted` est ajouté à l'objet du message.

En mode d'analyse du trafic, l'application se trouve en permanence dans la mémoire vive de l'ordinateur. **L'intercepteur de messages** analyse le flux de messagerie en provenance du serveur Exchange et le transmet au composant Antivirus pour le traitement. Antivirus traite le message et, en fonction des paramètres définis :

- exécute l'analyse de l'objet à l'aide des bases de l'Antivirus ;
- si un message électronique ou une partie de celui-ci est infecté, l'objet infecté est traité conformément aux paramètres définis ;
- avant le traitement, la copie de l'objet peut être conservée dans le dossier de sauvegarde.

Si la protection antivirus du serveur est activée, le lancement et l'arrêt de l'analyse du trafic s'opère en même temps que le lancement et l'arrêt de Microsoft Exchange Server.

Kaspersky Security n'analyse pas les messages créés par des utilisateurs protégés dans les **Dossiers partagés** des serveurs Microsoft Exchange non protégés. Quand un message est transféré hors des **Dossiers partagés** 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.

Les messages enregistrés sur le serveur et le contenu des dossiers partagés sont également analysés régulièrement à l'aide des bases antivirus les plus récentes (si l'analyse en arrière plan des banques est activée (cf. rubrique " Analyse en arrière-plan " à la page 51)). 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.

Le fonctionnement de l'application en mode arrière-plan peut entraîner un ralentissement de Microsoft Exchange Server 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.

En mode d'analyse en arrière-plan, l**e** module interne d'administration de l'application reçoit du serveur Microsoft Exchange, conformément aux paramètres, tous les messages situés dans les dossiers partagés 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 composant Antivirus pour traitement. Le traitement des objets en arrière-plan est identique à celui des objets en mode d'analyse du trafic.

Le programme vérifie le corps du message ainsi que les pièces jointes, quel que soit leur format.

Il convient de signaler que Kaspersky Security fait la différence entre 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 virus est également scindé en plusieurs parties lors du téléchargement partiel de données, il ne sera pas découvert lors 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. Les archives, les objets conteneurs dont le niveau d'imbrication est supérieur au niveau défini et les fichiers selon des masques peuvent être exclus de l'analyse.

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 de conservation des données de l'application. Le dossier Store et la banque des fichiers temporaires (dossier TMP) doivent être exclus de l'analyse par les logiciels antivirus installés sur les ordinateurs dotés d'un serveur Microsoft Exchange.

### DANS CETTE SECTION DE L'AIDE

Activation et désactivation de la protection antivirus du serveur ..... 47

Création de règles de traitement des objets ..... 48

Analyse des archives jointes et des conteneurs ..... 49

Création d'exclusions de l'analyse ..... 49

Configuration des paramètres de protection des boîtes aux lettres ..... 50

Analyse en arrière-plan ..... 51

# ACTIVATION ET DÉSACTIVATION 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 tant que le lancement et l'arrêt de Microsoft Exchange Server. Si les paramètres de la protection contre les virus prévoient l'analyse en arrière-plan (cf. rubrique " Analyse en arrière-plan " à la page 51), elle peut être lancée manuellement ou selon une programmation.

Notez que 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 pour une longue durée.

- *Pour activer ou désactiver la protection antivirus, procédez comme suit :*

1. Lancez Kaspersky Security via le menu **Démarrer** → **Programmes** → **Kaspersky Security 8.0 for Microsoft Exchange Servers** → **Console d'administration**.
2. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
3. Sélectionnez le nœud **Protection du serveur**.
4. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe **Paramètres d'analyse**.

5. Cochez la case d'activation de la protection antivirus pour tous les rôles de Microsoft Exchange Server.

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

7. Pour désactiver la protection, décochez toutes les cases d'activation de la protection antivirus, puis cliquez sur le bouton **Enregistrer**.

8. Vous pouvez arrêter la protection activée pour des rôles distincts de Microsoft Exchange Server. Pour ce faire, cochez la case d'activation de la protection antivirus pour les rôles de Microsoft Exchange Server que vous avez sélectionnés. Cliquez sur le bouton **Enregistrer**.

*Si la nécessité de désactiver manuellement les services Kaspersky Security s'impose, procédez comme suit :*

1. Désactivez la protection antivirus du courrier via la console d'administration (cf. ci-dessus).

2. Arrêtez le service Kaspersky Security et définissez le type d'exécution **Désactivé**.

*Pour lancer l'application après la désactivation du lancement automatique du service Kaspersky Security, procédez comme suit :*

1. Assurez-vous que le type de lancement de Kaspersky Security a été configuré sur **Automatique**.

2. Activez la protection antivirus du courrier via la console d'administration (cf. ci-dessus).

# CRÉATION DE RÈGLES DE TRAITEMENT DES OBJETS

Les règles de traitement des objets permettent de sélectionner une action pour chaque type d'objet. À la fin de l'analyse antivirus, chaque objet peut se voir attribuer un des états suivants :

- **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.

*Pour créer des règles de traitement des objets, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe **Paramètres d'analyse**.

4. Dans la liste déroulante **Objet infecté** de la rubrique **Règles de traitement des objets**, sélectionnez le type d'action :

   - **Ignorer**. Laisser passer le message et l'objet qu'il contient sans réaliser aucune action.
   - **Supprimer l'objet**. Supprimer l'objet infecté et laisser passer le message.
   - **Supprimer le message**. Supprimer le message contenant l'objet infecté avec toutes les pièces jointes.

5. Dans la liste déroulante **Objet protégé**, sélectionnez le type d'action :

   - **Ignorer**. L'analyse antivirus des objets protégés peut être gênée par la protection par mot de passe. Sélectionnez l'option **Ignorer** si vous souhaitez ignorer de tels objets.

- **Supprimer le message**. Sélectionnez cette option si vous souhaitez supprimer des objets protégés par mot de passe. Le message sera complètement supprimé.

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

   - **Ignorer**. Sélectionnez cette option si vous souhaitez ignorer de tels objets.

   - **Supprimer le message**. Sélectionnez cette option pour supprimer les objets endommagés.

Cochez la case **Enregistrer une copie de l'objet original dans la sauvegarde** afin de conserver une copie de l'objet dans le dossier de sauvegarde avant son traitement.

# ANALYSE DES ARCHIVES JOINTES ET DES CONTENEURS

*Pour configurer les paramètres d'analyse des archives jointes et des conteneurs, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe **Règles d'exclusion de l'analyse**.

4. Cochez la case **Analyser les archives** si vous souhaitez que l'application analyse les archives.

5. Cochez la case **Analyser les conteneurs dont le niveau d'imbrication est inférieur à** et indiquez le niveau d'imbrication des conteneurs dans le champ avec la liste déroulante. Le niveau d'imbrication maximum est **128**.

Pour optimiser le fonctionnement de Kaspersky Security, réduire la charge sur le serveur et accélérer le traitement du trafic, vous pouvez désactiver l'analyse des pièces jointes. Pour ce faire, décochez les cases **Analyser les archives** et **Analyser les conteneurs intégrés**. Il est déconseillé de désactiver l'analyse des pièces jointes pour une longue durée car elles peuvent contenir des virus et autres objets malveillants.

# CRÉATION D'EXCLUSIONS DE L'ANALYSE

Pour réduire la charge sur le serveur lors de l'exécution de l'analyse antivirus, vous pouvez limiter les objets à analyser. Les restrictions de l'analyse interviennent aussi bien lors de l'analyse du trafic que lors de l'analyse en arrière-plan des banques. Afin de réduire la charge sur le serveur, vous pouvez désactiver l'analyse des archives et des conteneurs (cf. rubrique " Analyse des archives jointes et des conteneurs " à la page 49) ainsi que définir les masques des fichiers qui ne seront pas analysés ou les destinataires dont les messages seront exclus de l'analyse.

*Pour exclure des fichiers de l'analyse en fonction d'un masque, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe **Règles d'exclusion de l'analyse**.

4. Cochez la case **Ne pas analyser les fichiers en fonction des masques**.

5. Dans le champ de saisie, indiquez le masque des fichiers qui ne seront pas analysés.

   Exemples de masques admis :

   *.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.

6. Cliquez sur le bouton à droite du champ pour ajouter le masque du champ à la liste globale des masques d'exclusion.
7. Cliquez sur le bouton **Enregistrer**.

*Pour exclure de l'analyse les messages envoyés à des destinataires particuliers, procédez comme suit :*

1. Cochez la case **Ne pas analyser les messages destinés à**.
2. Dans le champ, saisissez l'adresse du destinataire dont les messages ne seront pas analysés.
3. Cliquez sur le bouton à droite du champ pour ajouter les destinataires à la liste des destinataires de confiance.
4. Pour enregistrer la liste des destinataires dans un fichier, cliquez sur le bouton .
5. Dans la fenêtre qui s'ouvre, indiquez le nom du fichier dans le champ **Nom du fichier**, puis cliquez sur **Enregistrer**.
6. Pour importer la liste des destinataires dans l'application, cliquez sur le bouton .
7. Dans la fenêtre qui s'ouvre, saisissez le nom du fichier contenant la liste des exclusions dans le champ **Nom du fichier**, puis cliquez sur **Ouvrir**.
8. Cliquez sur le bouton **Enregistrer**.

# CONFIGURATION DES PARAMÈTRES DE PROTECTION DES BOÎTES AUX LETTRES

*Pour activer de manière sélective la protection des boîtes aux lettres, procédez comme suit :*

1. Dans la console d'administration, choisissez le noeud **Protection du serveur**.
2. Sous l'onglet **Protection antivirus**, ouvrez le groupe de paramètres **Protection des boîtes aux lettres**.
3. Dans la section **Banques de boîtes aux lettres à protéger**, cochez les cases en regard des banques de boîtes aux lettres que vous souhaitez protéger.
4. Dans la rubrique **Banques de dossiers public à protéger** , cochez les cases des banques des dossiers partagés que vous souhaitez protéger.
5. Cliquez sur le bouton **Enregistrer** pour que les modifications entrent en vigueur.

Les listes proposées reprennent l'ensemble des banques des boîtes aux lettres et des dossiers partagés du serveur Microsoft Exchange protégé. Par défaut, celles qui existaient déjà au moment de l'installation de l'application et les nouvelles banques sont protégées.

# ANALYSE EN ARRIÈRE-PLAN

Kaspersky Security recherche en arrière-plan la présence éventuelle de virus dans le courrier stocké sur le serveur et dans le contenu des dossiers partagés selon les paramètres définis par l'utilisateur. Tous les dossiers partagés et boîtes aux lettres protégés sont analysés. Sont également analysés les messages qui n'avaient pas encore été analysés à l'aide des bases de Kaspersky Security les plus récentes. L'application analyse le corps du message et les fichiers joints conformément aux paramètres généraux de la protection antivirus. L'analyse en arrière-plan est disponible uniquement pour le serveur Microsoft Exchange déployé dans un rôle de boîte aux lettres. Seuls les dossiers partagés et les boîtes aux lettres des banques protégées sont analysés.

*Pour que l'application réalise l'analyse en arrière-plan des messages stockés sur le serveur et du contenu des dossiers partagés, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection antivirus**, déployez le groupe de paramètres **Protection des boîtes aux lettres**.

4. Dans la liste déroulante **Planification** de la rubrique **Analyse en arrière-plan**, sélectionnez l'option qui vous convient le mieux :

   - **Manuel**. L'utilisateur lance manuellement l'analyse en arrière-plan.

   - **Chaque jour**. Indiquez l'heure précise de l'analyse dans le champ de saisie de l'heure au format **HH:MM**.

   - **Le jour sélectionné**. Cochez la case en regard des jours de la semaine où vous souhaitez réaliser l'analyse en arrière-plan et indiquez l'heure précise du début de l'analyse dans le champ de saisie de l'heure au format **HH**:**MM**.

   - **Chaque mois**. Dans la liste déroulante du champ, indiquez le jour du mois pour l'analyse et indiquez l'heure précise de l'analyse dans le champ de saisie de l'heure au format **HH:MM**.

5. Cochez la case **Analyser le corps du message** afin d'analyser le corps du message lors de l'analyse en arrière-plan.

6. Cochez la case **Analyser uniquement les messages récents** afin d'analyser les messages reçus au cours d'une certaine période avant le début de l'analyse en arrière-plan.

7. Indiquez le nombre de jour à l'aide de la liste déroulante du champ **Analyser les messages arrivés au plus tard il y a N jours avant le lancement de l'analyse en arrière-plan**. La valeur maximale admise pour le nombre de jour est **364**.

8. Cochez la case **Limiter l'analyse dans le temps** et définissez la valeur du paramètre **Stopper l'analyse après N heures de fonctionnement** afin d'optimiser la durée de l'analyse.

9. Cliquez sur **Enregistrer** pour que les changements entrent en vigueur.

10. Cliquez sur **Lancer l'analyse** si vous devez absolument lancer l'analyse immédiatement.

11. Après le lancement, vous pouvez arrêter l'analyse en arrière-plan à l'aide du bouton **Arrêter**. Le début et l'arrêt de l'analyse en arrière-plan ont lieu dans la minute qui suit le clic sur le bouton.

# PROTECTION CONTRE LE COURRIER INDÉSIRABLE

Une des principales tâches de Kaspersky Security consiste à filtrer le courrier indésirable dans le flux de messagerie qui transite via le serveur de transport. Le module de recherche du courrier indésirable (Anti-Spam) filtre le courrier électronique entrant au moment de sa réception via le protocole SMTP, c'est-à-dire avant que les messages n'arrivent dans les boîtes aux lettres des utilisateurs.

Les données suivantes sont soumise à la recherche de spam :

- le trafic interne et externe via le protocole SMTP avec authentification anonyme sur le serveur ;
- les messages qui arrivent sur le serveur via des connexions externes anonymes (serveur edge).

Les types de données suivants ne sont pas soumis à la recherche de courrier indésirable :

- le trafic interne de l'entreprise ;
- le trafic externe qui arrive sur le serveur via une sessions d'authentification. L'analyse de ce trafic peut être activée manuellement (cf. rubrique " Utilisation des possibilités complémentaires de l'Anti-Spam " à la page 59).

Chaque message électronique est soumis à la recherche d'indices de courrier indésirable. Pour ce faire, tous les attributs possibles du message sont d'abord analysés : adresse du destinataire et de l'expéditeur, taille du message, en-tête (y compris les en-têtes From et To), etc.

Ensuite, l'application exploite le filtrage selon le contenu. Autrement dit, le contenu du message (y compris le champ Subject de l'en-tête) et les fichiers joints sont analysés. Des algorithmes linguistiques et heuristiques uniques sont appliqués. Ils reposent sur la comparaison avec des modèles de messages ainsi que sur une analyse plus profonde du texte, de la mise en forme et d'autres attributs des messages électroniques.

Un des verdicts suivants est attribué à l'issue du filtrage des messages :

- Courrier indésirable. L'application considère le message à 100 % comme un message non sollicité.
- Courrier indésirable potentiel. Le message est peut-être non sollicité.
- Notification formelle. Message technique, par exemple sur la remise d'un message au destinataire.
- L'objet ne contient pas de courrier indésirable.. L'objet a été analysé et ne contient pas de courrier indésirable.
- Expéditeur interdit. L'adresse électronique ou l'adresse IP de l'expéditeur du message figure dans la liste noire des adresses.

Grâce à la souplesse de la configuration, l'administrateur peut choisir lui-même le type d'action pour chaque état de message. Les actions suivantes sont applicables aux messages :

- Ignorer. Le message est remis au destinataire sans modification.
- Rejeter. Quand cette action est sélectionnée, le serveur d'où provient le message reçoit en guise de code de retour un message sur l'erreur d'envoi du message (code d'erreur 500). Le message ne sera pas remis au destinataire.
- Supprimer. Si vous sélectionnez cette action, le serveur d'où provient le message recevra une notification sur l'envoi du message (code 250), mais le destinataire ne recevra pas le message..
- Ajouter un classement SCL. Les messages recevront une évaluation sur la probabilité de courrier indésirable (SCL). L'évaluation SCL peut être un chiffre compris entre -1 et 9. Plus l'évaluation SCL est élevée, plus la probabilité que le message soit non sollicité est importante. Pour le calcul de l'évaluation SCL, le classement

spam du message obtenu lors de l'analyse est divisé sur 10. La valeur obtenu est prise comme l'évaluation SCL. Si à la fin du calcul la valeur est supérieure à 9, l'évaluation SCL est égale à 9.

- Ajouter un intitulé. La correspondance électronique considérée comme indésirable par Kaspersky Security ou comme courrier indésirable potentiel reçoit l'intitulé spécial [!!SPAM], [??Probable Spam] ou [!!Blacklisted] dans le champ **Objet**. Les intitulés peuvent être modifiés.

De plus, l'application prévoit la configuration souple de niveau d'agressivité de la recherche de courrier indésirable. Les niveaux d'agressivité suivants sont prévus :

- Maximal. Ce niveau d'agressivité doit être utilisé si vous recevez fréquemment 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. Niveau optimum, selon les experts de Kaspersky Lab, pour la lutte contre le courrier indésirable. Ce niveau convient à la majorité des cas.

- Faible. La protection offerte par ce niveau d'agressivité est quelque peu inférieure à celle du niveau élevé. Ce niveau 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 réduire le niveau. Selon le niveau d'agressivité défini, les états **Courrier indésirable** ou **Courrier indésirable potentiel** sont attribués aux messages analysés conformément au classement spam obtenu lors de l'analyse.

*Tableau 2. La concordance des niveaux d'agressivité et des seuils du classement spam pour attribuer les états **Courrier indésirable** et **Courrier indésirable potentiel***

| NIVEAU D'AGRESSIVITE | COURRIER INDESIRABLE POTENTIEL | COURRIER INDESIRABLE |
|---|---|---|
| Maximal | 50 | 75 |
| Élevé | 50 | 80 |
| Faible | 60 | 90 |
| Minimum | 80 | 100 |

Pour réaliser un filtrage plus précis du courrier indésirable, il est possible d'utiliser les services externes DNSBL et SURBL par défaut ainsi que des listes DNSBL et SURBL définies par l'utilisateur. SURBL est une liste de liens hypertextes qui mènent vers les sites dont la publicité est assurée par les diffuseurs des messages non sollicités. DNSBL est une liste d'adresses IP utilisées pour la diffusion de courrier indésirable. Les listes DNSBL et SURBL sont actualisées en même temps que les bases de l'Anti-Spam toutes les cinq minutes. Le classement de courrier indésirable est attribué aux messages y compris sur la base des réponses des serveurs DNSBL et SURBL. 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 sera augmenté jusqu'à 100. S'il est inférieur, le classement de courrier indésirable ne sera pas augmenté.

Kaspersky Security permet d'utiliser un client DNS dynamique. Le client DNS dynamique 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 utilisant une connexion xDSL ou Dial-up.

Vous pouvez activer la technologie SPF pour traiter le courrier indésirable. La technologie SPF (structure de stratégie de l'expéditeur) permet de vérifier si le nom de domaine de l'expéditeur est authentique. 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 message ne sera pas accepté.

**DANS CETTE SECTION DE L'AIDE**

Configuration des paramètres de recherche de courrier indésirable ..... 54

Création des listes noire et blanche d'expéditeurs ..... 55

Configuration avancée de l'Anti-Spam ..... 57

Utilisation de services externes de traitement du courrier indésirable ..... 58

Utilisation des fonctionnalités avancées de l'Anti-Spam ..... 59

# CONFIGURATION DES PARAMÈTRES DE RECHERCHE DE COURRIER INDÉSIRABLE

*Pour configurer les paramètres de recherche de courrier indésirable, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
2. Sélectionnez le nœud **Protection du serveur**.
3. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres d'analyse**.
4. Cochez la case **Rechercher la présence de courrier indésirable** si vous souhaitez analyser le courrier entrant à l'aide du module **Anti-Spam**.
5. Faites glisser le curseur pour définir le **Niveau d'agressivité** de la recherche de courrier indésirable. Kaspersky Security applique quatre niveaux d'agressivité au filtrage des messages :
   - **Maximal**. Ce niveau d'agressivité doit être utilisé si vous recevez fréquemment 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**. Niveau optimum, selon les experts de Kaspersky Lab, pour la lutte contre le courrier indésirable. Ce niveau convient à la majorité des cas.
   - **Faible**. La protection offerte par ce niveau d'agressivité est quelque peu inférieure à celle du niveau élevé. Ce niveau offre la combinaison optimale de rapidité et de qualité de l'analyse.
   - **Minimum**. Ce niveau d'agressivité doit être utilisé si vous recevez rarement du courrier indésirable, par exemple si vous travaillez dans l'environnement protégé du système de messagerie de l'entreprise.
6. Dans le groupe **Règles de traitement du courrier indésirable**, sélectionnez une des actions possibles pour chaque verdict :
   - **Ignorer**. Dans ce cas, le message sera remis au destinataire sans modifications.
   - **Rejeter**. Quand cette action est sélectionnée, le serveur d'où provient le message reçoit en guise de code de retour un message sur l'erreur d'envoi du message (code d'erreur 500). Le message ne sera pas remis au destinataire.
   - **Supprimer**. Si vous sélectionnez cette action, le serveur d'où provient le message recevra une notification sur l'envoi du message (code 250), mais le destinataire ne recevra pas le message..

7. Définissez les autres actions que vous souhaitez réaliser sur les messages électroniques. Pour ce faire, cochez les cases des paramètres suivants en fonction de vos besoins :

   - **Ajouter un classement SCL**. Un classement de probabilité de courrier indésirable (SCL) sera ajouté au message. L'évaluation SCL peut être un chiffre compris entre -1 et 9. Plus l'évaluation SCL est élevée, plus la probabilité que le message soit non sollicité est importante.

   - **Enregistrer une copie**. Une copie du message sera enregistrée dans la sauvegarde

   - **Ajouter un intitulé**. La correspondance électronique considérée comme indésirable par Kaspersky Security ou comme courrier indésirable potentiel reçoit l'intitulé spécial **[!!SPAM]**, **[??Probable Spam]** ou **[!!Blacklisted]** dans le champ **Objet**. Les intitulés peuvent être modifiés.

# CREATION DES LISTES NOIRE ET BLANCHE D'EXPEDITEURS

Vous pouvez composez une liste d'expéditeurs auxquels vous faites confiance (liste blanche) ou non (liste noire).. Vous pouvez utiliser aussi bien l'adresse électronique de l'expéditeur que l'adresse IP. Après avoir créé la liste, cliquez sur **Enregistrer**, pour que les modifications entrent en vigueur.

*Pour configurer les paramètresdes listes noires et blanche, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres des listes blanche et noire**.

### Création des listes noire et blanche d'adresses électroniques

*Pour créer une listeblanche d'expéditeurs, procédez comme suit :*

1. Cochez la case **Inclure l'adresse de l'expéditeur dans la liste blanche**.

2. Dans le champ, saisissez l'adresse de l'expéditeur dont les messages ne seront pas soumis à l'analyse antispam.

3. Cliquez sur le bouton  pour ajouter à la liste les données saisies dans le champ.

4. Pour supprimer l'entrée sélectionnée de la liste, cliquez sur le bouton  .

5. Pour enregistrer la liste dans un fichier, cliquez sur le bouton  .

6. Pour importer la liste depuis un fichier, cliquez sur le bouton  .

*Pour créer une listenoire d'expéditeurs, procédez comme suit :*

1. Cochez la case **Ajouter l'adresse de l'expéditeur à la liste noire**.

2. Dans le champ, saisissez l'adresse de l'expéditeur dont le message sera considéré comme indésirable.

3. Cliquez sur le bouton  pour ajouter à la liste les données saisies dans le champ.

4. Pour supprimer l'entrée sélectionnée de la liste, cliquez sur le bouton  .

5. Pour enregistrer la liste dans un fichier, cliquez sur le bouton .

6. Pour importer la liste depuis un fichier, cliquez sur le bouton .

### Création des listes noire et blanche d'adresses IP d'expéditeurs

- *Pour créer une listeblanche d'adresses IP, procédez comme suit :*

1. Cochez la case du paramètre **Ajouter l'adresse de l'expéditeur à la liste blanche des adresses IP**.

2. Dans le champ, saisissez l'adresse IP de l'expéditeur dont les messages ne seront pas soumis à l'analyse antispam.

3. Cliquez sur le bouton pour ajouter à la liste les données saisies dans le champ.

4. Pour supprimer l'entrée sélectionnée de la liste, cliquez sur le bouton .

5. Pour enregistrer la liste dans un fichier, cliquez sur le bouton .

6. Pour importer la liste depuis un fichier, cliquez sur le bouton .

- *Pour créer une listenoire d'adresses IP, procédez comme suit :*

1. Cochez la case du paramètre **Ajouter l'adresse de l'expéditeur à la liste noire des adresses IP**.

2. Dans le champ, saisissez l'adresse IP de l'expéditeur dont le message sera considéré comme indésirable.

3. Cliquez sur le bouton pour ajouter à la liste les données saisies dans le champ.

4. Pour supprimer l'entrée sélectionnée de la liste, cliquez sur le bouton .

5. Pour enregistrer la liste dans un fichier, cliquez sur le bouton .

6. Pour importer la liste depuis un fichier, cliquez sur le bouton .

### Création d'une liste blanche d'adresses de destinataires

- *Pour ajouter des destinataires à laliste blanche, procédez comme suit :*

1. Cochez la case du paramètre **Ajouter l'adresse du destinataire à la liste blanche**.

2. Dans le champ, saisissez l'adresse SMTP du destinataire dont les messages ne seront pas soumis à l'analyse antispam.

3. Cliquez sur le bouton pour ajouter à la liste les données saisies dans le champ.

4. Pour supprimer l'entrée sélectionnée de la liste, cliquez sur le bouton .

5. Pour enregistrer la liste dans un fichier, cliquez sur le bouton .

6. Pour importer la liste depuis un fichier, cliquez sur le bouton .

# CONFIGURATION AVANCÉE DE L'ANTI-SPAM

La configuration avancée de l'Anti-Spam permet de configurer en détails les paramètres d'analyse antispam. La configuration avancée permet d'augmenter le classement de courrier indésirable des messages à l'analyse de l'adresse de l'expéditeur, de l'objet du message ou de la langue de rédaction du message.

*Pour augmenter le classement de courrier indésirable à l'analyse de l'adresse de l'expéditeur, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plusou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres avancés**.

4. Dans le groupe de paramètres **Augmenter le classement du courrier indésirable lors de l'analyse de l'adresse de l'expéditeur :** cochez les cases des paramètres suivants en fonction de vos besoins :

   - **Si le champ " À " ne contient pas d'adresses**. Si le champ " À " est vide, le classement de courrier indésirable du message sera augmenté.

   - **Si l'adresse de l'expéditeur contient des chiffres**. Si l'adresse de l'expéditeur et/ou du destinataire contient des chiffres, le classement de courrier indésirable du message sera augmenté.

   - **Si l'adresse de l'expéditeur du message ne contient pas de nom de domaine (@domain.com)**. Si l'adresse de l'expéditeur ne contient pas le nom de domaine, le classement de courrier indésirable du message sera augmenté.

*Pour augmenter le classement de courrier indésirable à l'analyse de l'objet du message, procédez comme suit :*

1. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres avancés**.

2. Dans le groupe de paramètres **Augmenter le classement du courrier indésirable lors de l'analyse de l'objet du message :** cochez les cases des paramètres suivants en fonction de vos besoins :

   - **Si l'objet du message compte plus de 250 caractères**. Si l'objet du message compte plus de 250 caractères, le classement de courrier indésirable du message sera augmenté.

   - **Si l'objet du message contient 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 sera augmenté.

   - **Si l'objet du message contient une balise d'horodatage**. Si l'objet du message contient un identifiant numérique ou une balise d'horodatage, le classement de courrier indésirable du message sera augmenté.

Dans le groupe de paramètres **Augmenter le classement de courrier indésirables si le message est écrit:** cochez les cases des langues de rédaction des messages que vous considérez comme indésirable :

- **En chinois**, si vous considérez que les messages écrits en chinois sont non sollicités.

- **En coréen**, si vous considérez que les messages écrits en coréen sont non sollicités.

- **En thaï**, si vous considérez que les messages écrits en thaï sont non sollicités.

- **En japonais**, si vous considérez que les messages écrits en japonais sont non sollicités.

# UTILISATION DE SERVICES EXTERNES DE TRAITEMENT DU COURRIER INDÉSIRABLE

Kaspersky Security peut traiter le courrier indésirable à l'aide de services externes. Les services externes sont des ressources et des services accessibles sur Internet, par exemple, des listes noires d'adresses IP, etc. Vous pouvez également exploiter la technologie UDS (Urgent Detection System). Le service UDS crée chez le client une signature non réversible du message (elle ne permet pas de rétablir l'objet, le texte du message ou l'adresse/le nom des expéditeurs/destinataires) et l'envoie vers le serveur UDS. Si la signature figure dans les listes noires du serveur UDS, le classement de courrier indésirable du message augmente. Pour pouvoir utiliser ce service, il faut ouvrir les ports suivants : 7060 pour UDS1 et 7080 pour UDS2. La connexion est établie selon le protocole UDP.

*Afin d'utiliser les services externes d'analyse des adresses IP et des URL, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Utilisation de services extemes**. Cochez la case **Utiliser des services externes d'analyse des adresses IP et des URL pour identifier le courrier indésirable**, si vous souhaitez que la recherche de courrier indésirable utilise également des services externes.

4. Dans le groupe de paramètres **Paramètres du service DNSBL**, cochez la case **Utiliser la liste noire du service DNSBL installée par défaut** pour réaliser la recherche du courrier indésirable sur la base des services DNSBL (Domain Name System Block List). DNSBL est une liste d'adresses IP utilisées pour la diffusion de courrier indésirable.

5. Cochez la case **Utiliser une autre liste de la sélection de listes noires du service DNSBL**. Une fois que vous avez activé ce paramètre, vous devez composer une liste. Pour ajouter une entrée à la liste, 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 ou exporter la liste, utilisez les boutons  ou  respectivement.

6. Dans le groupe de paramètres **Paramètres du service SURBL**, cochez la case **Utiliser la liste noire du service SURBL installée par défaut** afin d'analyser les messages sur la base de la liste noire SURBL (Spam URI Realtime Block List) choisie par défaut. SURBL est une liste de liens hypertextes qui mènent vers les sites dont la publicité est assurée par les diffuseurs des messages non sollicités. Ainsi, si le message contient une URL de cette liste, elle sera considérée comme indésirable.

7. Cochez la case **Utiliser une autre liste de la sélection de listes noires du service SURBL**. Une fois que vous avez activé ce paramètre, vous devez composer une liste. Pour ajouter une entrée à la liste, 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 ou exporter la liste, utilisez les boutons  ou  respectivement.

8. Afin de vérifier 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**.

9. Pour utiliser la technologie SPF (Sender Policy Framework), cochez la case **Utiliser la technologie SPF**.

10. Pour vérifier l'adresse IP de l'expéditeur sur l'appartenance du botnet, cochez la case **Vérifier si l'adresse de l'expéditeur est de type DNS dynamique**. Dans le cas du résultat positif, le classement du message sera augmenté.

11. Définissez le délai d'attente pour les requêtes DNS à l'aide du menu déroulant. Par défaut, le délai d'attente est de 10 s.

*Pour utiliser la technologie UDS, procédez comme suit :*

1. Cochez la case **Appliquer la technologie UDS à l'analyse des messages**.

2. Définissez le délai d'attente pour les requêtes UDS à l'aide du menu déroulant. Par défaut, le délai d'attente est de 10 s.

# UTILISATION DES FONCTIONNALITÉS AVANCÉES DE L'ANTI-SPAM

Vous pouvez utiliser les fonctionnalités avancées de l'Anti-Spam. Parmi celles-ci, citons : les paramètres d'analyse, les paramètres d'analyse des documents et d'autres paramètres.

*Pour définir des restrictions au niveau de la durée de l'analyse et de la taille de l'objet, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

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

3. Dans la fenêtre des résultats, sous l'onglet **Protection contre le courrier indésirable**, déployez le groupe **Paramètres complémentaires**. Dans le groupe **Paramètres d'analyse**, définissez la valeur du paramètre **Durée maximale d'analyse des messages (s)** à l'aide du menu déroulant. Si la durée de l'analyse dépasse la valeur indiquée, l'analyse n'aura pas lieu. La valeur par défaut est de 30 s. Cet objet recevra le verdict **objet sain**, mais si les en-têtes de service sont activées, elles contiendront les informations relatives au dépassement de la durée d'analyse.

4. Dans le groupe **Paramètres d'analyse**, définissez la valeur du paramètre **Taille maximale de l'objet à analyser** à l'aide du menu déroulant. Si la taille de l'objet dépasse la valeur indiquée, l'analyse n'aura pas lieu. La valeur par défaut est de 300 Ko. Cet objet recevra le verdict **objet sain**, mais si les en-têtes de service sont activées, elles contiendront les informations relatives au dépassement de la taille maximale de l'objet à analyser.

*Pour configurer les paramètres d'analyse des document, dans le groupe Paramètres d'analyse **Paramètres d'analyse des fichiers Microsoft Office**, procédez comme suit :*

1. Cochez la case **Analyser les fichiers DOC** afin d'analyser les documents créés par Microsoft Word.

2. Cochez la case **Analyser les fichiers RTF** afin d'analyser les fichiers RTF.

*Pour configurer les paramètres avancés, dans le groupe **Autres paramètres** procédez comme suit :*

1. Cochez la case **Activer le résultat d'analyse** si vous souhaitez que l'application attribue le verdict " Courrier indésirable potentiel " aux messages suspects.

2. Cochez la case **Utiliser la technologie d'analyse des images** si vous souhaitez que les images jointes aux messages soient analysées selon la technologie GSG (technologie de traitement des images). Cette technologie permet de rechercher dans les images les modèles présents dans les bases antispam. Si une équivalence est confirmée, le classement de courrier indésirable du message augmente.

3. Cochez la case **Activer l'enregistrement et l'utilisation des modèles de courrier indésirable encodés en UTF8** afin d'activer l'enregistrement et l'utilisation des exemples de courrier indésirable dans l'encodage UTF8. Ce mode permet d'éviter les pertes d'informations dans les modèles de courrier indésirable en langues orientales, mais augmente légèrement la durée de traitement de chaque message. L'activation de ce paramètre est recommandée si l'encodage UTF8 est utilisé dans la correspondance. La modification de ce paramètre entre en vigueur après la mise à jour des bases de l'Anti-Spam.

4. Cochez la case **Inclure les en-têtes de résultats d'analyse (X-Headers) au message** si vous souhaitez ajouter au message les en-têtes X qui reprennent les informations relatives à l'issue de l'analyse.

5. Cochez la case **Analyser les connexions autorisées** afin d'activer l'analyse des messages reçus via des connexions de confiance (Trusted Connection).

6. Cochez la case **Ne pas rechercher la présence de courrier indésirable dans les messages destinés au Postmaster** pour désactiver l'analyse des messages reçus à l'adresse Postmaster.

Si l'évaluation SCL du message est égale à -1, alors Kaspersky Security n'analysera pas le message.

# SAUVEGARDE

Kaspersky Security permet de conserver une copie de l'objet original dans la sauvegarde avant de le traiter.

Par la suite, il sera possible de réaliser les opérations suivantes sur l'objet dans la sauvegarde :

- **L'enregistrer sur le disque** afin de récupérer les informations contenues dans l'objet. Il est possible également de restaurer l'objet et de le soumettre à une nouvelle analyse antivirus à l'aide de la version actualisée des bases ;
- **Le supprimer** ;
- **L'envoyer à Kaspersky Lab pour examen** (uniquement pour les objets suspects contenant la modification d'un virus connu ou le code d'un virus toujours inconnu). Nos experts analyseront l'objet et tenteront de récupérer les données. S'il s'avère que l'objet est infecté par un virus inconnu, les enregistrements des bases seront actualisés. Dans ce cas, la prochaine analyse de cet objet par un logiciel antivirus pour système de fichiers (par exemple, Kaspersky Anti-Virus for Windows Servers) à l'aide de la version actualisée des bases permettra de réparer l'objet et de préserver l'intégrité des données qu'il contient.
- **L'envoyer aux destinataires**. Les objets enregistrés seront accessibles au(x) destinataire(s).

La copie de sauvegarde de l'objet analysé par le composant Antivirus est créée uniquement si la case **Enregistrer une copie de l'objet d'origine dans la sauvegarde** a été cochée dans les paramètres de la protection contre les virus. Les objets traités par le composant Anti-Spam sont également conservés dans la sauvegarde.

L'objet placé dans la sauvegarde est chiffré, ce qui offre les avantages suivants :

- l'absence de risque d'infection (l'objet doit être décodé pour être accessible) ;
- un gain de temps au niveau du travail du logiciel antivirus (les fichiers au format du dossier de sauvegarde ne sont pas considérés comme des fichiers infectés).

Le volume d'informations de la sauvegarde est limité de la manière suivante :

- Le nombrer total d'objets dans la banque ne peut pas dépasser un million. Cette restriction ne peut être levée.
- L'utilisateur peut également définir une limite au niveau de la taille de la sauvegarde et de la durée de conservation des objets qu'elle contient.

Le contrôle du respect des instructions a lieu à intervalle régulier (toutes les minutes). L'ordre des actions de l'application est le suivant :

- quand le nombre maximum d'objets est dépassé, le nombre d'anciens objets nécessaire est supprimé ;
- si la limite a été définie au niveau de la taille de la banque et qu'il n'y a plus de place pour accueillir le nouvel objet, le volume nécessaire est obtenu en supprimant les objets les plus anciens ;
- si la limite a été définie au niveau de la durée de conservation de l'objet, les objets dont la durée de conservation est écoulée seront supprimés.

Le noeud **Sauvegarde** permet de réaliser les opérations suivantes :

- Consultation de la sauvegarde ;
- Manipulation des copies de sauvegarde des objets : consultation des propriétés, restauration, envoi aux destinataires, envoi pour examen et suppression.

Pour faciliter la consultation et la recherche d'informations dans la sauvegarde et sa structure, il est possible de filtrer les données de la sauvegarde (cf. rubrique " Filtrage de la sauvegarde " à la page 65).

**DANS CETTE SECTION DE L'AIDE**

Consultation du dossier de sauvegarde ..... 62

Consultation des propriétés des objets placés dans la sauvegarde ..... 64

Filtrage de la sauvegarde ..... 65

Restauration d'un objet depuis la sauvegarde ..... 66

Envoi d'un objet pour examen ..... 66

Suppression d'un objet de la sauvegarde ..... 67

Configuration des paramètres de la sauvegarde ..... 67

# CONSULTATION DU DOSSIER DE SAUVEGARDE

Vous pouvez consulter tous les objets conservés dans la sauvegarde sous la forme d'un tableau avec des titres (cf. ill. ci-après). Chaque titre propose un type d'informations particulières sur l'objet. Le coin inférieur gauche de la fenêtre des résultats indique le nombre d'objets dans la sauvegarde et l'espace qu'ils occupent sur le disque, ainsi que le nombre d'objets affichés après l'application du filtre.

*Pour consulter le contenu de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

   La fenêtre des résultats présente la liste des copies d'objets dans la sauvegarde.

   Par défaut, vous pouvez obtenir les informations suivantes sur chaque objet de la sauvegarde.

   - **De**. Adresse de l'expéditeur du message.
   - **À**. Adresse du destinataire du message
   - **Objet**. Objet du message.
   - **Verdict**. État du message.
   - **Heure de réception**. Heure exacte de l'arrivée du message sur le serveur Microsoft Exchange.

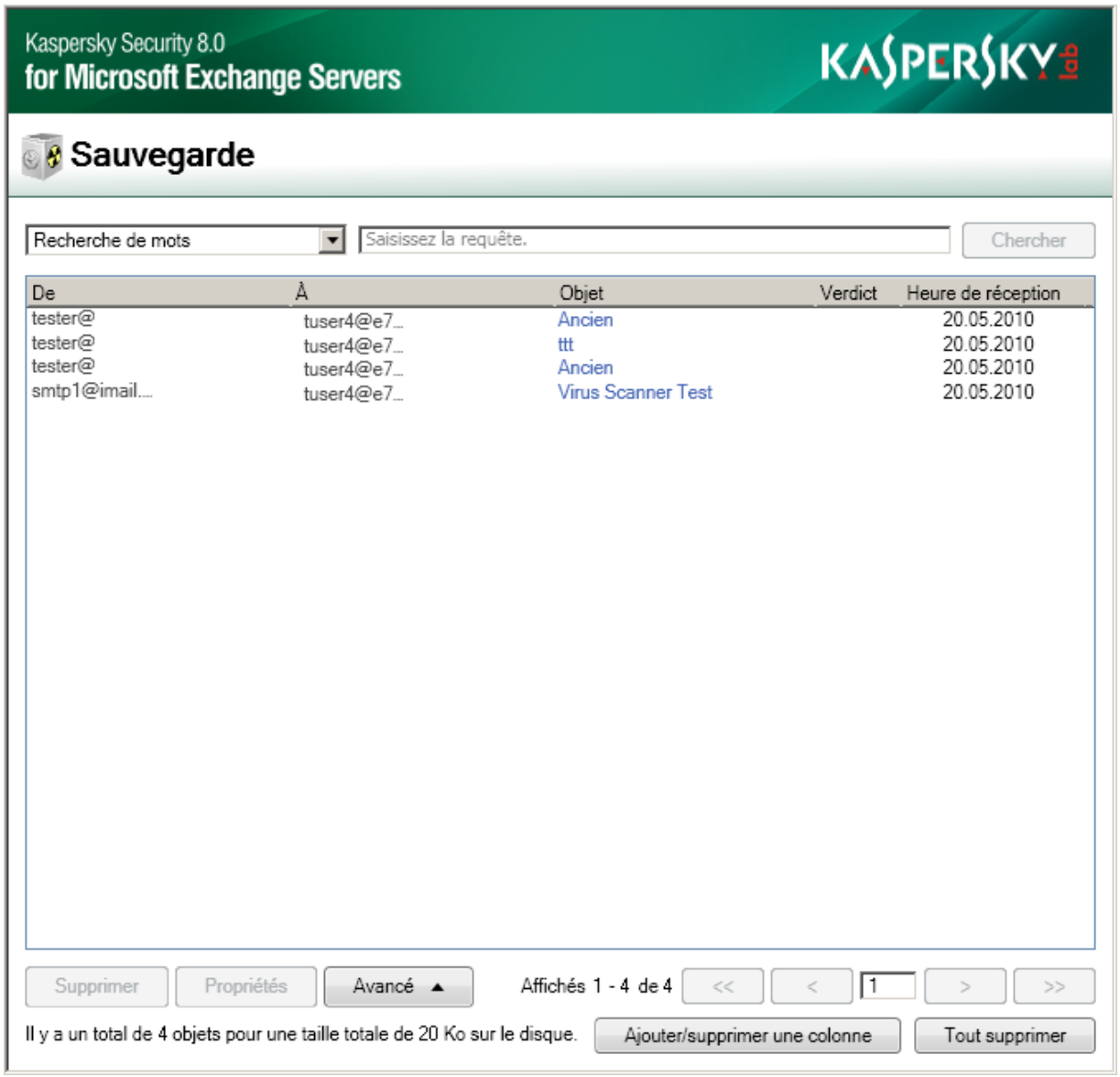


*Illustration 5. Consultation du dossier de sauvegarde*

*Pour configurer l'aspect de la fenêtre des résultats, procédez comme suit :*

1. Pour ajouter des colonnes à la fenêtre des résultats, cliquez sur le bouton **Ajouter/supprimer une colonne**.

2. Dans la fenêtre qui s'ouvre, cochez les cases qui correspondent au type de données que vous souhaitez consulter dans la fenêtre des résultats.

Vous pouvez trier les informations du tableau par ordre croissant ou décroissant selon n'importe quelle colonne. Pour ce faire, cliquez sur un des titres de colonne, par exemple **De**, **À**, **Objet**, etc. Il est possible également de trier les données à l'aide de filtres (cf. rubrique " Filtrage de la sauvegarde " à la page 65).

Un nombre restreint d'objets peut être affiché en une fois dans la fenêtre des résultats. Pour afficher le reste des objets, utilisez les touches de navigation située dans le coin inférieur droit de la fenêtre 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 PROPRIÉTÉS DES OBJETS PLACÉS DANS LA SAUVEGARDE

*Pour consulter le contenu de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

3. Dans la fenêtre des résultats, sélectionnez l'objet placé dans la sauvegarde.

4. Cliquez sur le bouton **Propriétés**. Si le bouton **Propriétés** n'apparaît pas dans la fenêtre des résultats par manque de place, cliquez sur le bouton **Avancé** et choisissez l'option **Propriétés** dans le menu.

   La fenêtre **Propriétés du message** s'ouvre. Les propriétés vous donnent accès aux informations suivantes :

   - **Virus**. Si le message est infecté par un virus, le nom de ce dernier apparaîtra dans ce champ.
   - **Heure d'édition des bases**. La date d'édition des bases.
   - **De**. Adresse de l'expéditeur.
   - **À**. Adresse du destinataire.
   - **Copie**. Destinataire de la copie du message.
   - **Taille sur le disque**. Espace que le message occupe sur le disque.
   - **Objet**. Objet du message.
   - **Chemin d'accès**. Chemin d'accès au message enregistré.
   - **Heure de réception**. Moment exact de la remise du message (jour, mois, année, heures, minutes).
   - **Date de création du message**. Moment exact de la création du message (jour, mois, année, heures, minutes)
   - **Taille**. Taille du message (octet).

Vous pouvez sélectionner plusieurs objets et en consulter les propriétés. Pour ce faire, sélectionnez les objets, cliquez sur le bouton **Avancé**, puis choisissez l'option **Propriétés** dans le menu. La fenêtre **Propriétés des objets sélectionnés** qui s'ouvre permet de consulter le verdict de tous les objets sélectionnés.

# FILTRAGE DE LA SAUVEGARDE

Le recours aux filtres permet de structurer les informations reprises dans la sauvegarde et de lancer des recherches. En effet, quand un filtre est appliqué (cf. ill. ci-après), seules les informations qui répondent aux critères du filtre sont affichées. Cette possibilité s'impose en raison du volume important de données conservées dans la sauvegarde. Le filtre peut par exemple servir à rechercher les objets qui doivent être restaurés.

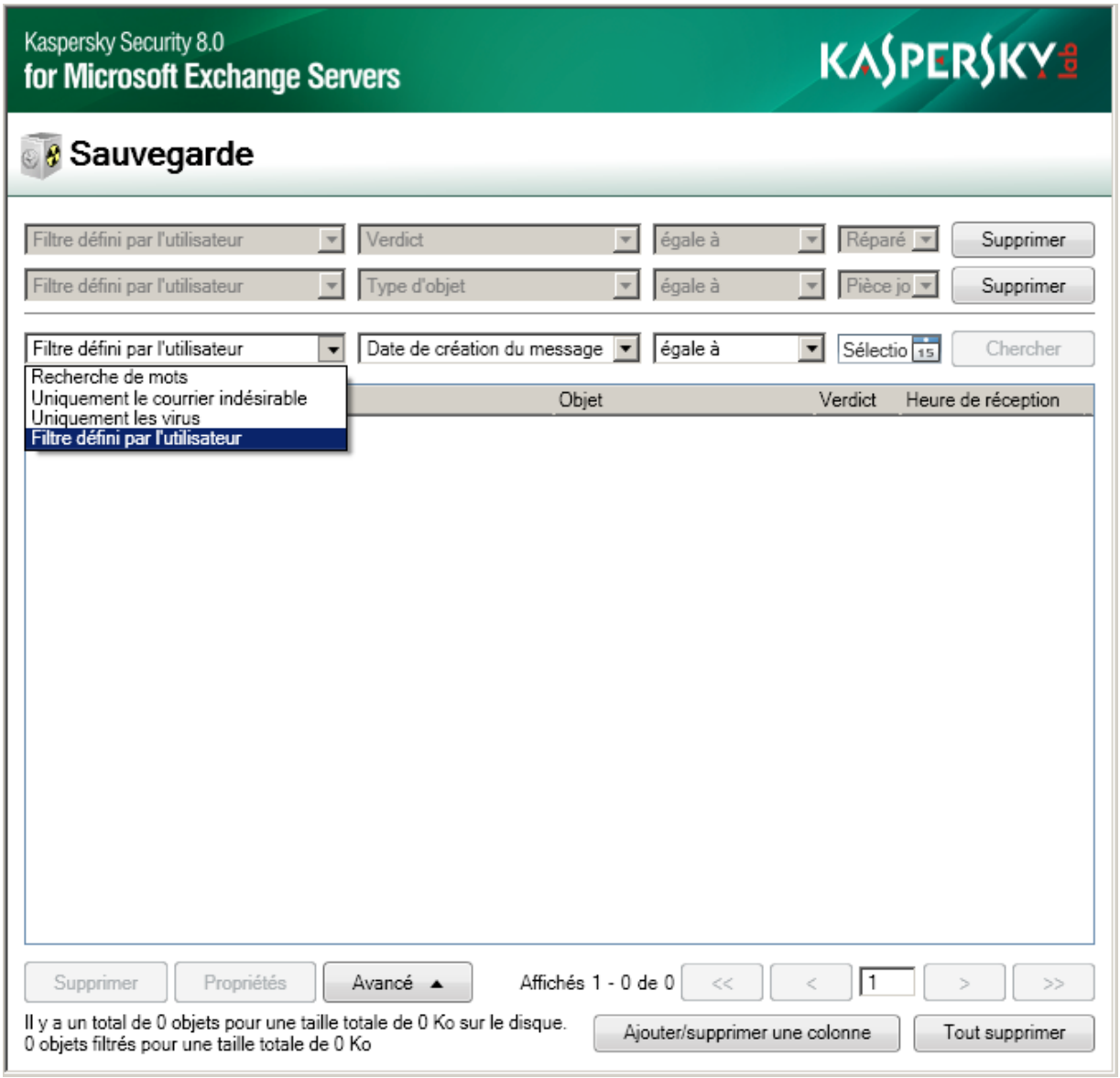


*Illustration 6. Configuration des filtres de la sauvegarde*

➧ *Pour configurer les filtres de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud duserveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

3. Dans la fenêtre des résultats, sélectionnez un des critères de filtrage des objets de la sauvegarde dans la liste déroulante du dessus. Vous avez le choix entre les critères suivants :

   - **Uniquement le courrier indésirable**. La fenêtre des résultats affichera uniquement les messages dont le verdict est " Courrier indésirable ".

- **Uniquement les virus**. Dans ce cas, la fenêtre des résultats affichera uniquement les messages infectés par des virus ou contenant des virus dans les pièces jointes, le corps du messages, etc.

- **Recherche de mots**. Si vous choisissez cette option, il faudra saisir les mots clés à utiliser pour la recherche des messages. La recherche portera sur le champ Objet et sur les adresses des expéditeurs et des destinataires.

- **Filtre défini par l'utilisateur**. Dans ce cas, sélectionnez les critères du filtre dans la liste déroulante, définissez la condition de correspondance du critère à une valeur donnée (par exemple, **égale à** ou **pas égale à**) et saisissez la valeur. 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 **Verdict**, sélectionnez le verdict requis dans la liste déroulante. Pour les autres critères, saisissez les valeurs manuellement dans le champ.

4. Cliquez sur le bouton **Chercher**. Le filtre appliqué apparaîtra en haut de la fenêtre des résultats tandis que les objets correspondant aux critères de la recherche apparaîtront dans la fenêtre.

5. Pour supprimer le filtre, cliquez sur le bouton **Supprimer** à droite du filtre.

6. Pour supprimer tous les objets, cliquez sur le bouton **Tout supprimer**.

Vous pouvez également trier les informations du tableau par ordre croissant ou décroissant selon n'importe quelle colonne. Pour ce faire, cliquez sur un des titres de colonne, par exemple **De**, **À**, **Objet**, etc.

# RESTAURATION D'UN OBJET DEPUIS LA SAUVEGARDE

*Pour restaurer un objet depuis la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

3. Dans la fenêtre des résultats, sélectionnez l'objet que vous souhaitez restaurer.

4. Cliquez sur le bouton **Enregistrer sur le disque**. Si le bouton **Enregistrer sur le disque** n'apparaît pas dans la fenêtre des résultats par manque de place, cliquez sur le bouton **Avancé**, puis sélectionnez l'option **Enregistrer sur le disque** dans le menu.

5. Dans la fenêtre qui s'ouvre, indiquez le dossier dans lequel l'objet restauré sera enregistré et, le cas échéant, saisissez un nom pour l'objet ou modifiez le nom existant.

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

L'objet est décrypté, sa copie est copiée dans le dossier indiqué et enregistrée sous le nom défini. L'objet restauré aura un format identique au format qu'il avait lorsqu'il a été traité par l'application. Un message de circonstance apparaît à l'écran pour confirmer la réussite de la restauration de l'objet. N'oubliez pas que la restauration d'objets peut entraîner l'infection de votre ordinateur.

Vous pouvez également envoyer une copie du message enregistré dans la sauvegarde au destinataire original. Pour ce faire, cliquez sur le bouton **Avancé** et choisissez l'option **Envoyer aux destinataires** dans le menu.

# ENVOI D'UN OBJET POUR EXAMEN

Seul les objets dont l'état est " Suspect " peuvent être envoyés aux experts de Kaspersky Lab pour examen. Avant d'envoyer des objets pour examen, il faut configurer les paramètres généraux de notification (cf. rubrique " Configuration des paramètres de notification " à la page 69).

*Pour envoyer un objet pour examen, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

3. Dans le tableau reprenant le contenu de la sauvegarde, sélectionnez l'objet dont l'état est **Suspect** afin de l'envoyer pour examen. Vous pouvez rechercher l'objet à l'aide d'un filtre (cf. rubrique " Filtrage de la sauvegarde " à la page 65).

4. Dans le menu contextuel de l'objet, choisissez l'option **Envoyer le fichier pour examen**.

Cette action entraîne la composition automatique d'une message électronique avec l'objet en pièce jointe et adressé à Kaspersky Lab sur l'ordinateur où le serveur de sécurité administré. L'objet est envoyé sous forme cryptée, ce qui signifie qu'il ne sera pas à nouveau détecté par Kaspersky Security. Après l'envoi du message, une notification apparaît à l'écran de l'ordinateur utilisé pour l'administration.

# SUPPRESSION D'UN OBJET DE LA SAUVEGARDE

Les objets suivants sont supprimés automatiquement de la sauvegarde :

- L'objet le plus ancien si l'ajout d'un nouvel objet entraîne le dépassement de la limite du nombre d'objets dans la sauvegarde (la limite globale pour cette version de l'application est d'un million d'objets).

- Les objets les plus anciens 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 dont la durée de conservation a expiré, pour autant qu'une telle limite ait été définie.

Il est possible également de supprimer manuellement les objets de la sauvegarde. Cette option peut se révéler utile afin de supprimer les objets qui ont bien été restaurés ou envoyés pour examen ou pour gagner de la place dans la sauvegarde lorsque le mode de suppression automatique des objets n'est pas approprié.

*Pour supprimer un objet de la sauvegarde, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Choisissez le noeud **Sauvegarde**.

3. Dans la fenêtre des résultats, sélectionnez le ou les objets que vous souhaitez supprimer. Vous pouvez rechercher les objets à l'aide d'un filtre (cf. rubrique " Filtrage de la sauvegarde " à la page 65).

4. Cliquez sur **Supprimer**.

5. Pour supprimer directement tous les objets, cliquez sur le bouton **Tout supprimer**.

   Les objets seront supprimé de la sauvegarde.

# CONFIGURATION DES PARAMÈTRES DE LA SAUVEGARDE

Le dossier de sauvegarde est créé 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, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Configuration**.

3. Dans la fenêtre des résultats, dans le groupe **Enregistrement des données**, cochez la case **Limiter la taille de la sauvegarde**.

4. Dans la liste déroulante du champ **La taille de la sauvegarde ne peut être supérieure à**, indiquez la taille maximale de la sauvegarde. Cette limite est fixée par défaut à 5 120 Mo.

5. Cochez la case **Limiter la durée de conservation des objets dans la sauvegarde** et, à l'aide du menu déroulant du champ **Ne pas conserver les objets plus de**, définissez le nombre de jours requis. Cette limite est fixée par défaut à 30 jours.

   Si aucune case n'est cochée, la taille de la banque sera limitée uniquement par le nombre d'objets qu'elle contient (dans cette version de l'application, la limite est d'un million d'objets). Cliquez sur **Enregistrer** pour que les changements entrent en vigueur.

# NOTIFICATIONS

Kaspersky Security offre la possibilité de signaler la détection d'objets infectés, protégés ou suspects lors de l'analyse.

La notification peut être communiquée de différentes manières :

- Envoi d'un courrier électronique. Dans ce cas, il faut configurer les paramètres généraux qui seront utilisés pour l'envoi des notifications.
- Enregistrement 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**

L'expéditeur et le destinataire du message peuvent être prévenus de la découverte d'un objet infecté, protégé ou suspect. Il est également possible de configurer l'envoi des notifications à des adresses électroniques complémentaires, par exemple l'adresse de l'administrateur ou de la personne chargée de la sécurité.

### DANS CETTE SECTION DE L'AIDE

Configuration des paramètres de notification ..... 69

Configuration des paramètres d'envoi des notifications ..... 70

# CONFIGURATION DES PARAMETRES DE NOTIFICATION

*Pour configurer les paramètres des notifications, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
2. Sélectionnez le noeud **Notifications**. La fenêtre des résultats permet de configurer les notifications pour les types d'objets suivants :
   - Objets infectés. Pour configurer les notifications relatives aux objets infectés, déployez le groupe de paramètres **Signaler les objets infectés**.
   - Objets endommagés. Pour configurer les notifications relatives aux objets endommagés déployez le groupe de paramètres **Signaler les objets endommagés**.
   - Objets protégés. Pour configurer les notifications relatives aux objets protégés, déployez le groupe de paramètres **Signaler les objets protégés**.
   - Erreurs système. Pour configurer les notifications relatives aux erreurs système, déployez le groupe **Signaler les erreurs système**. La notification du destinataire et de l'expéditeur n'est pas prévue pour ce type d'objet.
3. Pour chaque type d'objet, configurez les paramètres de la notification dans la rubrique **Signaler par courrier électronique**.
4. Cochez la case **Administrateur** si vous souhaitez envoyer les notifications à l'adresse électronique de l'administrateur.
5. Cochez la case **Expéditeur** si vous souhaitez envoyer les notifications à l'expéditeur du message dans lequel l'objet a été découvert.

6. Cochez la case **Destinataire** si vous souhaitez envoyer les notifications au destinataire du message dans lequel l'objet a été découvert.

7. Cochez la case **Destinataires suivants** et saisissez dans le champ la ou les adresses de courrier électronique auxquelles vous souhaitez envoyer les notifications.

8. Pour consigner les événements dans le journal système Microsoft Windows, cochez la case **Consigner dans le journal des événements Microsoft Windows**.

# CONFIGURATION DES PARAMÈTRES D'ENVOI DES NOTIFICATIONS

*Pour configurer les paramètres d'envoi des notifications, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Notifications**.

3. Ouvrez la fenêtre **Paramètres d'envoi des messages** via le menu contextuel du noeud **Notifications** ou via le lien **Paramètres d'envoi des messages** de la fenêtre des résultats.

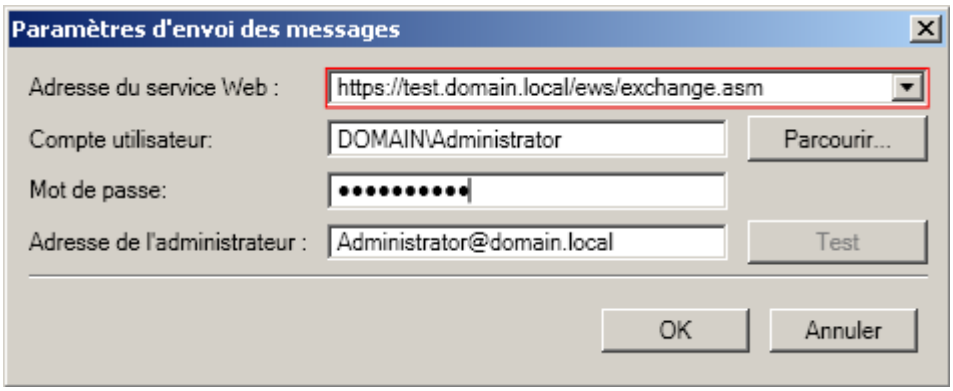


*Illustration 7. Configuration des paramètres d'envoi des messages électroniques*

4. Dans le champ **Adresse du service Web**, indiquez l'adresse du service Web d'envoi des messages électroniques via Microsoft Exchange Server. Par défaut, dans Microsoft Exchange Server, il s'agit de l'adresse :

   `https://<nom_du_serveur_accès_client>/ews/exchange.asmx`

5. Dans le champ **Compte utilisateur**, indiquez n'importe quel compte parmi les boîtes aux lettres inscrites sur Microsoft Exchange Server.

   Pour ce faire, cliquez sur le bouton **Parcourir** ou saisissez le nom du compte utilisateur manuellement.

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. Cliquez sur le bouton**Test** afin d'envoyer un message d'essai.

   Si le message d'essai arrive dans la boîte aux lettres indiquée, cela signifie que l'envoi des notifications est correctement configuré.

Vous pouvez également configurer les paramètres d'envoi des notifications dans le groupe de paramètres **Configuration des notifications** du noeud **Configuration**.

# RAPPORTS

Kaspersky Security permet de créer et de consulter des rapports sur le fonctionnement des composants Antivirus et Anti-Spam. Ces rapports reprennent les statistiques de fonctionnement de l'application pour une période déterminée. Un rapport distinct est créé pour chaque composant pour une période pouvant aller d'un jour à un mois. Les rapports peuvent être standard ou détaillés. Les rapports standard 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 fournissent plus de détails quant au moment où l'événement a eu lieu. L'intervalle de temps minimum repris dans le rapport détaillé est une heure. Les rapports peuvent être créés automatiquement selon une programmation ou manuellement. 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 un texte explicatif :

```
Le fichier joint contient le rapport sur le fonctionnement de Kaspersky Security 8.0 for
Microsoft Exchange Servers.
```

De plus, vous pouvez créer des rapports rapides sur tous les événements survenus au cours de la période définie par l'utilisateur. Les rapports rapides peuvent être créés séparément pour l'Antivirus et l'Anti-Spam. Les rapports rapides sont utiles si vous souhaitez configurer manuellement la période couverte par le rapport.

### DANS CETTE SECTION DE L'AIDE


Configuration des paramètres des rapports rapides ..... 71

Configuration des paramètres des rapports de l'Antivirus ..... 72

Configuration des paramètres de l'Anti-Spam ..... 73

Consultation des rapports prêts ..... 73

Envoi des rapports par courrier électronique ..... 76


# CONFIGURATION DES PARAMÈTRES DES RAPPORTS RAPIDES

*Pour configurer les paramètres des rapports rapides, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
2. Sélectionnez le noeud **Rapports** et dans la fenêtre des résultats, déployez le groupe de paramètres **Rapports rapides**.
3. Dans le champ **Nom du rapport**, saisissez le nom du rapport à créer.
4. Dans la liste déroulante **Type**, sélectionnez une des options suivantes :
   - **Antivirus**. Le rapport pour l'Antivirus sera créé.
   - **Anti-Spam**. Le rapport pour l'Anti-Spam sera créé.
5. Dans la liste déroulante **Niveau de détail**, sélectionnez une des options suivantes :
   - **Standard**. Le rapport contient des informations restreintes sur les objets traités au cours de toute la période couverte par le rapport, sans indication de l'intervalle de temps dans lequel l'événement est survenue.

- **Détaillé**. Le rapport détaillé indique l'intervalle de temps pour chaque événement survenu en fonction de la période sélectionnée pour 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 égale à une semaine, l'intervalle minimum pour chaque événement sera égal à six heures. Si la période est égale à un mois, l'intervalle minimum pour chaque événement sera égal à un jour.

6. Dans la liste déroulante **Fréquence**, sélectionnez une des options suivantes :

   - **pour 24 heures**. Le rapport sera créé pour les dernières 24 heures..
   - **pour la semaine**. Le rapport sera créé pour la dernière semaine.
   - **pour le mois**. Le rapport sera créé pour le dernier mois.

7. Dans le champ **À partir de**, indiquez la date de début de la période du rapport ou choisissez la date dans le calendrier.

8. Pour créer un rapport rapide sur la base des paramètres définis, cliquez sur le bouton **Créer un rapport**.

9. Cliquez sur le bouton **Enregistrer** pour que les modifications entrent en vigueur.

# CONFIGURATION DES PARAMÈTRES DES RAPPORTS DE L'ANTIVIRUS

*Pour configurer les paramètres des rapports de l'Antivirus, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Rapports** et dans la fenêtre des résultats, déployez le groupe de paramètres **Rapport antivirus**.

3. Cochez la case **Création programmée du rapport** si vous souhaitez que les rapports sur le fonctionnement de l'Antivirus soient créés selon un horaire défini.

4. Dans le champ **Nom du rapport**, saisissez le nom du rapport à créer.

5. Dans la liste déroulante **Niveau de détail**, sélectionnez une des options suivantes :

   - **Standard**. Le rapport contiendra les informations relatives aux objets traités tout au long de la période couverte par le rapport sans indication de l'intervalle de temps pour chaque événement.
   - **Détaillé**. Le rapport détaillé indique l'intervalle de temps pour chaque événement survenu en fonction de la période sélectionnée pour 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 égale à une semaine, l'intervalle minimum pour chaque événement sera égal à six heures. Si la période est égale à un mois, l'intervalle minimum pour chaque événement sera égal à un jour.

6. Dans la liste déroulante **Planification de la création du rapport**, sélectionnez une des options suivantes :

   - **Chaque jour**. Si vous choisissez cette option, sélectionnez dans le champ l'heure exacte de la création du rapport.
   - **Chaque semaine**. Si vous choisissez cette option, sélectionnez dans la liste déroulante le jour de la semaine où vous souhaitez créer le rapport. Saisissez dans le champ l'heure exacte de la création du rapport.
   - **Chaque mois**. Si vous choisissez cette option, sélectionnez le jour du mois quand vous souhaitez créer le rapport. Saisissez dans le champ l'heure exacte de la création du rapport.

7. Pour créer un rapport sur le fonctionnement de Kaspersky Antivirus sur la base des paramètres définis, cliquez sur le bouton **Créer un rapport**.

8. Cliquez sur le bouton **Enregistrer** pour que les modifications entrent en vigueur.

# CONFIGURATION DES PARAMÈTRES DE L'ANTI-SPAM

*Pour configurer les paramètres des rapports de l'Anti-Spam, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Rapports** et dans la fenêtre des résultats, déployez le groupe de paramètres **Rapport Anti-Spam**.

3. Cochez la case **Création programmée du rapport** si vous souhaitez que les rapport sur le fonctionnement de l'Anti-Spam soient créés selon un horaire défini.

4. Dans le champ **Nom du rapport**, saisissez le nom du rapport à créer.

5. Dans la liste déroulante **Niveau de détail**, sélectionnez une des options suivantes :

   - **Standard**. Le rapport contiendra les informations relatives aux objets traités tout au long de la période couverte par le rapport sans indication de l'intervalle de temps pour chaque événement.

   - **Détaillé**. Le rapport détaillé indique l'intervalle de temps pour chaque événement survenu en fonction de la période sélectionnée pour 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 égale à une semaine, l'intervalle minimum pour chaque événement sera égal à six heures. Si la période est égale à un mois, l'intervalle minimum pour chaque événement sera égal à un jour.

6. Dans la liste déroulante **Planification de la création du rapport**, sélectionnez une des options suivantes :

   - **Chaque jour**. Si vous choisissez cette option, sélectionnez dans le champ l'heure exacte de la création du rapport.

   - **Chaque semaine**. Si vous choisissez cette option, sélectionnez dans la liste déroulante le jour de la semaine où vous souhaitez créer le rapport. Saisissez dans le champ l'heure exacte de la création du rapport.

   - **Chaque mois**. Si vous choisissez cette option, sélectionnez le jour du mois quand vous souhaitez créer le rapport. Saisissez dans le champ l'heure exacte de la création du rapport.

7. Pour créer un rapport sur le fonctionnement de l'Anti-Spam sur la base des paramètres définis, cliquez sur le bouton **Créer un rapport**.

8. Cliquez sur le bouton **Enregistrer** pour que les modifications entrent en vigueur.

# CONSULTATION DES RAPPORTS PRETS

*Pour consulter les rapport sur le fonctionnement des composants dans l'application, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Rapports** et dans la fenêtre des résultats, déployez le groupe de paramètres **Rapports disponibles**.

Tous les rapports créés apparaissent dans le tableau des rapports disponibles. Les informations suivantes sont proposées pour chaque rapport :

- **Nom**. Nom par défaut ou nom choisi par l'utilisateur.
- **Type**. Le composant auquel se rapporte le rapport.
- **Date**. Date de création du rapport au format **JJ.MM.AAAA**.
- **Niveau de détail**. Détaillé ou standard.
- **Fréquence**. Intervalle de temps couvert par le rapport.

3. Pour consulter un rapport en particulier, sélectionnez le dans la liste, puis cliquez sur le bouton **Afficher**.

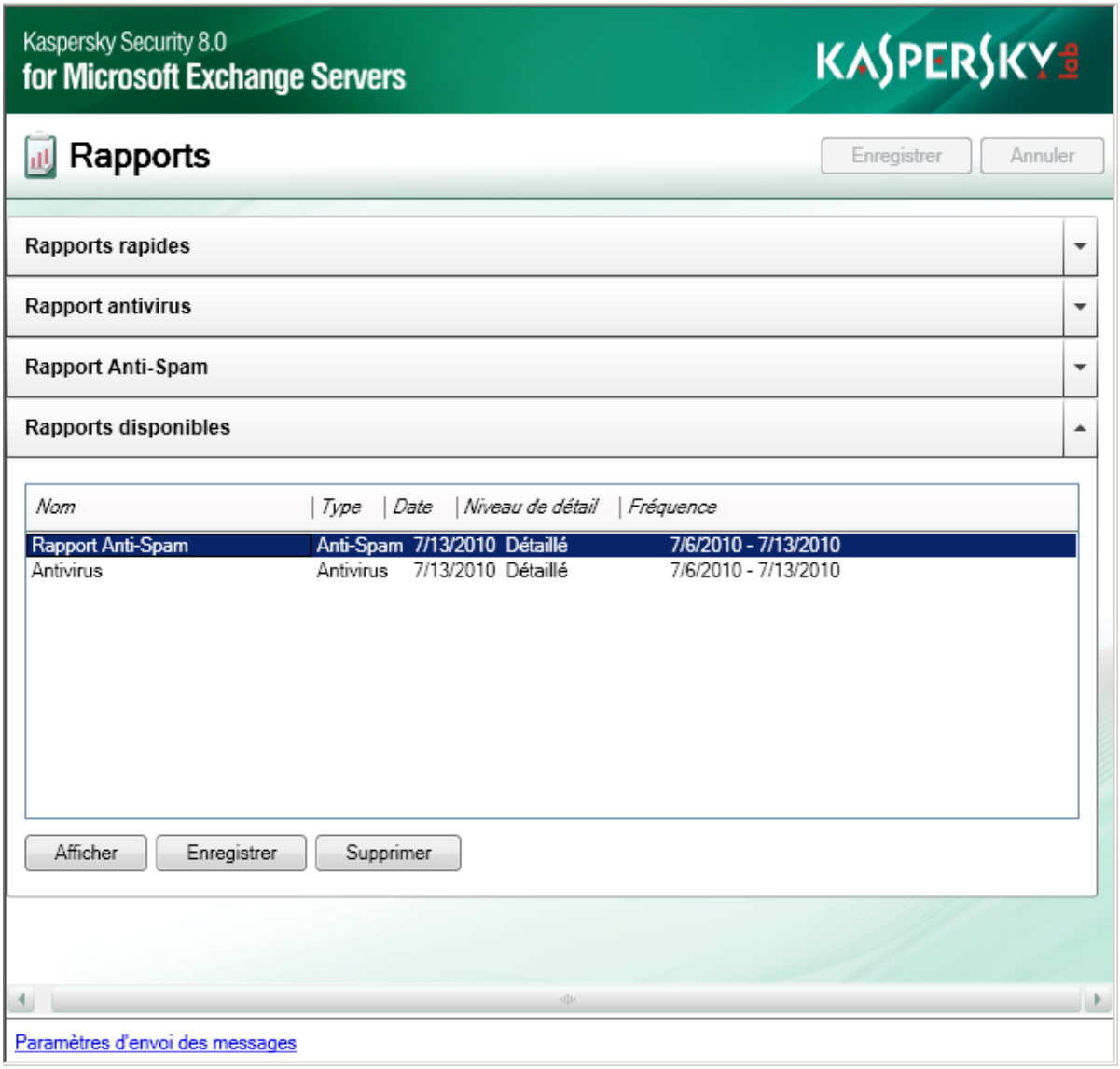


*Illustration 8. Consultation des rapports prêts*

### Consultation du rapport de l'Antivirus

Le rapport standard de l'Antivirus contient les données suivantes dans l'en-tête :

- Type de rapport ;

- Nom du serveur pour lequel le rapport est créé ;
- Période pour laquelle le rapport est créé ;
- Jour, mois et année de création du rapport (UTC).

Le tableau du rapport standard de l'Antivirus reprend les informations suivantes :

- **Verdict**. État de l'objet après le traitement par l'Antivirus.
- **Nombre d'objets**. Nombre d'objets portant ce verdict.
- **Part du nombre total**. Pourcentage d'objets portant ce verdict sur le total d'objets.
- **Taille**. Taille des objets (Mo).

Le rapport détaillé de l'Antivirus contient les données suivantes dans l'en-tête :

- Type de rapport ;
- Nom du serveur pour lequel le rapport est créé ;
- Période pour laquelle le rapport est créé ;
- Jour, mois et année de création du rapport (UTC).

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 sains**. Objets non infectés.
- **Objets réparés**. Les objets qui ont pu être réparés.
- **Objets infectés**. Objets infectés.
- **Objets suspects**. Objets qui peuvent contenir un virus inconnu.
- **Objets protégés**. Objets protégés par un mot de passe, par exemple des archives.
- **Objets endommagés**. Nombre total d'objets endommagés.
- **Violation de la licence**. Objets qui n'ont pas été analysés en raison d'une violation des conditions de la licence de Kaspersky Security.
- **Erreur de bases de l'Antivirus**. Erreur d'analyse provoquée par des bases incorrectes.
- **Erreur de traitement**. Objets dont le traitement a produit une erreur.
- **Nombre total d'objets**. Nombre total d'objets reçus.

Tous les rapports de l'Antivirus contiennent des informations sur la taille des objets traités. La colonne **Pour toute la période** indique le nombre total d'objets traités pour toute 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 :

- Type de rapport ;

- Nom du serveur pour lequel le rapport est créé ;
- Période pour laquelle le rapport est créé ;
- Jour, mois et année de création du rapport (UTC).

Le tableau du rapport standard de l'Anti-Spam reprend les informations suivantes :

- **Verdict**. État de l'objet après le traitement par l'Anti-Spam.
- **Nombre de messages**. Nombre de messages portant ce verdict.
- **Pourcentage du nombre total**. Pourcentage de messages portant ce verdict sur le total de messages.
- **Taille**. Taille du message.

Le rapport détaillé de l'Anti-Spam contient les données suivantes dans l'en-tête :

- Type de rapport ;
- Nom du serveur pour lequel le rapport est créé ;
- Période pour laquelle le rapport est créé ;
- Jour, mois et année de création du rapport (UTC).

Le tableau du rapport détaillé de l'Anti-Spam reprend les informations suivantes :

- **Période**. Période pendant laquelle les messages ont été traités.
- **Ne contient pas de courrier indésirable**. Messages qui ne contiennent pas de courrier indésirable.
- **De confiance**. Messages en provenance d'expéditeurs de confiance.
- **Courrier indésirable**. Messages qui appartiennent au courrier indésirable.
- **Courrier indésirable potentiel**. Messages qui pourraient appartenir au courrier indésirable.
- **Notification formelle**. Message sur la remise d'un courrier et autres notificatons de service.
- **Expéditeur interdit**. L'adresse de l'expéditeur a été ajoutée à la liste noire.
- **Non analysé**. Messages qui n'ont pas été analysés par l'Anti-Spam.

Tous les rapports de l'Anti-Spam contiennent des informations sur la taille des messages traités. La colonne **Pour toute la période** indique le nombre total de messages traités pour toute la période couverte par le rapport.

# ENVOI DES RAPPORTS PAR COURRIER ÉLECTRONIQUE

*Pour configurer l'envoi des rapports par courrier électronique, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
2. Choisissez le noeud **Rapports** et dans la fenêtre des résultats, déployez le groupe des paramètres des rapports au sujet desquels vous souhaitez être averti par courrier électronique.
3. Dans la rubrique **Envoyer le rapport à l'adresse électronique**, cochez la case **Administrateur** si vous souhaitez que les rapports soient envoyés à l'adresse électronique de l'administrateur.

4. Cochez la case **Destinataires suivants** et saisissez dans le champ d'adresse électronique à laquelle les rapports seront envoyés.

5. Cliquez sur le bouton **Enregistrer** pour enregistrer les paramètres d'envoi des rapports

6. Cliquez sur le bouton**Test** afin d'envoyer un message d'essai.

   Si le message de test est arrivé à l'adresse indiquée, cela signifie que les paramètres d'envoi des rapports ont été correctement configurés. Si le message de test n'est pas arrivé, assurez-vous que les paramètres d'envoi des messages électroniques (cf. rubrique " Configuration des paramètres d'envoi des notifications " à la page 70) ont été correctement configurés.

# JOURNAUX DES ÉVÉNEMENTS DE L'APPLICATION

Kaspersky Security permet de consigner les événements survenus dans le journal des applications du système d'exploitation Microsoft Windows et dans ses propres journaux.

Le niveau de détail des informations consignées dans les journaux dépend du niveau de diagnostic défini dans les paramètres de l'application.

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**. Pour Kaspersky Security, la colonne **Source** contiendra **KSCM8**.

Les journaux des événements 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 ajouté si plusieurs fichiers de rapport ont été créés pendant la période en question.
- antivirus_updater_tracelog_aaaajjmm[N].log est le journal de la mise à jour des bases de l'Antivirus
- antispam_updater_tracelog_aaaajjmm[N].log est le journal de la mise à jour des bases de l'Anti-Spam.

Un journal est créé par défaut chaque jour. La consignation des informations dans le journal des événements de Kaspersky Security s'opère à la fin du fichier le plus récent. Par défaut, la taille du journal est limitée à 100 Mo. Cette valeur peut être modifiée. Quand un journal atteint la taille limite, il est archivé et un autre journal est créé. La consultation des journaux des événements 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 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.

### DANS CETTE SECTION DE L'AIDE

Configuration du niveau de diagnostic ..... 78

Configuration des paramètres des journaux..... 79

# 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, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.
2. Sélectionnez le noeud **Configuration**.
3. Dans la fenêtre résultats, dans la rubrique **Diagnostic**, utilisez la liste déroulante **Niveau de détail** et choisissez l'option **Minimum**. Dans ce cas, les journaux contiendront le volume minimum d'informations. Pour configurer la journalisation détaillée des événements dont vous avez besoin pour analyser les défaillances et les résoudre, cliquez sur **Configuration** et dans la fenêtre **Configuration des paramètres de diagnostic** qui s'ouvre, cochez les cases en regard des événements pour lesquels vous souhaitez activer la journalisation détaillée. Cliquez sur **OK** dans la fenêtre **Configuration des paramètres de diagnostic**. L'option **Personnalisé** apparaît

dans la liste déroulante **Niveau de détail**. N'oubliez pas que la tenue de journaux détaillés peut ralentir l'application.

4. Cliquez sur le bouton **Enregistrer** dans la fenêtre des résultats.

# CONFIGURATION DES PARAMETRES DES JOURNAUX

*Pour configurer les paramètres des journaux, procédez comme suit :*

1. Dans l'arborescence de la console, sélectionnez le noeud du serveur connecté et déployez-le en cliquant sur le signe plus ou en double-cliquant sur le nom du serveur.

2. Sélectionnez le noeud **Configuration**.

3. Dans la rubrique **Diagnostic** de la fenêtre des résultats, dans la liste déroulante **Enregistrer un nouveau fichier de journal**, sélectionnez une des valeurs suivantes :

   - **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. Pour le paramètre **Taille maximale du fichier** indiquez la valeur à l'aide de la liste déroulante du champ. La taille maximale du fichier est de 100 Mo.

5. Cochez la case **Notifier les erreurs par courrier électronique** pour recevoir des notifications par courrier électronique (cf. rubrique " Configuration des paramètres d'envoi des notifications " à la page 70) sur les événements indiqués en plus de la consignation dans le journal. Les notifications seront envoyées à l'administrateur.

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

# QUESTIONS FRÉQUEMMENT POSÉES

Ce chapitre est consacré aux questions fréquemment posées sur l'installation, la configuration et l'utilisation de Kaspersky Security.

Question :l'application peut-elle être utilisée simultanément avec les logiciels d'autres éditeurs ?

Kaspersky Security est un logiciel de protection de la messagerie contre les virus et le courrier indésirable prévu pour les réseaux des entreprises. Par conséquent, il peut fonctionner conjointement avec d'autres solutions antivirus de Kaspersky Lab appartenant à la famille Kaspersky Open Space Security (par exemple Kaspersky Anti-Virus 6.0 for Windows Workstations, Kaspersky Anti-Virus 6.0 for Windows Servers) déployées sur le réseau.

Les logiciels antivirus et antispam d'autres éditeurs peuvent être installés sur le serveur Microsoft Exchange, déployé dans le rôle transport Hub ou transport Edge et fonctionner avec les intercepteurs de Kaspersky Security pour ces rôles. Mais cela augmente sensiblement la charge de l'ordinateur ainsi que les exigences en matière de compétences de l'administrateur qui doit garantir la compatibilité des configurations des logiciels antivirus. Par conséquent, il est conseillé de supprimer les logiciels antivirus d'éditeurs tiers avant d'installer Kaspersky Security.

Kaspersky Security ne fonctionne pas avec les logiciels antivirus d'éditeurs tiers sur un serveur Microsoft Exchange déployé dans le rôle de boîte aux lettres !

Question : pourquoi l'application entraîne-t-elle une baisse des performances de mon ordinateur et surcharge-t-elle le processeur ?

La détection des virus et le filtrage du courrier indésirable sont des tâches mathématiques liées à l'analyse de la structure, de la somme de contrôle et de transformation mathématiques des données. Pour cette raison, la principale ressource utilisée par l'application est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse.

À la différence des éditeurs d'autres logiciels antivirus qui ont choisi de réduire la durée de l'analyse en ignorant les virus les plus difficiles à déceler ou les plus rare (dans la zone géographique où l'éditeur est présent) ou en ignorant les formats plus complexes (par exemple, les pdf), Kaspersky Lab estime que la tâche d'un antivirus est de garantir la véritable protection antivirus des utilisateurs.

L'application Kaspersky Security permet à l'utilisateur expérimenté d'accélérer l'analyse antivirus et le filtrage du courrier indésirable en désactivant l'analyse de différents types de fichiers. Il convient de remarquer toutefois que cela s'accompagne d'une diminution du niveau de protection.

L'application Kaspersky Security est capable d'analyser plus de 700 formats de fichiers archivés ou compressés. Ceci est très important au niveau de la sécurité antivirus car chacun des formats reconnus peut contenir un code malicieux exécutable qui s'active après le décompactage/le désarchivage.

Question : à quoi sert la licence de Kaspersky Security ? L'application peut-elle fonctionner sans licence ?

L'application Kaspersky Security ne peut fonctionner sans licence.

Si vous n'avez pas encore décidé d'acheter une version sous licence de l'application, nous pouvons vous fournir une licence d'évaluation (Trial) qui fonctionnera deux semaines ou un mois. Passé ce délai, la licence sera bloquée.

Question : que se passe-t-il à l'expiration de la licence de Kaspersky Security?

À l'expiration de la licence, l'application continuera à fonctionner, mais il ne sera plus possible de mettre à jour les bases. Kaspersky Security réalisera comme avant la recherche de virus et le filtrage du courrier indésirable dans le trafic de messagerie ainsi que l'analyse en arrière-plan des banques à l'aide de l'ancienne version des bases.

Si vous vous retrouvez dans cette situation, contactez le revendeur chez qui vous avez acheté Kaspersky Security ou Kaspersky Lab directement afin de renouveller la licence.

Question : quelle doit être la fréquence des mises à jour ?

Il y a encore quelques années, les virus étaient transmis via disquette et afin de protéger l'ordinateur, il suffisait d'installer un logiciel antivirus et de procéder de temps à autre à la mise à jour des bases antivirus. Les épidémies les plus récentes se sont répandues à travers le monde entier en quelques heures uniquement et dans ces conditions, un logiciel antivirus équipé d'anciennes bases antivirus est impuissant face aux nouvelles menaces. Afin de ne pas devenir victime de la prochaine épidémie de virus, il est indispensable de mettre à jour les bases antivirus quotidiennement, voire plus souvent encore. La mise à jour des bases de l'Anti-Spam doit avoir lieu toutes les cinq minutes. Ceci permet d'actualiser en temps utiles la protection du serveur contre le courrier indésirable.

L'émergence de virus qui utilisent les nouvelles technologies de modification dissimulée des objets infectés impose la mise à jour non seulement des bases, mais également de tous les modules de l'application.

Question : un individu mal intentionné peut-il remplacer les bases de Kaspersky Security ?

Chaque base antivirus dispose d'une signature unique que l'application vérifie lorsqu'elle consulte ces bases. Si la signature ne correspond pas à celle octroyée par Kaspersky Lab ou que la date de la base de données est postérieure à la date d'expiration de la licence, l'application n'utilisera pas ces bases.

Question : j'utilise un serveur proxy et la mise à jour ne fonctionne pas. Que faire ?

Ce problème est provoqué probablement par un serveur proxy qui ne prend pas complètement en charge le protocole HTTP 1.0. Dans ce cas, nous vous recommandons d'utiliser n'importe quel autre serveur proxy.

Question : les nouvelles banques ajoutées à Microsoft Exchange n'apparaissent pas dans la liste des banques protégées. Que faire ?

Les banques apparaîtront après le redémarrage du service de Kaspersky Lab.

Après que vous aurez activé la protection de celles-ci, il faudra cocher manuellement les cases en regard des noms de ces banques dans le noeud **Protection du serveur** sous l'onglet **Protection antivirus** dans le groupe de paramètres **Protection des boîtes aux lettres**.

Question : il arrive parfois que des fichiers au format msg, intégrés à un message, s'endommagent lors de l'envoi et il n'est plus possible de les ouvrir. Cela est-il dû au fait que les fichiers ont été analysés par Kaspersky Security ?

Cette situation est survenue pendant les tests de l'application. Les résultats ont indiqué que les fichiers de ce format peuvent s'endommager lors de l'envoi via Microsoft Exchange, que l'application Kaspersky Security soit installée ou non.

# CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez déjà acheté Kaspersky Security, vous pouvez obtenir des informations sur cette application auprès des experts du service d'assistance technique par téléphone ou via Internet.

Les experts du Service d'assistance technique répondront à vos questions concernant l'installation et l'utilisation de l'application. En cas d'infection de votre ordinateur, ils vous aideront à supprimer les conséquences de l'action des programmes malveillants.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

### Envoi d'une demande au service d'assistance technique par voie électronique

Vous pouvez poser des questions aux experts du service d'assistance technique via le formulaire en ligne du système de traitement des requêtes des clients (http://support.kaspersky.ru/helpdesk.html?LANG=fr).

Vous pouvez soumettre votre requête en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une requête électronique, vous devez saisir le **numéro de client**, que vous avez obtenu lors de votre enregistrement sur le site du service d'assistance technique et votre **mot de passe**.

Si vous n'êtes pas encore un utilisateur enregistré des applications de Kaspersky Lab, vous pouvez remplir un formulaire d'inscription (https://support.kaspersky.com/fr/personalcabinet/registration/form/). Lors de l'enregistrement, saisissez le *code d'activation* de l'application ou le *nom du fichier de licence*.

Les experts du service d'assistance technique répondront à la question dans votre Espace personnel (https://support.kaspersky.com/fr/PersonalCabinet) et à l'adresse électronique que vous aurez communiquée.

Décrivez le problème rencontré avec le plus de détails possible dans le formulaire en ligne. Saisissez les informations suivantes dans les champs obligatoires :

- **Le type de requête**. Sélectionnez la catégorie qui correspond le mieux à votre problème, par exemple "Installation/désinstallation de l'application" ou "Recherche/suppression de virus". Si vous ne trouvez pas le thème qui se rapporte à votre cas, choisissez "Question générale".
- **Le nom et le numéro de version de l'application**.
- **Le texte du message**. Décrivez le problème rencontré avec le plus de détails possibles.
- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement sur le site du service d'assistance technique de Kaspersky Lab.
- **Courrier électronique**. Les experts du service d'assistance technique enverront leurs réponses à cette adresse.

### Assistance technique par téléphone

Si le problème est urgent, vous pouvez téléphoner au service d'assistance technique dans votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.com/fr/support/support_local) ou internationale (http://support.kaspersky.com/fr/support/international) veuillez rassembler toutes les informations (http://support.kaspersky.com/fr/support/details) relatives à votre ordinateur et au logiciel antivirus installé. Nos experts pourront ainsi vous venir en aide plus rapidement.

# INFORMATIONS SUR LE CODE TIERS

Du code développé par des éditeurs tiers a été utilisé pour créer l'application.

### DANS CETTE SECTION DE L'AIDE

Code d'application ..... 83

Autres informations ..... 104

## CODE D'APPLICATION

Informations relatives au code logiciel d'éditeurs tiers utilisé dans le développement de l'application.

## DANS CETTE SECTION DE L'AIDE

BOOST 1.30.0, 1.36 ..... 84

BZIP2/LIBBZIP2 1.0.5 ..... 85

EXPAT 1.2, 2.0.1 ..... 85

FREEBSD LIBC 2.3-2.6 ..... 85

GECKO SDK 1.8 ..... 86

ICU 4.0.1 ..... 92

INFO-ZIP 5.51 ..... 92

LIBJPEG 6B ..... 93

LIBNKFM 2.0.5 ..... 95

LIBPNG 1.2.29 ..... 95

LIBSPF2 1.2.9 ..... 95

LIBUNGIF 3.0 ..... 95

LIBXDR ..... 96

LOKI 0.1.3 ..... 96

LZMA SDK 4.43 ..... 97

MICROSOFT ENTERPRISE LIBRARY 4.1 ..... 97

MICROSOFT VISUAL STUDIO 2008 (MSVCP80.DLL, MSVCR80.DLL) ..... 97

OPENSSL 0,9.8D ..... 97

PCRE 7.4, 7.7 ..... 100

RFC1321-BASED (RSA-FREE) MD5 LIBRARY ..... 101

SPRING.NET 1.2.0 ..... 101

SQLITE 3.6.18 ..... 103

WPF TOOLKIT 3.5.40128.1 ..... 104

ZLIB 1.2, 1.2.3 ..... 104

# BOOST 1.30.0, 1.36



---

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007, Julian R Seward

---

# EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# FREEBSD LIBC 2.3-2.6

Copyright (C) 1992-2005, The FreeBSD Project

---

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# GECKO SDK 1.8

Copyright (C) 1998-2008, Mozilla Foundation

---

Mozilla Public License Version 1,1

1. *Definitions*.

1.0.1. "Commercial Use"

means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

a. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

b. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

gmeans an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. *Source Code License.*

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

a. under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

b. under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

c. the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

d. Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

a. under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

b. under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

c. the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

d. Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. *Distribution Obligations.*

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. *Inability to Comply Due to Statute or Regulation*.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent

version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. *Disclaimer of warranty*

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. *Termination*

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

a. such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

b. any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. *U.S. government end users*

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227,7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. *Miscellaneous*

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. *Responsibility for claims*

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. *Multiple-licensed code*

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

*Exhibit A - Mozilla Public License.*

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of

this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

# ICU 4.0.1

Copyright (C) 1995-2009, International Business Machines Corporation and others

---

ICU License

COPYRIGHT AND PERMISSION NOTICE

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

# INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

---

Info-ZIP license

This is version 2007-Mar-4 of the Info-ZIP license.

The definitive version of this document should be available at

ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely and

a copy at http://www.info-zip.org/pub/infozip/license.html.

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren,

Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further

prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

# LIBJPEG 6B

Copyright (C) 1991-1998, Thomas G. Lane

---

LEGAL ISSUES

==========

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of

CompuServe Incorporated.  GIF(sm) is a Service Mark property of

CompuServe Incorporated."

# LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

---

# LIBPNG 1.2.29

Copyright (C) 2004, 2006-2008, Glenn Randers-Pehrson

---

# LIBSPF2 1.2.9

Copyright (C) 2005, Shevek and Wayne Schlitt

---

The code in the libspf2 distribution is Copyright 2005 by Shevek and Wayne Schlitt, all rights reserved.  Copyright retained for the purpose of protecting free software redistribution.

The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR

IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIESOF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

---

The GIFLIB distribution is Copyright (c) 1997 Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to

use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LIBXDR

Copyright (C) Sun Microsystems, Inc

---

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

# LOKI 0.1.3

Copyright (C) 2001, Andrei Alexandrescu

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# LZMA SDK 4.43

---

# MICROSOFT ENTERPRISE LIBRARY 4.1

Copyright (C) 2008, Microsoft Corporation

---

Distributed under the terms of the Microsoft Public License (Ms-PL).

# MICROSOFT VISUAL STUDIO 2008 (MSVCP80.DLL, MSVCR80.DLL)

Copyright (C) Microsoft Corporation

---

# OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

---

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2006 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit. (http://www.openssl.org/)

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/ ) "

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation

included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

# PCRE 7.4, 7.7



---

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service, Cambridge, England.



THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# RFC1321-BASED (RSA-FREE) MD5 LIBRARY



---

# SPRING.NET 1.2.0



---

Apache License
Version 2,0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own

attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner] Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

# SQLITE 3.6.18

---

# WPF TOOLKIT 3.5.40128.1

Copyright (C) 2010, Microsoft Corporation

---

Distributed under the terms of the Microsoft Public License (Ms-PL)

# ZLIB 1.2, 1.2.3

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

---

# AUTRES INFORMATIONS

Informations supplémentaire sur le code tiers.

La bibliothèque du programme "Agava-C", développée par OOO "R-Alpha", est utilisée pour vérifier une signature numérique.

# 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'étaient pas reprises dans les bases utilisées pour les analyses antérieures, peuvent être ainsi découverts.

### Analyse du trafic

Analyse antivirus et anti-spam en temps réel des messages qui arrivent sur le serveur Microsoft Exchange à l'aide de la version actuelle (la plus récente) des bases de l'Antivirus et de l'Anti-Spam.

## B

### Bases de Kaspersky Security

Bases de données créées par les experts de Kaspersky Lab et qui contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes.

## C

### 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).

### Copie de sauvegarde

Création d'une copie de sauvegarde d'un objet avant son traitement et déplacement de cette copie dans le dossier de sauvegarde. Cette copie pourra être restaurée ultérieurement, envoyée pour examen à Kaspersky Lab ou supprimée.

### Courrier indésirable

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

## D

### Durée de validité de la licence

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. En général, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité de la licence est écoulée, les fonctions de l'application sont réduites : vous ne pourrez plus actualiser les bases de l'application.

## F

### Fichier de licence

Fichier portant l'extension .key et qui est votre " clé " personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans la boîte si vous avez achetez le logiciel chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

## I

### IGNORER L'OBJET

Mode de traitement selon lequel l'objet est ignoré et remis à l'utilisateur sans aucune modification. N'oubliez pas que la sélection de cette action peut entraîner l'infection de l'ordinateur.

### INTERCEPTEUR

Sous-composant du serveur de sécurité chargé d'analyser certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles du déploiement de Microsoft Exchange Server.

## L

### LICENCE COMPLÉMENTAIRE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active parvient à échéance.

### LISTE DES EXPÉDITEURS AUTORISÉS

(également liste blanche des adresses)

Liste des adresses électroniques des messages du courrier entrant qui ne seront pas analysés par l'application de Kaspersky Lab.

### LISTE DES EXPÉDITEURS INTERDITS

(également liste noire des adresses)

Liste des adresses de messagerie électronique bloquées par l'application de Kaspersky Lab, quel que soit le contenu des messages.

### LISTE NOIRE DES LICENCES

Base de données contenant des informations relatives aux fichiers de licence Kaspersky Lab bloquées. Le contenu du fichier de la liste noire est mis à jour en même temps que les bases.

## M

### MISE À JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés sur les serveurs de mise à jour de Kaspersky Lab.

## 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 contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

### OBJET SIMPLE

Corps du message ou pièce jointe simple, par exemple un fichier exécutable. Voir également Objet-conteneur.

### OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus, mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

## P

### POSTE DE TRAVAIL DE L'ADMINISTRATEUR

Ordinateur sur lequel le composant de Kaspersky Security Console d'administration est installé. La configuration et l'administration de la partie serveur de l'application sont réalisées au départ de ce poste à l'aide du composant Serveur de sécurité.

## R

### REMPLACEMENT DE L'OBJET

Mode de traitement de l'objet à l'issue duquel l'objet détecté est remplacé par du texte (corps du message) ou un fichier txt (pièce jointe), créée selon le modèle des remplacements.

### RESTAURATION

Déplacement de la copie de sauvegarde de l'objet depuis le dossier de sauvegarde vers le répertoire désigné par l'administrateur, décodage de l'objet et enregistrement de ce dernier sous le nom spécifié. L'objet restauré aura un format identique au format qu'avait l'objet lorsqu'il a été traité par l'application.

### RÉPARATION D'OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Avant la réparation, une copie de sauvegarde de l'objet est créé, si cette fonctionnalité n'a pas été désactivée. Une partie des données peut être endommagée pendant la réparation. Pour restaurer un objet à son état antérieur, il suffit d'utiliser la copie de sauvegarde de celui-ci.

## 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 anti-spam 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 intercepteur.

### SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

### 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

Mode de traitement d'un objet qui consiste à le supprimer physiquement de votre ordinateur. Ce traitement doit être appliqué aux objets infectés. Avant la suppression une copie de sauvegarde de l'objet est créé, si cette fonctionnalité n'a pas été désactivée. Cette copie vous permettra de restaurer l'objet original.

## V

### VIRUS INCONNU

Nouveau virus au sujet duquel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

# KASPERSKY LAB ZAO

Kaspersky Lab a été fondé en 1997. Il s'agit à l'heure actuelle de l'éditeur russe de logiciels de sécurité polyvalents le plus connu : protection contre les virus, le courrier indésirable et les hackers.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A. 16 autres un doctorat. 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. En qualité de produit phare de la société, Kaspersky Anti-Virus offre une protection efficace pour tous les éléments qui pourraient être la cible d'un virus : postes de travail, serveurs de fichiers, systèmes de messagerie,, pare-feu, passerelles Internet et ordinateurs de poches. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le moteur antivirus de Kaspersky Anti-Virus : Nokia ICG (États-Unis), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en oeuvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab Ltd. Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

| | |
|---|---|
| Site de Kaspersky Lab | http://www.kaspersky.fr |
| Encyclopédie des virus : | http://www.securelist.com/fr/ |
| Laboratoire d'étude des virus : | newvirus@kaspersky.com<br>(envoi uniquement d'objets suspects sous forme d'archive)<br>http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr<br>(pour les questions aux experts antivirus) |

# CONTRAT DE LICENCE

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

## 1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *" Vous "* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *" entité ",* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patchs, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

## 2. Concession de la Licence

2.1. Le Titulaire des droits convient par la présente de Vous accorder une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (" l'utilisation ") du Logiciel sur un nombre spécifié d'Ordinateurs pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la " Licence ") et vous acceptez cette Licence :

Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs précisé dans les licences que vous avez obtenues auprès du Titulaire des droits, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.

2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acquis le Logiciel auprès du Titulaire des droits.

2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

## 3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.

3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone. Si le Titulaire des droits fixe une autre durée pour la période d'évaluation unique applicable, Vous serez informé(e) par notification.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

3.10. Le détenteur des droits se réserve le droit de limiter la possibilité d'activation en dehors de la région dans laquelle le logiciel a été acquis auprès du détenteur des droits et/ou de ses partenaires.

3.11. Si vous avez acheté le logiciel avec un code d'activation valide pour la localisation de la langue parlée dans la région où il a été acquis auprès du détenteur des droits ou de ses partenaires, vous ne pouvez pas activer le logiciel avec le code d'activation prévu pour la localisation d'une autre langue.

3.12. En cas de restrictions précisées dans les clauses 3.10 et 3.11, vous trouverez des informations concernant ces restrictions sur l'emballage et/ou le site Web du détenteur et/ou de ses partenaires.

**4. Assistance technique**

4.1 L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com

**5 Recueil d'informations**

5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.

5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.

5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.

5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

**6. Limitations**

6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.

6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.

6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

7. **Garantie limitée et avis de non-responsabilité**

7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.

7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.

7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

7.6. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LE " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

**8. Exclusion et Limitation de responsabilité**

8.1 DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU

TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

## 9. Licence GNU et autres licences de tierces parties

9.1 Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

## 10. Droits de propriété intellectuelle

10.1 Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des Etats-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

10.2 Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

## 11. Droit applicable ; arbitrage

Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 11 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

**12. Délai de recours.**

12.1 Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

**13. Intégralité de l'accord ; divisibilité ; absence de renoncement.**

13.1 Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en equity de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

**14. Informations de contact du Titulaire des droits**

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com

# INDEX

## A


Ajout d'un serveur ..... 38
Analyse en arrière-plan ..... 51
Anti-Spam
- facteur de courrier indésirable potentiel ..... 59
- importation de la liste des expéditeurs autorisés ..... 55
- liste blanche ..... 55
- liste des expéditeurs autorisés ..... 55
- liste des expéditeurs interdits ..... 55
- liste noire ..... 55
- niveau d'agressivité ..... 54


## B


Barre d’outils ..... 32


## C


Clusters ..... 18
Composants de l'application ..... 15
CONTRAT DE LICENCE ..... 110


## D


Diagnostic ..... 78


## E


EICAR ..... 25
Exclusions ..... 49


## F


Fenêtre principale ..... 32
- Arborescence de la console ..... 32


## I


INSTALLATION DE L'APPLICATION ..... 19
INTERFACE DE L'APPLICATION ..... 32


## J


JOURNAL DES ÉVÉNEMENTS ..... 78


## K


KASPERSKY LAB ..... 109


## L


Lancement
- Console d'administration ..... 38

Liste blanche
- Anti-Spam ..... 55

Liste noire
- Anti-Spam ..... 55

## M

MISE À JOUR ..... 41

## N

NOTIFICATIONS ..... 69

## P

Pièces jointes ..... 49
Protection des banques ..... 31
Protection des boîtes aux lettres ..... 31
Protection des dossier partagés ..... 31

## R

RAPPORTS ..... 71

## S

Sauvegarde
    consultation des données des copies de sauvegarde ..... 64
    purge de la banque ..... 67
Serveur de sécurité ..... 15

## V

Vérification du fonctionnement ..... 25