

Kaspersky Anti-Virus 6.0 for Windows Servers MP4

MANUEL DE L'UTILISATEUR

VERSION DE L'APPLICATION : 6.0 MP4 CRITICAL FIX 1



KASPERSKY lab

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que cette documentation vous sera utile et qu'elle répondra à la majorité des questions que vous pourriez avoir sur le logiciel.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et informatives.

Il peut être modifié sans préavis. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse <http://www.kaspersky.fr/docs>.

Kaspersky Lab ne pourra être tenue responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Ce document fait référence aux autres noms et aux marques déposés qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 24/02/10

© 1997-2010 Kaspersky Lab ZAO. Tous droits réservés.

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

TABLE DES MATIERES

INTRODUCTION.....	9
Distribution.....	9
Contrat de licence.....	9
Services pour les utilisateurs enregistrés.....	10
Configuration matérielle et logicielle requises.....	10
KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS WORKSTATIONS MP4.....	11
Obtention d'informations sur l'application.....	11
Sources d'informations pour les recherches indépendantes.....	11
Contacter le service commercial.....	12
Contacter le service du Support Technique.....	12
Forum sur les applications de Kaspersky Lab.....	13
Nouveautés de Kaspersky Anti-Virus 6.0 for Windows Servers MP4.....	13
Configuration de la protection.....	14
Antivirus Fichiers.....	14
Tâches de recherche d'éventuels virus.....	14
Mise à jour.....	15
Fonctions de service de l'application.....	15
INSTALLATION DE KASPERSKY ANTI-VIRUS 6.0.....	17
Installation à l'aide de l'Assistant d'installation.....	17
Etape 1. Vérification des configurations minimum requises pour l'installation de Kaspersky Anti-Virus.....	18
Etape 2. Fenêtre d'accueil de la procédure.....	18
Etape 3. Lecture du Contrat de licence.....	18
Etape 4. Sélection du répertoire d'installation.....	18
Etape 5. Utilisation des paramètres de l'application conservés de l'installation antérieure.....	19
Etape 6. Sélection du type d'installation.....	19
Etape 7. Sélection des composants de l'application à installer.....	19
Etape 9. Recherche d'autres logiciels antivirus.....	20
Etape 10. Derniers préparatifs pour l'installation de l'application.....	20
Etape 11. Fin de la procédure d'installation.....	20
Installation de l'application via la ligne de commande.....	21
Procédure d'installation via l'Editeur d'objets de stratégie de groupe (Group Policy Object).....	21
installation de l'application.....	21
Description des paramètres du fichier setup.ini.....	22
Mise à jour de la version de l'application.....	22
Suppression de l'application.....	23
PREMIERE UTILISATION.....	24
Assistant de configuration initiale.....	24
Utilisation des objets sauvegardés de la version précédente.....	25
Activation de l'application.....	25
Activation en ligne.....	26
Activation de la version d'évaluation.....	26
Activation à l'aide du fichier de licence.....	26
Fin de l'activation.....	27
Configuration de la mise à jour.....	27

Programmation de la recherche de virus.....	27
Restriction de l'accès à l'application.....	28
Fin de l'Assistant de configuration.....	28
Recherche de virus sur l'ordinateur	28
Mise à jour de l'application.....	29
Administration des licences	29
Administration de la sécurité.....	30
Suspension de la protection.....	31
Suppression des problèmes. Service d'assistance technique aux utilisateurs.....	32
Création d'un fichier de trace	32
Configuration des paramètres de l'application	33
Rapports sur le fonctionnement de l'application. Rapports.....	33
INTERFACE DE L'APPLICATION.....	34
Icône dans la zone de notification de la barre des tâches	34
Menu contextuel	35
Fenêtre principale de l'application.....	36
Notifications	37
Fenêtre de configuration des paramètres de l'application.....	38
PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS DE L'ORDINATEUR.....	39
Algorithme de fonctionnement du composant.....	40
Modification du niveau de protection	41
Modification de l'action à réaliser sur les objets identifiés.....	41
Constitution de la zone de protection.....	42
Utilisation de l'analyse heuristique	43
Optimisation de l'analyse	44
Analyse des fichiers composés.....	44
Analyse des objets composés de grande taille.....	45
Modification du mode d'analyse.....	45
Technologie d'analyse	46
Suspension du composant : programmation.....	46
Suspension du composant : composition de la liste des applications.....	46
Restauration des paramètres de protection par défaut.....	47
Statistiques de la protection des fichiers.....	47
Réparation différée des objets	48
RECHERCHE DE VIRUS SUR LE SERVEUR.....	49
Lancement de la recherche d'éventuels virus.....	50
Composition de la liste des objets à analyser	51
Modification du niveau de protection	52
Modification de l'action à exécuter après la découverte d'une menace	53
Modification du type d'objets à analyser	54
Optimisation de l'analyse	54
Analyse des fichiers composés.....	55
Modification de la méthode d'analyse	55
Technologie d'analyse	56
Performances de l'ordinateur pendant l'exécution des tâches	57
Suspension de la tâche : programmation.....	57
Suspension du composant : composition de la liste des applications.....	58
Mode de lancement : configuration du compte utilisateur	58

Mode de lancement : programmation	58
Particularité du lancement programmé des tâches de l'analyse	59
Statistiques de recherche d'éventuels virus	59
Définition de paramètres d'analyse uniques pour toutes les tâches	60
Restauration des paramètres d'analyse par défaut.....	60
MISE A JOUR DE L'APPLICATION	61
Lancement de la mise à jour	62
Annulation de la dernière mise à jour.....	63
Sélection de la source de mises à jour	63
Paramètres régionaux.....	64
Utilisation du serveur proxy.....	64
Mode de lancement : configuration du compte utilisateur	65
Mode de lancement : programmation	65
Sélection de l'élément à actualiser.....	66
Modification du mode de lancement de la tâche de mise à jour	66
Mise à jour depuis un répertoire local	67
Statistiques de la mise à jour	68
Problèmes possibles lors de la mise à jour.....	68
CONFIGURATION DES PARAMETRES DE L'APPLICATION	72
Protection.....	73
Désactivation/activation de la protection de l'ordinateur.....	74
Lancement de l'application au démarrage du système d'exploitation	74
Sélection des catégories de menaces identifiées.....	74
Constitution de la zone de confiance	75
Création d'une règle d'exclusion.....	75
Masques autorisés pour l'exclusion des fichiers	76
Masques d'exclusion autorisés selon le classement de l'encyclopédie des virus	77
Composition de la liste des applications de confiance.....	78
Exportation / importation des composants de la zone de confiance	78
Exportation et importation des paramètres de fonctionnement de Kaspersky Anti-Virus	79
Restauration des paramètres par défaut.....	79
Antivirus Fichiers	80
Analyse	80
Mise à jour	81
Paramètres	81
Autodéfense du logiciel	82
Restriction de l'accès à l'application.....	82
Restriction de taille des fichiers iSwift	83
Poste serveur multiprocesseur.....	83
Notifications relatives aux événements de Kaspersky Anti-Virus	84
Sélection du type d'événement et de mode d'envoi des notifications	85
Configuration de l'envoi des notifications par courrier électronique.....	85
Configuration des paramètres du journal des événements	86
Eléments actifs de l'interface.....	86
Rapports et Stockages.....	87
Principes d'utilisation des rapports	87
Configuration des paramètres du rapport.....	88
Quarantaine pour les objets potentiellement infectés.....	88

Manipulation des objets en quarantaine.....	89
Copie de sauvegarde des objets dangereux.....	89
Manipulation des copies de sauvegarde.....	90
Configuration de la quarantaine et du dossier de sauvegarde.....	90
DISQUE DE DEPANNAGE.....	90
Création d'un disque de dépannage.....	91
Etape 1. Sélection de la source de l'image du disque.....	92
Etape 2. Copie (téléchargement) de l'image du disque.....	92
Etape 3. Mise à jour de l'image du disque.....	92
Etape 4. Chargement de l'ordinateur distant.....	93
Etape 5. Fin de l'Assistant.....	93
Démarrage de l'ordinateur à l'aide du disque de dépannage.....	93
Utilisation de Kaspersky Rescue Disk au départ de la ligne de commande.....	95
Recherche de virus.....	96
Mise à jour de Kaspersky Anti-Virus.....	97
Annulation de la dernière mise à jour.....	97
Consultation de l'aide.....	98
VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY ANTI-VIRUS.....	99
Virus d'essai "EICAR" et ses modifications.....	99
Vérification de l'exactitude de la configuration d'Antivirus Fichiers.....	100
Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus.....	101
TYPES DE MESSAGE.....	102
Un objet suspect a été détecté.....	102
La réparation de l'objet est impossible.....	103
Un objet suspect a été détecté.....	103
UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE.....	105
Consultation de l'aide.....	106
Recherche de virus.....	106
Mise à jour de l'application.....	108
Annulation de la dernière mise à jour.....	109
Lancement / arrêt d'Antivirus Fichiers ou d'une tâche.....	109
Statistiques du fonctionnement du composant ou de la tâche.....	110
Exportation des paramètres de protection.....	111
Importation des paramètres de protection.....	111
Activation de l'application.....	111
Restauration du fichier de la quarantaine.....	112
Arrêt de l'application.....	112
Obtention du fichier de trace.....	112
Codes de retour de la ligne de commande.....	113
MODIFICATION, REPARATION OU SUPPRESSION DE L'APPLICATION.....	114
Modification, réparation ou suppression du logiciel à l'aide d'assistant d'installation.....	114
Etape 1. Fenêtre d'accueil du programme d'installation.....	114
Etape 2. Sélection de l'opération.....	115
Etape 3. Fin de la réparation, de la modification ou de la suppression du logiciel.....	115
Procédure de suppression de l'application via la ligne de commande.....	116
ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT.....	117
Administration du logiciel.....	119

Lancement et arrêt de l'application.....	120
Configuration des paramètres de l'application	121
Configuration des paramètres spécifiques	122
Analyse antivirus des fichiers.....	124
Lancement et arrêt des tâches.....	125
Création d'une tâche	125
Assistant pour la création d'une tâche locale	126
Etape 1. Saisie des données générales sur la tâche	126
Etape 2. Sélection de l'application et du type de tâche.....	126
Etape 3. Configuration des paramètres du type de tâche sélectionné.....	127
Etape 4. Configuration de la programmation	127
Etape 5. Fin de la création d'une tâche	127
Configuration des tâches.....	127
Administration des stratégies.....	129
Création d'une stratégie	129
Assistant pour la création d'une stratégie.....	130
Etape 1. Saisie des données générales sur la stratégie	130
Etape 2. Sélection de l'état de la stratégie.....	130
Etape 3. Importation des paramètres de l'application	130
Etape 4. Configuration des paramètres de protection	130
Etape 5. Configuration de la protection par un mot de passe.....	131
Etape 6. Configuration de la zone de confiance	131
Etape 7. Configuration des paramètres d'interaction avec l'utilisateur.....	131
Etape 8. Fin de la création d'une stratégie	131
Configuration de la stratégie	132
UTILISATION D'UN CODE TIERS	134
Bibliothèque Boost-1.30.0.....	135
Bibliothèque LZMA SDK 4.40, 4.43	135
Bibliothèque Windows Template Library 7.5.....	135
Bibliothèque Windows Installer XML (WiX) toolset 2.0	136
Bibliothèque ZIP-2.31	139
Bibliothèque ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3	140
Bibliothèque UNZIP-5.51	140
Bibliothèque LIBPNG-1.0.1, LIBPNG-01/02/08, LIBPNG-01/02/12	141
Bibliothèque LIBJPEG-6B.....	143
Bibliothèque LIBUNGIF-04/01/04	145
Bibliothèque MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.....	145
Bibliothèque MD5 MESSAGE-DIGEST ALGORITHM-V. 18/11/04.....	145
Bibliothèque INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04/11/99.....	145
Bibliothèque CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02/11/04.....	146
Bibliothèque COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum	146
Bibliothèque PLATFORM INDEPENDENT IMAGE CLASS.....	146
Bibliothèque FLEX PARSER (FLEXLEXER)-V. 1993.....	147
Bibliothèque ENSURECLEANUP, SWMRG, LAYOUT-V. 2000	147
Bibliothèque STDSTRING- V. 1999.....	148
Bibliothèque T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006	148
Bibliothèque NTSERVICE- V. 1997	149
Bibliothèque SHA-1-1.2	149

Bibliothèque COCOA SAMPLE CODE- V. 18/07/07.....	150
Bibliothèque PUTTY SOURCES-25/09/08.....	150
Autre information	151
GLOSSAIRE.....	152
CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB.....	159
KASPERSKY LAB.....	165
INDEX	166

INTRODUCTION

DANS CETTE SECTION

Distribution	9
Services pour les utilisateurs enregistrés	10
Configuration matérielle et logicielle requises	10

DISTRIBUTION

Vous pouvez acheter Kaspersky Anti-Virus chez nos partenaires (version en boîte) ou en ligne (par exemple, <http://www.kaspersky.fr>, rubrique **Boutique en ligne**).

Si vous achetez le logiciel en boîte, vous recevrez :

- Une enveloppe cachetée contenant le cédérom d'installation avec les fichiers du logiciel et la documentation au format .pdf.
- La version "papier" du guide de l'utilisateur (si cette option avait été incluse dans la commande) ou du guide du logiciel.
- Le fichier de licence de l'application sur une disquette spéciale.
- Une carte d'inscription (reprenant le numéro de série du logiciel).
- Le contrat de licence.

Avant d'ouvrir l'enveloppe contenant le cédérom (ou les disquettes), veuillez lire attentivement le contrat de licence.

Si vous achetez Kaspersky Anti-Virus en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce guide. Le fichier de licence vous sera envoyé par courrier électronique après le paiement.

CONTRAT DE LICENCE

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

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez rendre la boîte avec le logiciel au magasin où vous l'avez acheté en échange du remboursement intégral. Dans ce cas, l'enveloppe contenant le cédérom ou les disquettes ne peut avoir été ouverte.

L'ouverture de l'enveloppe contenant le cédérom (ou les disquettes) d'installation marque votre accord avec les termes du 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/subscribe/>).

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.

CONFIGURATION MATERIELLE ET LOGICIELLE REQUISES

Pour garantir le fonctionnement normal de Kaspersky Anti-Virus 6.0, l'ordinateur doit répondre aux exigences minimales suivantes :

Recommandations d'ordre général :

- 300 Mo d'espace disponible sur le disque dur.
- Microsoft Internet Explorer 6.0 ou suivant (pour la mise à jour des bases et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0 minimum (ou similaire).

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Processeur Intel Pentium 400 Mhz 32 bits (x86) / 64-bit (x64) minimum (ou similaire).
- 512 Mo de mémoire vive disponible.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 ou similaire), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 ou similaire), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Processeur Intel Pentium 800 Mhz 32 bits (x86) / 64-bit (x64) minimum ou similaire (ou analogue).
- 1 Go de mémoire vive disponible.

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS WORKSTATIONS MP4

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 - représente la nouvelle génération de solution de protection des données.

DANS CETTE SECTION

Obtention d'informations sur l'application	11
Nouveautés de Kaspersky Anti-Virus 6.0 for Windows Servers MP4	13
Configuration de la protection.....	14

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Anti-Virus, vous pouvez trouver la réponse rapidement.

Kaspersky Lab offre diverses sources d'informations sur l'application. Parmi elles, vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

Sources d'informations pour les recherches indépendantes	11
Contacteur le service commercial	12
Contacteur le service du Support Technique.....	12
Forum sur les applications de Kaspersky Lab	13

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez consulter les sources d'informations suivantes sur l'application :

- La page de l'application sur le site de Kaspersky Lab ;
- La 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 Web de Kaspersky Lab

http://www.kaspersky.com/fr/anti-virus_windows_server

Sur cette page vous allez retrouver les informations générales sur l'application, ses possibilités et ses particularités.

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

<http://support.kaspersky.com/fr/corporate/index.php?Cible=1>

Cette page propose des articles publiés par les experts du service d'assistance technique.

Ces articles proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. Ils sont regroupés par thèmes tels que "Manipulation des licences", "Configuration des mises à jour des bases" ou "Résolution de problèmes". Les articles peuvent répondre à des questions en rapport non seulement avec l'application mais également en rapport avec d'autres applications de Kaspersky Lab ; ils peuvent également fournir des nouvelles sur le service d'assistance technique dans son ensemble.

Système d'aide électronique

La distribution de l'application reprend le fichier d'aide complète et contextuelle qui contient les informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, analyse de divers secteurs de l'ordinateur, exécution d'autres tâches ainsi que les informations relatives à chaque fenêtre de l'application : description des paramètres qui figurent dans chacune d'entre elles et liste des tâches exécutées.

Pour ouvrir le fichier d'aide, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse ou sur la touche **<F1>** du clavier.

Documentation

Le document **Manuel de l'utilisateur** (au format pdf) fait partie de l'installation de Kaspersky Anti-Virus. Ce document contient une description des fonctions et des possibilités de l'application ainsi que des principaux algorithmes de fonctionnement.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, l'achat de Kaspersky Anti-virus ou le renouvellement de la licence, vous pouvez contacter notre service Commercial par courrier électronique en écrivant à :

info@fr.kaspersky.com

ou consulter notre boutique en ligne :

- Petites Entreprises : http://kaspersky.telechargement.fr/cata_tpe.html
- PME / Grands Comptes : <http://kaspersky.telechargement.fr/entreprises.html>

CONTACTER LE SERVICE DU SUPPORT TECHNIQUE

Si vous avez déjà acheté Kaspersky Anti-Virus, vous pouvez obtenir des renseignements sur cette application auprès du Support Technique, par téléphone ou via Internet.

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et, en cas d'infection de votre ordinateur, ils vous aideront à surmonter 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>).

Assistance technique par téléphone

Si le problème est urgent, vous pouvez contacter le service d'assistance technique dans votre ville. Si vous contactez l'assistance technique russe (http://support.kaspersky.ru/support/support_local) ou internationale (<http://support.kaspersky.ru/support/international>) veuillez fournir l'information

(<http://support.kaspersky.com/support/details>) sur votre ordinateur et l'application antivirus installée. Ceci permettra à nos experts de vous venir en aide le plus vite possible.

FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

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.com>.

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

NOUVEAUTES DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4

Kaspersky Anti-Virus 6.0 - est un outil universel de protection des informations. Voici une liste détaillées des nouveautés introduites dans Kaspersky Anti-Virus 6.0.

Nouveautés au niveau de la protection :

- Le nouveau noyau antivirus sur lequel repose Kaspersky Anti-Virus est plus efficace dans la découverte des programmes malveillants. Il garantit également une accélération sensible de la recherche d'éventuels virus dans le système. Ces résultats sont obtenus grâce au traitement amélioré des objets et à l'optimisation de l'utilisation des ressources de l'ordinateur (en particulier la plate-forme à base de deux et quatre processeurs).
- Introduction d'un nouvel analyseur heuristique qui permet d'identifier et de bloquer les programmes malveillants inconnus de manière plus efficace. Si la signature d'un programme ne figure pas dans les bases de Kaspersky Anti-Virus, l'analyseur heuristique imite son exécution dans un milieu virtuel isolé. Cette méthode est inoffensive et permet d'analyser toutes les actions du programme avant qu'il ne soit exécuté en milieu réel.
- La procédure de mise à jour de l'application a été améliorée: désormais, le redémarrage de l'ordinateur est rarement nécessaire.

Nouveautés au niveau de l'interface :

- L'interface permet un accès simple et convivial à n'importe quel composant de l'application.
- L'interface tient compte des besoins des administrateurs de petits réseaux ou de réseaux de grandes entreprises.

Nouveautés dans l'utilisation avec Kaspersky Administration Kit :

- Kaspersky Administration Kit assure une administration simple et conviviale du système de défense antivirus d'une entreprise. L'application est capable d'assurer l'administration centralisée de la protection d'un réseau d'entreprise de n'importe quelle taille, comptant plusieurs dizaines de milliers de nœuds, dont des utilisateurs distants et nomades.
- Installation distante de l'application avec la dernière version des bases.
- Amélioration de l'utilisation distante de l'application (révision de la structure des stratégies).
- Possibilité de créer la stratégie sur la base d'un fichier de configuration.
- Ajout de paramètres spécifiques aux utilisateurs mobiles dans la configuration des tâches de mise à jour.
- Possibilité d'exclure provisoirement des ordinateurs clients équipés de l'application du champ d'action de stratégies et tâches de groupe (après introduction d'un mot de passe).

CONFIGURATION DE LA PROTECTION

La protection offerte par Kaspersky Anti-Virus for Windows Servers comprend :

- L'Antivirus Fichiers (cf. page [14](#)) qui contrôle en temps réel les objets du système de fichiers de l'ordinateur.
- Des tâches d'analyse antivirus (cf. page [14](#)) qui procède à la recherche d'éventuels virus dans l'ordinateur ou dans des fichiers, des répertoires, des disques ou des secteurs particuliers.
- La mise à jour (cf. page [15](#)), garantit l'actualité des modules internes de l'application et des bases utilisées pour la recherche des programmes malveillants.
- Des services (cf. section "Services du programme" à la page [15](#)), qui garantissent le soutien information dans le cadre de l'utilisation du logiciel et permettent d'en élargir les fonctions.

ANTIVIRUS FICHIERS

La protection du serveur est assurée par l'Antivirus Fichiers.

Le système de fichiers peut contenir des virus et d'autres programmes dangereux. Les programmes malveillants peuvent rester des années dans le système de fichiers de votre ordinateur sans jamais se manifester. Il suffit cependant d'ouvrir le fichier infecté pour qu'il se réveille.

L'Antivirus Fichiers est le composant qui contrôle le système de fichiers de l'ordinateur. Il analyse tous les fichiers ouverts, exécutés et enregistrés sur l'ordinateur et tous les disques connectés. Chaque requête adressée au fichier est interceptée par Kaspersky Anti-Virus et le logiciel recherche la présence éventuelle de virus dans le fichier. Il sera possible de continuer à utiliser le fichier uniquement si celui-ci est sain ou s'il a pu être réparé par l'application. Si le fichier ne peut pas être réparé pour une raison quelconque, il sera supprimé (dans ce cas, une copie du fichier est placée dans le dossier de sauvegarde) ou mis en quarantaine.

TACHES DE RECHERCHE D'EVENTUELS VIRUS

En plus de la protection à l'aide de l'Antivirus Fichiers, il est important de procéder régulièrement à une analyse antivirus du serveur. Cette activité est indispensable afin d'éviter la propagation de programmes malveillants qui n'auraient pas été interceptés par l'Antivirus Fichiers en raison d'un niveau de protection trop bas ou de tout autre motif.

Kaspersky Anti-Virus prévoit les tâches suivantes pour l'analyse antivirus :

Analyse

Analyse des objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.

Analyse complète

Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.

Analyse rapide

Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

MISE A JOUR

Afin d'être toujours prêt à neutraliser tout virus ou programme malveillant, à intercepter le courrier indésirable, il faut veiller à ce que Kaspersky Anti-Virus for Windows Servers soit toujours à jour. Le composant **Mise à jour** a été conçu à cette fin. Il est chargé de la mise à jour des bases et des modules de l'application utilisés.

Le service de copie des mises à jour permet d'enregistrer la mise à jour des bases et des modules de l'application obtenue depuis les serveurs de Kaspersky Lab dans un répertoire local en vue de les partager avec les autres ordinateurs et ce, afin d'économiser la bande passante.

FONCTIONS DE SERVICE DE L'APPLICATION

Kaspersky Anti-Virus propose divers services. Ces fonctions visent à maintenir l'application à jour, à élargir les possibilités d'utilisation et à faciliter l'utilisation.

Rapports

Un rapport est constitué pour chaque composant, chaque tâche d'analyse antivirus ou chaque mise à jour de l'application. Ce rapport contient les informations relatives aux opérations exécutées et à leurs résultats. Vous pourrez toujours vérifier en détail le fonctionnement de n'importe quel composant de Kaspersky Anti-Virus. Si un problème survient, il est possible d'envoyer les rapports à Kaspersky Lab où ils seront étudiés en détails par nos spécialistes qui tenteront de vous aider le plus vite possible.

Kaspersky Anti-Virus déplacent tous les objets suspects du point de vue de la sécurité dans un répertoire spécial : la *Quarantaine*. Ces objets sont chiffrés, ce qui permet d'éviter l'infection de l'ordinateur. Ces objets pourront être soumis à une analyse antivirus, restaurés dans leur emplacement d'origine, supprimés ou ajoutés indépendamment dans la quarantaine. Tous les objets jugés sains après l'analyse sont automatiquement restaurés dans leur emplacement d'origine.

Le *dossier de sauvegarde* contient les copies des objets réparés ou supprimés par le programme. Ces copies sont créées au cas où il faudra absolument restaurer l'objet ou le scénario de son infection. Les copies de sauvegarde des objets sont également chiffrées afin d'éviter l'infection de l'ordinateur.

Il est possible de restaurer l'objet au départ de la copie de sauvegarde vers son emplacement d'origine ou de la supprimer.

Disque de dépannage

Le disque de dépannage est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.

Licence

Au moment d'acheter Kaspersky Antivirus, vous et Kaspersky Lab signez un contrat de licence qui vous donne le droit d'utiliser l'application, de recevoir les mises à jour des bases de l'application et de contacter le service d'assistance technique durant une période déterminée. La durée d'utilisation ainsi que toute autre information requise pour le fonctionnement de l'application figurent dans la licence.

Grâce à la fonction **Licence**, vous pouvez obtenir des informations détaillées sur la licence que vous utilisez ainsi qu'acheter une nouvelle licence ou renouveler la licence en cours.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Anti-Virus ont accès au service d'assistance technique. Utilisez la fonction **Assistance technique** pour savoir où vous pouvez obtenir l'assistance technique dont vous avez besoin.

Les liens proposés vous permettent d'accéder au forum des utilisateurs des produits de Kaspersky Lab, de consulter la liste des questions fréquemment posées et de trouver peut-être la solution à votre problème dans les réponses fournies. De plus, vous pouvez envoyer au service d'assistance technique des messages relatifs à des erreurs ou des commentaires sur le fonctionnement du logiciel en remplissant un formulaire spécial sur le site Web de Kaspersky Lab.

Vous avez également accès à l'assistance technique en ligne et nos collaborateurs sont bien sûr toujours prêts à vous aider dans votre utilisation de Kaspersky Anti-Virus par téléphone.

INSTALLATION DE KASPERSKY ANTI-VIRUS 6.0

Il existe plusieurs méthodes pour installer Kaspersky Anti-Virus 6.0 for Windows Servers MP4 sur un ordinateur :

- Installation locale : installation de l'application sur un ordinateur individuel. L'installation de ce type requiert un accès direct à cet ordinateur. L'installation locale peut être réalisée selon deux modes :
 - Le mode interactif à l'aide de l'Assistant d'installation de l'application (cf. chapitre "Installation à l'aide de l'Assistant d'installation" à la page [17](#)) ; ce mode requiert l'intervention de l'utilisateur tout au long de la procédure ;
 - Le mode autonome : l'installation est lancée via la ligne de commande et elle ne requiert pas l'intervention de l'utilisateur (cf. chapitre "Installation de l'application via la ligne de commande" à la page [21](#)).
- Installation à distance : installation de l'application sur les ordinateurs du réseau réalisée à distance depuis le poste de travail de l'administrateur à l'aide de :
 - La suite logicielle Kaspersky Administration Kit (cf. "Guide de déploiement de Kaspersky Administration Kit") ;
 - Stratégies de domaines de groupe de Microsoft Windows Server 2000/2003 (cf. chapitre "Procédure d'installation via l'Editeur d'objets de stratégie de groupe (Group Policy Object)" à la page [21](#)).

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

DANS CETTE SECTION

Installation à l'aide de l'Assistant d'installation.....	17
Installation de l'application via la ligne de commande	21
Procédure d'installation via l'Editeur d'objets de stratégie de groupe (Group Policy Object)	21

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

Pour installer Kaspersky Anti-Virus sur votre ordinateur, exécutez le fichier de distribution repris sur le cédérom d'installation.

L'installation de l'application au départ d'une distribution téléchargée depuis Internet est identique à l'installation depuis le cédérom.

Le programme d'installation se présente sous la forme d'un Assistant. Chaque fenêtre contient une sélection de boutons qui permettent d'administrer le processus d'installation. Voici une brève description de leur fonction :

- **Suivant** : exécute l'action et passe à l'étape suivante de l'installation.
- **Précédent** : revient à l'étape précédente de l'installation.
- **Annuler** : annule l'installation du logiciel.

- **Terminer** : termine la procédure d'installation de l'application.

Examinons en détail chacune des étapes de la procédure d'installation du paquet.

ETAPE 1. VERIFICATION DES CONFIGURATIONS MINIMUM REQUISES POUR L'INSTALLATION DE KASPERSKY ANTI-VIRUS

Avant d'installer l'application, le programme vérifie si le système d'exploitation et les Services Packs installés correspondent à la configuration requise pour l'installation de Kaspersky Anti-Virus. Le système vérifie également si l'ordinateur est doté des programmes requis et si vous jouissez des privilèges nécessaires pour réaliser l'installation.

Si une des conditions n'est pas remplie, le message de circonstance apparaîtra. Il est conseillé d'installer tous les Service Pack à l'aide du service **Windows Update** ainsi que les programmes requis avant de lancer l'installation de Kaspersky Anti-Virus.

ETAPE 2. FENETRE D'ACCUEIL DE LA PROCEDURE

Si la configuration du système correspond aux exigences, une fenêtre d'accueil apparaîtra directement après l'exécution du fichier d'installation. Cette fenêtre contient des informations relatives au début de l'installation de Kaspersky Anti-Virus sur l'ordinateur.

Pour poursuivre l'installation, cliquez sur **Suivant**. Pour annuler l'installation, cliquez sur le bouton **Annuler**.

ETAPE 3. LECTURE DU CONTRAT DE LICENCE

Cette fenêtre de l'Assistant d'installation contient le Contrat de licence qui est conclu entre vous et Kaspersky Lab. Lisez-le attentivement et si vous n'avez aucune objection à formuler, sélectionnez l'option **J'accepte les termes du contrat de licence** puis cliquez sur **Suivant**. L'installation se poursuit.

Pour arrêter l'installation, cliquez sur le bouton **Annuler**.

ETAPE 4. SELECTION DU REPERTOIRE D'INSTALLATION

L'étape suivante de l'installation de Kaspersky Anti-Virus consiste à déterminer le répertoire de l'ordinateur dans lequel l'application sera installée. Le chemin proposé par défaut est le suivant :

- <Disque> → **Program Files** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – pour les systèmes 32 bits.
- <Disque> → **Program Files (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – pour les systèmes 64 bits.

Vous pouvez choisir un autre dossier à l'aide du bouton **Parcourir** qui ouvre la fenêtre standard de sélection de dossier ou saisir le chemin d'accès dans le champ prévu à cet effet.

N'oubliez pas que si vous saisissez manuellement le chemin d'accès complet au dossier d'installation, le nom ne pourra pas compter plus de 200 caractères ni contenir des caractères spéciaux.

Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 5. UTILISATION DES PARAMETRES DE L'APPLICATION CONSERVES DE L'INSTALLATION ANTERIEURE

Cette étape vous permet de décider si vous souhaitez utiliser les paramètres de protection et les bases de l'application, si elles ont été préservées sur le serveur, lors de la suppression de la version antérieure de Kaspersky Anti-Virus 6.0.

Examinons en détail la manière d'utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Anti-Virus était installée sur l'ordinateur et que lors de sa suppression, vous avez conservé les bases de l'application, vous pouvez les activer en vue d'une utilisation avec la nouvelle version installée. Pour ce faire, cochez la case **Bases de l'application**. Les bases de l'application reprises dans la distribution ne seront pas copiées sur le serveur.

Pour utiliser les paramètres de protection configurés dans la version antérieure et préservés sur l'ordinateur, cochez la case **Paramètres de fonctionnement de l'application**.

ETAPE 6. SELECTION DU TYPE D'INSTALLATION

Cette étape vous permet de définir l'ampleur de l'installation que vous souhaitez réaliser sur l'ordinateur. Il existe deux types d'installation :

Complète. Dans ce cas, tous les composants de Kaspersky Anti-Virus sont installés sur le serveur. Pour connaître la suite de l'installation, passez à l'Etape 8.

Personnalisée. Dans ce cas, vous devrez choisir les composants de l'application que vous souhaitez installer sur le serveur. Pour de plus amples informations, consultez l'Etape 7.

Cliquez sur le bouton correspondant au type d'installation que vous souhaitez réaliser.

ETAPE 7. SELECTION DES COMPOSANTS DE L'APPLICATION A INSTALLER

Cette étape est présente uniquement si vous choisissez l'installation de type **Personnalisée**.

Dans ce type d'installation, vous devez composer la liste des composants de Kaspersky Anti-Virus que vous souhaitez installer. Le composant Antivirus Fichiers, le composant de recherche de virus et le connecteur à l'agent d'administration pour l'administration à distance de l'application via Kaspersky Administration Kit sont sélectionnés par défaut pour l'installation.

Pour sélectionner un composant en vue de l'installation, il faut cliquer avec le bouton gauche de la souris sur l'icône située à côté du nom du composant et sélectionnez l'option **Le composant sera installé sur le disque dur local** dans le menu contextuel. Pour en savoir plus sur le type de protection offert par le composant sélectionné et l'espace requis pour son installation, lisez les informations reprises dans la partie inférieure de cette fenêtre du programme d'installation.

Pour obtenir des informations détaillées sur l'espace disponible sur les disques durs de votre ordinateur, cliquez sur le bouton **Disque**. Les informations seront proposées dans une nouvelle fenêtre.

Si vous ne souhaitez pas installer un composant, sélectionnez l'option **Le composant sera inaccessible** dans le menu contextuel. N'oubliez pas qu'en annulant l'installation d'un composant quelconque, vous vous privez de la protection contre toute une série de programmes dangereux.

Une fois que la sélection des composants est terminée, cliquez sur le bouton **Suivant**. Pour revenir à la liste des composants à installer par défaut, cliquez sur le bouton **Abandon**.

ETAPE 9. RECHERCHE D'AUTRES LOGICIELS ANTIVIRUS

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation simultanée avec Kaspersky Anti-Virus pourrait entraîner des conflits.

Si de tels programmes existent sur le serveur, une liste reprenant leur nom s'affichera. Vous serez invité à les supprimer avant de poursuivre l'installation.

Sous la liste des logiciels antivirus découverts, vous pouvez choisir de les supprimer automatiquement ou manuellement (seulement les produits de Kaspersky Lab seront supprimés automatiquement).

Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 10. DERNIERS PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Lors de cette étape, vous êtes invité à réaliser les derniers préparatifs pour l'installation de l'application sur le serveur.

En cas d'installation initiale de Kaspersky Anti-Virus 6.0, il est déconseillé de désélectionner la case **Protéger l'installation de l'application**. L'activation de la protection des modules permet, en cas d'erreur lors de l'installation, de réaliser la procédure correcte de remise à l'état antérieur. En cas de nouvelle tentative d'installation, il est conseillé de désélectionner cette case.

En cas d'installation à distance via **Windows Bureau distant**, il est conseillé de désélectionner la case **Protéger l'installation de l'application**. Dans le cas contraire, l'installation pourrait ne pas se dérouler ou pourrait se solder sur des erreurs.

Si vous voulez que les exclusions, recommandées par Microsoft pour les serveurs, soient automatiquement ajoutées dans les exclusions, cochez la case **Exclure les exclusions définies par Microsoft**.

Si vous voulez, qu'après l'installation le chemin d'accès à avp.com a été ajouté dans la variable système %PATH%, cochez la case **Ajouter le chemin d'accès à la variable système %PATH%**.

Pour poursuivre l'installation, cliquez sur **Installer**.

Durant l'installation des composants de Kaspersky Anti-Virus qui interceptent le trafic de réseau, les connexions de réseau ouvertes sont interrompues. La majorité des connexions interrompues seront rétablies après un certain temps.

ETAPE 11. FIN DE LA PROCEDURE D'INSTALLATION

La fenêtre **Fin de l'installation** contient des informations sur la fin du processus d'installation de Kaspersky Anti-Virus.

Pour lancer l'Assistant de configuration initiale de l'application, cliquez sur **Suivant**.

Si le redémarrage de l'ordinateur est requis pour finaliser correctement l'installation, le message de circonstance sera affiché.

INSTALLATION DE L'APPLICATION VIA LA LIGNE DE COMMANDE

➤ Pour installer Kaspersky Anti-Virus 6.0 for Windows Servers MP4 saisissez dans la ligne de commande :

```
msiexec /i <nom_du_paquet>
```

Cette action entraîne l'ouverture de l'Assistant d'installation (cf. chapitre "Installation à l'aide de l'Assistant d'installation" à la page [17](#)). Il faudra redémarrer l'ordinateur à la fin de l'installation de l'application.

➤ Pour installer l'application en mode autonome (sans recours à l'Assistant d'installation), saisissez :

```
msiexec /i <nom_du_paquet> /qn
```

Dans ce cas, il faudra redémarrer l'ordinateur manuellement à la fin de l'installation de l'application. Pour réaliser le redémarrage automatique, saisissez dans la ligne de commande :

```
msiexec /i <nom_du_paquet> ALLOWREBOOT=1 /qn
```

N'oubliez pas que le redémarrage automatique de l'ordinateur ne peut avoir lieu qu'en mode autonome (avec l'argument /qn).

➤ Pour installer l'application avec un mot de passe pour la suppression, saisissez :

```
msiexec /i <nom_du_paquet> KLUNINSTPASSWD=***** – en cas d'installation de l'application en mode interactif ;
```

```
msiexec /i <nom_du_paquet> KLUNINSTPASSWD=***** /qn – en cas d'installation de l'application en mode autonome sans redémarrage de l'ordinateur ;
```

```
msiexec /i <nom_du_paquet> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – en cas d'installation de l'application en mode autonome avec redémarrage de l'ordinateur.
```

En cas d'installation de Kaspersky Anti-Virus en mode autonome, la lecture du fichier setup.ini, contenant les paramètres généraux d'installation de l'application, du fichier de configuration *install.cfg* (cf. section "Importation des paramètres de protection" à la page [111](#)) et du fichier de licence est prise en charge. N'oubliez pas que ces fichiers doivent être situés dans le même répertoire que le fichier de distribution de Kaspersky Anti-Virus.

PROCEDURE D'INSTALLATION VIA L'ÉDITEUR D'OBJETS DE STRATEGIE DE GROUPE (GROUP POLICY OBJECT)

Grâce à l'Éditeur d'objets de stratégie de groupe, vous pouvez installer, actualiser et supprimer Kaspersky Anti-Virus sur les postes de travail de l'entreprise faisant partie du domaine sans utiliser Kaspersky Administration Kit.

INSTALLATION DE L'APPLICATION

➤ Pour installer Kaspersky Anti-Virus, réalisez les opérations suivantes :

1. Créez un dossier réseau partagé sur le contrôleur de domaine et copiez-y le paquet d'installation de Kaspersky Anti-Virus au format *.msi*.

Vous pouvez également ajouter à ce répertoire le fichier *setup.ini* contenant les paramètres d'installation de Kaspersky Anti-Virus, le fichier de configuration *install.cfg* (cf. section "Importation des paramètres de protection" à la page [111](#)) ainsi que le fichier de licence.

- Ouvrez l'**Editeur d'objets de stratégie de groupe** via la console standard MMC (pour en savoir plus sur l'utilisation de l'Editeur, consultez l'aide de Microsoft Windows Server).
- Créez un nouveau paquet. Pour ce faire, sélectionnez **Objet de stratégie de groupe/ Configuration de l'ordinateur / Configuration des programmes / Installation d'une application** dans l'arborescence et utilisez la commande **Créer / Paquet** du menu contextuel.

Dans la fenêtre qui s'ouvre, indiquez le chemin d'accès au répertoire partagé contenant la distribution de Kaspersky Anti-Virus. Dans la boîte de dialogue **Déploiement de l'application**, sélectionnez le paramètre **Cible** et cliquez sur **OK**.

La stratégie de groupe sera appliquée à chaque poste de travail lors du prochain enregistrement d'ordinateurs dans le domaine. Kaspersky Anti-Virus sera installé sur tous les ordinateurs.

DESCRIPTION DES PARAMETRES DU FICHIER SETUP.INI

Le fichier *setup.ini* situé dans le répertoire de la distribution de Kaspersky Anti-Virus est utilisé lors de l'installation de l'application en mode autonome via la ligne de commande ou l'Editeur d'objets de stratégie de groupe. Ce fichier contient les paramètres suivants :

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

- InstallDir**=<chemin d'accès au répertoire d'installation>.
- Reboot=yes|no** – redémarrage ou non de l'ordinateur à la fin de l'installation de l'application (par défaut, le redémarrage n'a pas lieu).
- SelfProtection=yes|no** – activation ou non de l'auto-défense de Kaspersky Anti-Virus pendant l'installation (par défaut, l'auto-défense est activée).

[Components] – sélection des composants de l'application à installer. En cas, si ce groupe ne contient pas d'éléments, l'application s'installe intégralement.

- FileMonitor=yes|no** – installation de d'Antivirus Fichiers.

[Tasks] – activation des tâches de Kaspersky Anti-Virus. Si aucune tâche n'est reprise, toutes les tâches fonctionneront après l'installation. Si au moins une tâche est reprise, les autres tâches seront désactivées.

- ScanMyComputer=yes|no** – tâche d'analyse complète.
- ScanStartup=yes|no** – tâche d'analyse rapide.
- Scan=yes|no** – tâche d'analyse.
- Updater=yes|no** – tâche de mise à jour des bases et des modules de l'application.

La valeur **yes** peut être remplacée par 1, on, enable, enabled, et la valeur **no** par 0, off, disable, disabled.

MISE A JOUR DE LA VERSION DE L'APPLICATION

➔ Pour procéder à la mise à jour de Kaspersky Anti-Virus, procédez comme suit :

- Placez la distribution contenant la mise à jour de Kaspersky Anti-Virus au format .msi dans le répertoire de réseau.
- Ouvrez l'**Editeur d'objets de tâche de groupe** et créez un paquet de la manière décrite ci-dessus.
- Sélectionnez le nouveau paquet dans la liste et choisissez l'option **Propriétés** du menu contextuel. Dans la fenêtre des propriétés du paquet, ouvrez l'onglet **Mises à jour** et sélectionnez le paquet de la distribution

antérieure de Kaspersky Anti-Virus. Pour installer la version actualisée de Kaspersky Anti-Virus en conservant les paramètres de la protection, choisissez la méthode d'installation sur le paquet existant.

La stratégie de groupe sera appliquée à chaque poste de travail lors du prochain enregistrement d'ordinateurs dans le domaine.

N'oubliez pas, que la mise à jour de Kaspersky Anti-Virus via l'Éditeur d'objets de stratégie de groupe n'est pas soutenue sur les ordinateurs sous Microsoft Windows 2000 Server.

SUPPRESSION DE L'APPLICATION

➡ Pour supprimer Kaspersky Anti-Virus, réalisez les opérations suivantes :

1. Ouvrez **Éditeur d'objets de stratégie de groupe**.
2. Dans l'arborescence de la console, choisissez **Objet_de_stratégie_de_groupe / Configuration de l'ordinateur/ Configuration des programmes/ Installation d'une application**.

Dans la liste, choisissez le paquet de Kaspersky Anti-Virus, ouvrez le menu contextuel et choisissez l'option **Toutes les tâches/ Supprimer**.

Dans la boîte de dialogue **Suppression des applications**, sélectionnez **Suppression immédiate de cette application des ordinateurs de tous les utilisateurs** afin que Kaspersky Anti-Virus soit supprimé au prochain redémarrage de l'ordinateur.

PREMIERE UTILISATION

Une des principales tâches des experts de Kaspersky Lab dans le cadre du développement de Kaspersky Anti-Virus fut de veiller à la configuration optimale de tous les paramètres du logiciel.

Afin de rendre l'utilisation plus conviviale, nous avons tenté de regrouper ces paramètres au sein d'une interface unique : l'assistant de configuration initiale qui démarre à la fin de la procédure d'installation de l'application. En suivant les indications de l'Assistant, vous pourrez activer le programme, configurer la mise à jour et le lancement de l'analyse antivirus, limiter l'accès au programme grâce à un mot de passe.

Une fois que vous aurez installé et lancé le logiciel sur l'ordinateur, nous vous conseillons de réaliser les tâches suivantes :

- Evaluer l'état actuel de la protection pour s'assurer (cf. section "Administration de la sécurité" à la page [30](#)) que Kaspersky Anti-Virus offre le niveau de sécurité souhaité.
- Mise à jour du logiciel (cf. section "Mise à jour du logiciel" à la page [29](#)) (au cas où cela n'aurait pas été réalisé à l'aide de l'Assistant de configuration ou automatiquement après l'installation de l'application).
- Recherche de virus sur le serveur (cf. section "Recherche de virus sur l'ordinateur" à la page [28](#)).

DANS CETTE SECTION

Assistant de configuration initiale	24
Recherche de virus sur l'ordinateur	28
Mise à jour de l'application	29
Administration des licences	29
Administration de la sécurité	30
Suspension de la protection	31
Suppression des problèmes. Service d'assistance technique aux utilisateurs	32
Création d'un fichier de trace.....	32
Configuration des paramètres de l'application.....	33
Rapports sur le fonctionnement de l'application. Rapports.....	33

ASSISTANT DE CONFIGURATION INITIALE

L'Assistant de configuration de Kaspersky Anti-Virus est lancé à la fin de la procédure d'installation du logiciel. Son rôle est de vous aider à réaliser la configuration initiale du logiciel sur la base des particularités et des tâches de votre ordinateur.

L'interface de l'Assistant de configuration se présente sous la forme d'un Assistant Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Pour une installation complète de l'application sur l'ordinateur, il est nécessaire d'exécuter toutes les étapes de l'assistant. Si pour des raisons quelconques le fonctionnement de l'Assistant a été interrompu, alors les valeurs des paramètres déjà établis ne sont pas sauvegardées. Ensuite, lors de la tentative d'utilisation de l'application, l'Assistant de

configuration initiale se lance de nouveau, ce qui entraîne la nécessité d'effectuer à nouveau la configuration des paramètres.

UTILISATION DES OBJETS SAUVEGARDES DE LA VERSION PRECEDENTE

Cette fenêtre de l'Assistant s'affiche lors de l'installation sur la version précédente de Kaspersky Anti-Virus. Vous devrez choisir les données utilisées par la version précédente qui devront être transmises dans la version nouvelle. Il peut s'agir d'objets en quarantaine, dans le dossier de sauvegarde ou de paramètres de la protection.

Pour utiliser ces données avec la version nouvelle, cochez les cases adéquates.

ACTIVATION DE L'APPLICATION

La procédure d'activation de l'application consiste en enregistrement de la licence à l'aide d'installation du fichier clé. Sur la base de la licence l'application déterminera l'existence des droits d'utilisation et de leur durée.

La licence contient les informations de service indispensables pour assurer le parfait fonctionnement de Kaspersky Anti-Virus, ainsi que des renseignements complémentaires :

- Les informations sur l'assistance technique (qui l'assure et comment l'obtenir) ;
- le nom et le numéro de licence ainsi que sa date d'expiration.

Les moyens d'activation proposés varient si vous êtes déjà en possession du fichier de licence pour Kaspersky Anti-Virus ou si vous devez le télécharger depuis un serveur de Kaspersky Lab :

- activation en ligne (à la page [26](#)). Sélectionnez cette option si vous avez acheté une version commerciale du logiciel et que vous avez reçu le code d'activation. Vous recevrez, sur la base de ce code, le fichier de licence qui vous donnera accès à l'ensemble des fonctions de l'application pendant toute la durée de validité de la licence.
- activation de version d'évaluation (à la page [26](#)). Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous recevrez un fichier de licence gratuite dont la durée de validité sera limitée par la licence associée à la version d'évaluation de l'application.
- activation à l'aide du fichier de licence obtenu au préalable (cf. section "Activation à l'aide du fichier de licence" à la page [26](#)). Activez l'application à l'aide du fichier de licence pour Kaspersky Anti-Virus 6.0 obtenu au préalable.
- activer le logiciel plus tard. Si vous sélectionnez cette option, l'activation de Kaspersky Anti-Virus sera reportée à plus tard. Le programme sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser Kaspersky Anti-Virus une seule fois après l'installation). L'option **Activer le logiciel plus tard** est accessible uniquement au premier lancement de l'Assistant d'activation. Aux démarrages suivants de l'Assistant, dans le cas, si l'application est déjà activée, l'option **Supprimer le fichier de licence** est accessible pour exécuter l'opération correspondante.

En cas de sélection des deux premières options, l'activation de l'application est réalisée via le serveur Web de Kaspersky Lab, ce qui requiert un accès à Internet. Avant de lancer la procédure d'activation, vérifiez et, le cas échéant, modifiez les paramètres de connexion au réseau dans la fenêtre qui s'ouvre à l'aide du bouton **Paramètres LAN**. Pour obtenir de plus amples informations sur la configuration des paramètres de réseau, contactez votre administrateur système ou votre fournisseur d'accès Internet.

Si vous ne disposez pas d'une connexion Internet au moment de réaliser l'installation, vous pouvez réaliser l'activation plus tard au départ de l'interface de l'application ou en vous connectant à Internet depuis un autre ordinateur afin d'obtenir le fichier de licence associé au code d'activation après vous être enregistré sur le site Web du service d'assistance technique de Kaspersky Lab.

Vous pouvez aussi activer l'application via Kaspersky Administration Kit. Pour ce faire, il faut créer une tâche d'installation du fichier de licence (cf. page [125](#)) (pour de plus amples informations, consultez le manuel de référence de "Kaspersky Administration Kit").

VOIR EGALEMENT

Activation en ligne	26
Réception de la licence	26
Activation à l'aide du fichier de licence	26
Fin de l'activation	27

ACTIVATION EN LIGNE

L'activation en ligne repose sur la saisie du code d'activation que vous recevez par courrier électronique après avoir acheté Kaspersky Anti-Virus dans un magasin en ligne. Si vous avez acheté le logiciel dans un magasin traditionnel, le code d'activation sera repris sur l'enveloppe contenant le disque d'installation.

SAISIE DU CODE D'ACTIVATION

Cette étape requiert l'indication du code d'activation. Le code d'activation se présente sous la forme d'une série de chiffres et de lettres séparés par des traits d'union en 4 groupes de cinq chiffres, sans espace. Par exemple, 11111-11111-11111-11111. N'oubliez pas que le code doit être saisi en caractères romains.

Saisissez vos coordonnées dans la partie inférieure : nom, prénom, courrier électronique, pays et ville. Ces informations servent à identifier les utilisateurs enregistrés, par exemple en cas de dégradation ou de vol des informations relatives à la licence. Dans ce cas, vous pourrez obtenir un nouveau code d'activation sur la base des coordonnées que vous aurez fournies.

RECEPTION DE LA LICENCE

L'Assistant de configuration établit une connexion avec les serveurs de Kaspersky Lab sur Internet et les envoie vos données d'enregistrement (code d'activation, coordonnées). Après avoir établi la connexion, le code d'activation est contrôlé côté serveur et les informations de contact peuvent être complétées. Si le code d'activation est valide, l'assistant télécharge le fichier de licence qui s'installe alors automatiquement. Le processus d'activation se termine et une fenêtre contenant des informations détaillées sur la licence est affichée.

Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, contactez la société où vous avez acheté Kaspersky Anti-Virus pour obtenir des informations.

Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. Le processus d'activation est alors interrompu et l'application vous redirige vers l'assistance technique de Kaspersky Lab.

ACTIVATION DE LA VERSION D'ÉVALUATION

Il est conseillé d'utiliser cette option d'activation, si vous souhaitez installer une version d'évaluation de Kaspersky Anti-Virus avant de décider d'acheter la version commerciale. Vous recevrez une licence gratuite dont la durée de validité sera déterminée par le contrat de licence de la version d'évaluation de l'application. Après la date d'expiration de la licence, vous ne pourrez plus réutiliser une version d'évaluation.

ACTIVATION A L'AIDE DU FICHIER DE LICENCE

Si vous possédez un fichier de licence, vous pouvez l'utiliser pour activer Kaspersky Anti-Virus. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier possédant l'extension **.key**.

Une fois qu'une clé aura été installée, les informations relatives à la licence seront reprises dans la partie inférieure de la fenêtre : numéro de licence, type de licence (commerciale, évaluation, etc.), date d'expiration de licence, ainsi que le nombre d'ordinateurs sur lesquels la licence a été déployée.

FIN DE L'ACTIVATION

L'Assistant de configuration vous signale la réussite de l'activation de Kaspersky Anti-Virus. Il fournit également des renseignements relatifs à la licence : numéro de licence, type de licence (commerciale, test bêta, évaluation, etc.), date d'expiration de licence, ainsi que le nombre d'ordinateurs sur lesquels la licence a été déployée.

CONFIGURATION DE LA MISE A JOUR

La qualité de la protection de votre ordinateur dépend de la date des bases et des modules du logiciel. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de mise à jour du logiciel et de la programmer :

- **Automatique.** Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source de la mise à jour. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si le logiciel découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est utilisé par défaut.
- **Toutes les 2 heures** (l'intervalle peut varier en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.
- **Manuel.** Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules du logiciel qui font partie de l'installation peuvent être dépassés au moment de l'installation. Pour cette raison, nous vous conseillons d'obtenir les mises à jour les plus récentes du logiciel. Il suffit simplement de cliquer sur **Mettre à jour maintenant**. Dans ce cas, Kaspersky Anti-Virus recevra toutes les mises à jour depuis Internet et les installera sur l'ordinateur.

Si vous souhaitez passer à la configuration des paramètres des mises à jour (sélectionner les paramètres de réseau, sélectionner la ressource au départ de laquelle la mise à jour sera réalisée, configurer l'exécution sous les privilèges d'un compte déterminé ou activer la copie des mises à jour dans une source locale), cliquez sur **Configuration**.

PROGRAMMATION DE LA RECHERCHE DE VIRUS

La recherche des objets malveillants dans certains secteurs est l'une des tâches les plus importantes pour la protection de l'ordinateur.

Lors de l'installation de Kaspersky Anti-Virus, trois tâches d'analyse sont créées par défaut. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de lancement de la tâche d'analyse :

Analyse complète

Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles. Il est possible de modifier la programmation dans la fenêtre qui s'ouvre après que vous aurez cliqué sur **Modifier**.

Analyse rapide

Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation. Il est possible de modifier la programmation dans la fenêtre qui s'ouvre après que vous aurez cliqué sur **Modifier**.

RESTRICTION DE L'ACCES A L'APPLICATION

Le serveur peut être utilisé par plusieurs personnes dont les connaissances en informatique peuvent varier et étant donné que des programmes malveillants pourraient désactiver la protection, vous avez la possibilité de limiter l'accès à Kaspersky Anti-Virus à l'aide d'un mot de passe. Le mot de passe protège l'application contre les tentatives de désactivation non autorisée, de modification de ses paramètres ou de suppression de l'application.

Afin d'activer cette option, cochez la case **Activer la protection par un mot de passe** et saisissez les informations dans les champs **Mot de passe** et **Confirmation**.

Indiquez ensuite l'ampleur de la restriction :

- **Toutes les opérations (sauf les notifications dangereuses)**. Le mot de passe devra être saisi pour réaliser n'importe quelle opération à l'exception des notifications relatives à la découverte d'objets dangereux.
- **Les opérations choisies :**
 - **Configuration des paramètres de fonctionnement de l'application** – demande le mot de passe lorsque l'utilisateur tente de modifier les paramètres de fonctionnement de Kaspersky Anti-Virus.
 - **Arrêt de l'application** : l'utilisateur doit saisir le mot de passe s'il souhaite arrêter le programme.
 - **Désactivation des composants de la protection et arrêt des tâches d'analyse** – demande un mot de passe quand un utilisateur tente de désactiver le fonctionnement d'Antivirus Fichiers ou d'arrêter une tâche d'analyse.
 - **Désactivation de la stratégie de Kaspersky Administration Kit** – demande le mot de passe lorsque l'utilisateur tente de faire sortir l'ordinateur de la couverture de la stratégie et des tâches de groupe (en cas d'utilisation via Kaspersky Administration Kit).
 - **Lors de la suppression de l'application** – demande le mot de passe lorsque l'utilisateur tente de supprimer l'application de l'ordinateur.

FIN DE L'ASSISTANT DE CONFIGURATION

La dernière fenêtre de l'Assistant reprend un message confirmant la réussite de l'installation et de la configuration de Kaspersky Anti-Virus. Vous pouvez lancer directement l'application en cochant la case **Lancer le logiciel**.

Si une erreur est survenue lors de l'installation (par exemple : découverte de versions incompatibles d'autres logiciels antivirus) vous serez invité à redémarrer l'ordinateur.

RECHERCHE DE VIRUS SUR L'ORDINATEUR

Les développeurs de programmes malveillants déploient de gros efforts pour dissimuler l'activité de leurs programmes et c'est la raison pour laquelle il peut arriver que vous ne remarquiez pas la présence de programmes malveillants sur votre ordinateur.

Au moment de l'installation, Kaspersky Anti-Virus exécute automatiquement la tâche **Analyse rapide de l'ordinateur**. Cette tâche est orientée sur la recherche et la neutralisation de programmes malveillants dans les objets chargés au démarrage du système d'exploitation.

Les experts de Kaspersky Lab conseillent également d'exécuter la tâche **Analyse complète** de l'ordinateur.

➔ *Pour lancer/arrêter la tâche de recherche de virus, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.

3. Cliquez sur le bouton **Lancer l'analyse** afin de commencer l'analyse. Cliquez sur **Arrêter l'analyse** pendant le fonctionnement de la tâche si vous devez interrompre son exécution.

MISE A JOUR DE L'APPLICATION

La mise à jour de Kaspersky Anti-Virus nécessite une connexion Internet.

Kaspersky Anti-Virus est livré avec des bases qui contiennent les signatures des menaces. Toutefois, au moment de l'installation, les bases de l'application peuvent être dépassées vu que Kaspersky Lab actualise régulièrement les bases et les modules de l'application.

L'Assistant de configuration de l'application vous permet de sélectionner le mode d'exécution des mises à jour. Kaspersky Anti-Virus vérifie automatiquement la présence des mises à jour sur les serveurs de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Anti-Virus les télécharge et les installe en arrière plan.

Pour maintenir la protection de serveur au niveau le plus actuel possible, il est conseillé d'actualiser Kaspersky Anti-Virus directement après l'installation.

➔ Pour procéder à la mise à jour manuelle de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Lancer la Mise à jour**.

ADMINISTRATION DES LICENCES

Kaspersky Anti-Virus fonctionne grâce à une licence. Elle vous est donnée lors de l'achat du logiciel et vous donne le droit d'utiliser celui-ci à partir de son activation.

Sans licence, si la version d'évaluation n'a pas été activée, Kaspersky Anti-Virus ne réalisera qu'une - seule mise à jour. Les mises à jour suivantes disponibles sur le serveur ne seront pas téléchargées.

Si la version d'évaluation avait été activée, Kaspersky Anti-Virus ne fonctionnera plus une fois que la licence d'évaluation sera arrivée à échéance.

Une fois la clé commerciale expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettre à jour les bases de l'application. Vous pourrez toujours analyser l'ordinateur à l'aide de la recherche de virus et utiliser l'Antivirus Fichiers, mais uniquement sur la base des bases de l'application d'actualité à la fin de validité de la licence. Par conséquent, nous ne pouvons pas garantir une protection totale contre les nouveaux virus qui apparaîtraient après l'expiration de la licence.

Afin que le serveur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la licence d'utilisation de Kaspersky Anti-Virus. Deux semaines avant la date d'expiration, le programme vous avertira. Le message de circonstance apparaîtra à chaque exécution de l'application pendant un certain temps.

L'information générale sur la licence utilisée (active et complémentaire, si la dernière était installée) est présentée dans la section **Licence** de la fenêtre principale de Kaspersky Anti-Virus : type de licence (commerciale, évaluation, test bêta), le nombre maximum d'ordinateurs sur lesquels cette licence peut être installée, date de fin de validité et nombre de jours restant avant l'expiration. Pour garantir la précision des informations, optez pour le lien se rapportant à votre type de licence.

Pour lire les termes du contrat de licence pour l'utilisation de l'application, cliquez sur le bouton **Lire le contrat de licence**.

Afin de supprimer la licence, cliquez sur le bouton **Ajouter / Supprimer** et suivez les consignes de l'Assistant.

Kaspersky Lab organise à intervalles réguliers des actions qui permettent de renouveler la licence d'utilisation de ses logiciels en bénéficiant de remises considérables. Soyez à l'affût de ces actions sur le site de Kaspersky Lab dans la rubrique **Produits** → **Actions et offres spéciales**.

➔ *Pour acheter une licence ou pour prolonger sa durée de validité, procédez comme suit :*

1. Achetez un nouveau fichier de licence ou code d'activation. Pour ce faire, cliquez sur **Acheter une licence** (si l'application n'a pas été activée) ou sur **Renouveler votre licence**. Dans la page Web qui s'ouvre, vous pourrez saisir toutes les informations relatives à l'achat de la clé via la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la société. En cas d'achat via la boutique en ligne, vous recevrez, après confirmation du paiement, le fichier de clé ou le code d'activation de l'application dans un message envoyé à l'adresse indiquée dans le bon de commande.
2. Activez l'application. Pour ce faire, cliquez sur le bouton **Ajouter / Supprimer** dans la section **Licence** de la fenêtre principale de l'application ou utilisez la commande **Activation** du menu contextuel de l'application. Cette action entraînera l'ouverture de l'Assistant d'activation.

ADMINISTRATION DE LA SECURITE

L'état de la protection de l'ordinateur (cf. la section "Fenêtre principale de l'application" à la page [36](#)) signale l'apparition d'un problème dans la protection de celui-ci en modifiant la couleur de l'icône de l'état de la protection et du panneau dans laquelle elle se trouve. Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se manifestent.



Illustration 1. Etat actuel de la protection de l'ordinateur

Vous pouvez consulter la liste des problèmes, leur description et les solutions possibles à l'aide de l'Assistant de sécurité (cf. ill. ci-après) accessible en cliquant sur le lien **Corriger** (cf. ill. ci-dessus).



Illustration 2. Résolution des problèmes de sécurité

Vous pouvez consulter la liste des problèmes rencontrés. Les problèmes sont présentés dans l'ordre de l'urgence de la solution : viennent d'abord les problèmes les plus importants, à savoir ceux dont l'icône d'état est rouge, ensuite les problèmes moins importants (icône jaune) et en fin, les messages d'information. Chaque problème est accompagné d'une description et les actions suivantes sont proposées :

- **Résolution immédiate.** Grâce aux liens correspondants, vous pouvez passer à la suppression directe du problème, ce qui est l'action recommandée.
- **Reporter la suppression.** Si la suppression immédiate de la menace est impossible pour une raison quelconque, vous pouvez la reporter et y revenir plus tard. Cochez la case **Ignorer cette menace dans l'état de la sécurité annoncé dans la fenêtre principale** afin que la menace n'influence pas l'état actuel de la protection.

Sachez toutefois que cette possibilité n'est pas reprise pour les problèmes graves. Un problème grave peut être des objets malveillants non neutralisés, l'échec d'un ou de plusieurs composants de la protection ou la corruption des bases de l'application. Ce genre de problème doit être réglé le plus vite possible.

SUSPENSION DE LA PROTECTION

La suspension signifie que l'Antivirus Fichiers est désactivé pendant certain temps.

► Pour suspendre le fonctionnement de Kaspersky Anti-Virus, procédez comme suit :

1. Dans la Sélectionnez **Suspension de la protection** dans le menu contextuel.

2. Dans la fenêtre **Suspension de la protection** qui s'ouvre, sélectionnez la durée au terme de laquelle la protection sera réactivée parmi les options proposées.

SUPPRESSION DES PROBLEMES. SERVICE D'ASSISTANCE TECHNIQUE AUX UTILISATEURS

Si des problèmes surviennent pendant l'utilisation de Kaspersky Anti-Virus, vérifiez si la solution à ces problèmes ne figure pas dans le système d'aide ou dans la Banque de solutions de Kaspersky Lab (<http://support.kaspersky.com/fr/corporate>). La *banque des solutions* est une rubrique distincte du site du service d'assistance technique qui contient les recommandations sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées. Tentez de trouver la réponse à votre question ou la solution à votre problème dans cette ressource.

➔ *Pour consulter la banque de solutions, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Service d'assistance technique**.

Il existe une autre ressource où vous pouvez obtenir des informations sur l'utilisation des applications : le forum des utilisateurs des applications de Kaspersky Lab. Cette source est également une rubrique distincte du service d'assistance technique. Elle contient les questions, les commentaires et les suggestions des utilisateurs de l'application. Vous pouvez voir les principaux sujets de discussion, envoyer des commentaires sur l'application ou rechercher les réponses à votre question.

➔ *Pour ouvrir le forum des utilisateurs, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Accès direct aux FAQs**.

Si vous ne trouvez pas la solution à votre problème dans ce document, dans la banque de solutions ou dans le forum des utilisateurs, contactez le service d'assistance technique de Kaspersky Lab.

CREATION D'UN FICHIER DE TRACE

Le système d'exploitation ou certaines applications peuvent rencontrer des problèmes après l'installation de Kaspersky Anti-Virus. Il s'agit probablement de conflit entre l'application et les logiciels installés sur l'ordinateur ou les pilotes de votre ordinateur. Pour pouvoir résoudre vos problèmes, les experts du service d'assistance de Kaspersky Lab peuvent vous demander de créer un fichier de trace.

➔ *Pour créer un fichier de trace, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, utilisez la liste déroulante du bloc **Traçages** afin de sélectionner le niveau de traçage. Le niveau de traçage est indiqué par l'expert du service d'assistance technique. En cas d'absence de recommandations du service d'assistance technique, il est conseillé de choisir le niveau **500**.

5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation qui entraîne le problème.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

Pour accéder rapidement aux paramètres de Kaspersky Anti-Virus 6.0, utilisez la fenêtre de configuration des paramètres de l'application (cf. page [72](#)), que vous pouvez provoquer à l'aide du bouton **Configuration** de la fenêtre principale.

RAPPORTS SUR LE FONCTIONNEMENT DE L'APPLICATION. RAPPORTS

Le fonctionnement de l'Antivirus Fichier et l'exécution de chaque tâche d'analyse et de la mise à jour est consignée dans un rapport (cf. page [87](#)). Pour consulter les rapports : cliquez sur le bouton **Journaux**, qui se situe en bas à droite de la fenêtre principale.

Les objets placés en quarantaine (cf. page [88](#)) ou dans le dossier de sauvegarde (cf. page [89](#)) pendant l'utilisation de Kaspersky Anti-Virus, sont appelés *les fichiers de données du programme*. A l'aide du bouton **Menaces détectées**, vous pouvez ouvrir la fenêtre **Dossier de données**, où vous pouvez exécuter les actions nécessaires avec ces objets.

INTERFACE DE L'APPLICATION

L'interface de Kaspersky Anti-Virus est à la fois simple et conviviale. Ce chapitre est consacré à ses principaux éléments, à savoir :

- icône de la barre des tâches ;
- menu contextuel ;
- fenêtre principale ;
- notifications ;
- fenêtre de configuration des paramètres de Kaspersky Anti-Virus.



DANS CETTE SECTION

Icône dans la zone de notification de la barre des tâches	34
Menu contextuel	35
Fenêtre principale de l'application	36
Notifications.....	37
Fenêtre de configuration des paramètres de l'application	38




ICONE DANS LA ZONE DE NOTIFICATION DE LA BARRE DES TACHES

L'icône de Kaspersky Anti-Virus apparaît dans la barre des tâches directement après son installation.

Cette icône est un indicateur du fonctionnement de Kaspersky Anti-Virus. Elle représente l'état de la protection et montre également plusieurs actions fondamentales exécutées par l'application.

Si l'icône est activée  (en couleur), cela signifie que la protection du serveur est activée. Si l'icône n'est pas activée  (noir et blanc) cela signifie que la protection est désactivée.

L'icône de Kaspersky Anti-Virus change en fonction de l'opération exécutée :

-  – l'analyse d'un fichier ouvert, enregistré ou exécuté par vous ou un programme quelconque est en cours.
-  – la mise à jour des bases et des modules de Kaspersky Anti-Virus est en cours.
-  – une erreur s'est produite dans le fonctionnement d'un composant de Kaspersky Anti-Virus.

L'icône permet également d'accéder aux éléments fondamentaux de l'interface de l'application que sont le menu contextuel et la fenêtre principale.

Pour ouvrir le menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de l'application.

Pour ouvrir la fenêtre principale de Kaspersky Anti-Virus, double-cliquez avec le bouton gauche de la souris sur l'icône du programme.

MENU CONTEXTUEL

Le menu contextuel permet d'exécuter toutes les tâches principales liées à la protection.

Le menu de Kaspersky Anti-Virus contient les éléments suivants :

- **Analyse complète** : lance l'analyse complète de votre ordinateur à la recherche d'éventuels objets malveillants. Les objets de tous les disques, y compris sur les disques amovibles, seront analysés.
- **Analyse** : passe à la sélection des objets et à la recherche d'éventuels virus parmi eux. La liste contient par défaut une série d'objets tels que la mémoire système, les objets de démarrage, les bases de messagerie, tous les disques du serveur, etc. Vous pouvez enrichir la liste, sélectionner des objets à analyser et lancer l'analyse antivirus.
- **Mise à jour** : lancement de la mise à jour des modules et des bases de l'application pour Kaspersky Anti-Virus et son installation sur l'ordinateur.
- **Activation** : passe à l'activation de l'application. Afin d'obtenir le statut d'utilisateur enregistré qui vous donnera accès à toutes les fonctions de l'application et au service d'assistance technique, vous devez absolument activer votre version de Kaspersky Anti-Virus. Ce point du menu est visible uniquement si l'application n'a pas été activée.
- **Configuration** : permet d'examiner et de configurer les paramètres de fonctionnement de Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** : ouvre la fenêtre principale de l'application.
- **Suspension de la protection / Activation de la protection** : désactive temporairement / active le fonctionnement d'Antivirus Fichiers. Ce point du menu n'a aucune influence sur la mise à jour de l'application ou sur l'exécution des tâches d'analyse.
- **Désactivation de la stratégie / Activation de la stratégie** : désactive temporairement / active la stratégie (en cas d'utilisation de l'application via Kaspersky Administration Kit). Ce point du menu permet d'exclure l'ordinateur du champ d'application de stratégies et de tâches de groupe. Cette fonctionnalité est protégée par mot de passe (cf. section "Restriction de l'accès à l'application" à la page [82](#)). Ce point du menu apparaît lorsque le mot de passe correct est introduit.
- **A propos du programme** : affichage des informations relatives à l'application.
- **Quitter** : arrêt du fonctionnement de Kaspersky Anti-Virus (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).



Illustration 3. Menu contextuel

Si une tâche quelconque d'analyse est lancée à ce moment, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez consulter le rapport avec le résultat détaillé de l'exécution.

FENETRE PRINCIPALE DE L'APPLICATION

La fenêtre principale de l'application est scindée en trois parties :

- La partie supérieure reprend une évaluation globale de l'état de la protection de votre ordinateur.



Illustration 4. Etat actuel de la protection de l'ordinateur

Il existe trois états possibles de la protection et chacun est clairement indiqué par une couleur identique à celle d'un feu rouge. Le vert signale que la protection est assurée au bon niveau, tandis que le jaune et le rouge indiquent une menace pour la sécurité dans la configuration ou le fonctionnement de Kaspersky Anti-Virus. Les menaces regroupent non seulement les programmes malveillants, mais également les bases dépassées de l'application.

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent. Pour obtenir des informations détaillées sur ces menaces et sur les moyens de les résoudre rapidement, cliquez sur le lien **Corriger** (cf. ill. ci-dessus).

- La partie gauche de la fenêtre sert à la navigation. Elle permet de passer rapidement à l'utilisation de n'importe quelle fonction de l'application, à l'exécution d'une recherche de virus ou à l'analyse.



Illustration 5. Partie gauche de la fenêtre principale

- La partie droite de la fenêtre contient des informations relatives à la fonction de l'application sélectionnée dans la partie gauche. Elle permet de configurer les paramètres de chacune des fonctions, propose des outils pour l'exécution des tâches d'analyse, de mise à jour, etc.



Illustration 6. Partie droite de la fenêtre principale

Vous pouvez également utiliser les éléments suivants :

- le bouton **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application (cf. page [72](#)) ;
- le lien **Aide** : ouvre le système d'aide de Kaspersky Anti-Virus ;
- le bouton **Défectés** : passage à la manipulation des fichiers de données de l'application (cf. page [87](#)) ;
- le bouton **Journaux** : passage aux rapports sur le fonctionnement des composants (cf. page [87](#)) de l'application ;
- le lien **Assistance** : ouvre la fenêtre reprenant les informations relatives au système et des liens vers les sources d'informations proposées par Kaspersky Lab (cf. page [32](#)) (site du service d'assistance technique, forum).

NOTIFICATIONS

Lorsqu'un événement survient durant l'utilisation de Kaspersky Anti-Virus, des notifications apparaissent à l'écran sous la forme de messages contextuels au-dessus de l'icône de l'application dans la barre des tâches de Microsoft Windows.

En fonction du niveau de gravité de l'événement (du point de vue de la sécurité de l'ordinateur), le message peut appartenir à l'une des catégories suivantes :

- **Alertes**. Un événement d'importance critique s'est produit, par exemple la découverte d'un virus. Il faut immédiatement décider de la suite des événements. Ce type de message est de couleur rouge.

- **Attention.** Un événement présentant un risque potentiel s'est produit, par exemple la découverte d'un objet présentant un risque potentiel. Il faut prendre une décision en fonction du danger que représente la menace à vos yeux. Ce type de message est de couleur jaune.
- **Informations.** Ce message vous signale un événement qui n'est pas critique. Les messages à caractère informatif ont une couleur verte.

VOIR EGALEMENT

Types de message [102](#)

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky Anti-Virus peut être ouverte depuis la fenêtre principale. Pour ce faire, cliquez sur le bouton **Configuration** dans la partie supérieure.

La fenêtre de configuration ressemble à la fenêtre principale :

- La partie gauche offre un accès simple et rapide à la configuration de l'Antivirus Fichiers, des tâches d'analyse antivirus et de mise à jour ainsi qu'à la configuration des fonctions de service de l'application ;
- La partie droite reprend une énumération des paramètres de l'Antivirus Fichiers, de la tâche, etc. sélectionnés dans la partie gauche.

VOIR EGALEMENT

Configuration des paramètres de l'application [72](#)

PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS DE L'ORDINATEUR

L'**Antivirus Fichiers** permet d'éviter l'infection du système de fichiers de l'ordinateur. Ce composant est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, Antivirus Fichiers analyse uniquement les nouveaux fichiers et les fichiers modifiés. L'analyse des fichiers se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Quand Antivirus Fichiers découvre une menace, il exécute l'action définie.

Le niveau de protection des fichiers et de la mémoire est défini par les groupes de paramètres suivants qui :

- les paramètres qui définissent la zone protégée ;
- les paramètres qui définissent la méthode d'analyse utilisée ;
- les paramètres qui définissent l'analyse des fichiers composés (y compris les fichiers composés de grande taille) ;
- les paramètres qui définissent le mode d'analyse ;
- les paramètres qui permettent de suspendre le fonctionnement du composant (selon la programmation ; pendant le fonctionnement d'applications sélectionnées).

► *Afin de modifier les paramètres de fonctionnement d'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, introduisez les modifications nécessaires dans les paramètres du composant.

DANS CETTE SECTION

Algorithme de fonctionnement du composant	40
Modification du niveau de protection	41
Modification de l'action à réaliser sur les objets identifiés	41
Constitution de la zone de protection	42
Utilisation de l'analyse heuristique.....	43
Optimisation de l'analyse.....	44
Analyse des fichiers composés	44
Analyse des objets composés de grande taille.....	45
Modification du mode d'analyse	45
Technologie d'analyse.....	46
Suspension du composant : programmation	46
Suspension du composant : composition de la liste des applications	46
Restauration des paramètres de protection par défaut.....	47
Statistiques de la protection des fichiers	47
Réparation différée des objets.....	48

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Antivirus Fichiers est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, Antivirus Fichiers analyse uniquement les nouveaux fichiers ou les fichiers modifiés, c.-à-d. les fichiers qui ont été ajoutés ou modifiés depuis la dernière fois qu'ils ont été sollicités. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte les requêtes de l'utilisateur ou d'un programme quelconque adressé à chaque fichier.
2. Antivirus Fichiers recherche des informations sur le fichier intercepté dans les bases iChecker et iSwift et sur la base des informations obtenues, il décide d'analyser ou non le fichier.

L'analyse contient les étapes suivantes :

- Le fichier est soumis à la recherche d'éventuels virus. L'identification des objets s'opère sur la base des bases de l'application. Les bases contiennent la définition de tous les programmes malveillants, menaces et attaques de réseau connus à ce jour et leur mode de neutralisation.
- Les comportements suivants de Kaspersky Anti-Virus sont possibles en fonction des résultats de l'analyse :
 - a. Si le fichier contient un code malveillant, l'Antivirus Fichiers le bloque, place une copie dans le *dossier de sauvegarde* et tente de le neutraliser. Si la réparation réussit, le message reste accessible à l'utilisateur. Dans le cas contraire, l'objet infecté est supprimé.

- b. Si le fichier contient un code semblable à un code malveillant et que ce verdict ne peut pas être garanti à 100%, le fichier est réparé et placé dans un répertoire spécial : la *quarantaine*.
- c. Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

Quand l'application découvre un objet infecté ou potentiellement infecté, elle vous le signale. Vous devez réagir à ce message en choisissant une action.

- placer la menace en quarantaine en vue d'une analyse et d'un traitement ultérieur à l'aide de bases actualisées ;
- supprimer l'objet ;
- ignorer l'objet, si vous êtes absolument convaincu que cet objet ne peut pas être malveillant.

VOIR EGALEMENT

Protection antivirus du système de fichiers de l'ordinateur [39](#)

MODIFICATION DU NIVEAU DE PROTECTION

Le niveau de protection désigne un ensemble prédéfini de paramètres d'Antivirus Fichiers. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur.

- Si le risque d'infection de votre ordinateur est très élevé, sélectionnez un niveau de protection élevé.
- Le niveau recommandé assure l'équilibre entre les performances et la sécurité et convient à la majorité des cas.
- Si vous travaillez dans un milieu protégé (par exemple, un réseau d'entreprise avec un système de sécurité centralisé), ou si vous utilisez des applications gourmandes en ressources, le niveau de protection faible vous convient.

Avant d'activer le niveau de protection bas pour les fichiers, il est conseillé de lancer une analyse complète de l'ordinateur au niveau de protection élevé.

Si aucun des niveaux proposés ne répond à vos besoins, vous pouvez configurer les paramètres de fonctionnement d'Antivirus Fichiers. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➡ Afin de modifier le niveau de protection d'Antivirus Fichiers, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Sélectionnez le niveau de protection requis dans la fenêtre qui s'ouvre.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

Suite à l'analyse, Antivirus Fichiers attribue un des états suivants aux objets trouvés :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).

- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Si Kaspersky Anti-Virus découvre des objets infectés ou potentiellement infectés lors de l'analyse, la suite du fonctionnement de l'Antivirus Fichiers dépendra de l'état de l'objet et de l'action sélectionnée.

Par défaut, tous les objets infectés sont réparés et tous les objets probablement infectés - sont placés en quarantaine.

Toutes les actions possibles sont reprises dans le tableau plus bas.

ACTION CHOISIE	EN CAS DE DECOUVERTE D'UN OBJET DANGEREUX
<input checked="" type="checkbox"/> Réparer <input type="checkbox"/> Supprimer si la réparation est impossible	L'accès à l'objet est bloqué et il est soumis à une tentative de réparation, après la création d'une copie dans le dossier de sauvegarde. Si la désinfection réussit, l'objet est restitué à l'utilisateur pour être utilisé normalement. Si la réparation échoue, l'objet est placé en quarantaine. Les informations relatives à cette situation sont consignées dans le rapport. Vous pouvez plus tard tenter de réparer cet objet.
<input checked="" type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer si la réparation est impossible	L'accès à l'objet est bloqué et il est soumis à une tentative de réparation, après la création d'une copie dans le dossier de sauvegarde. Si la désinfection réussit, l'objet est restitué à l'utilisateur pour être utilisé normalement. Si l'objet ne peut être désinfecté, il est supprimé.
<input type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer	L'antivirus de fichiers bloque l'accès à l'objet et le supprime.
<input checked="" type="checkbox"/> Bloquer l'utilisateur pendant ... heures	Bloque la connexion actuelle du compte utilisateur au serveur lors d'une tentative de copie d'un objet infecté ou potentiellement infecté. Cette action peut être prise en plus de l'action associée au traitement de l'objet (réparation ou suppression). Si l'utilisateur se déconnecte puis qu'il entre à nouveau dans le système, Kaspersky Anti-Virus considèrera qu'il s'agit d'une nouvelle connexion et le blocage sera levé.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde. Cette copie est placée dans le dossier de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

Si le statut est *potentiellement infecté*, l'objet est placé en quarantaine sans tentative de réparation.

➔ Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, dans le groupe **Action**, sélectionnez l'action requise.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse fait référence non seulement à l'emplacement où se trouvent les objets analysés mais également au type de fichiers à analyser. Kaspersky Anti-Virus analyse par défaut uniquement les fichiers qui pourraient être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau.

Vous pouvez étendre ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets à analyser ou en modifiant les types de fichiers à analyser. Par exemple, vous souhaitez analyser uniquement les fichiers EXE lancés

depuis les disques de réseau. Toutefois, vous devez être certain que vous n'exposerez pas votre ordinateur à un risque d'infection lorsque vous réduisez la zone d'analyse.

Lors de la sélection du type de fichiers, il convient de garder à l'esprit les éléments suivants :

- Il existe toute une série de formats de fichier dans lesquels un code malveillant ne risque pas de s'incruster et dans lesquels son activité sera très réduite (exemple, *txt*). Il existe par contre des formats de fichier qui contiennent ou qui peuvent contenir un code exécutable (*exe*, *dll*, *doc*). Le risque d'intrusion et d'activation ultérieure d'un code malveillant dans ces fichiers est assez élevé.
- Il ne faut pas oublier qu'un individu mal intentionné peut envoyer un virus dans un fichier portant l'extension *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Fichiers analysés selon le format**, Antivirus Fichiers ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier *exe*. Le fichier sera alors soumis à une analyse antivirus.

La définition du type de fichiers analysés vous permet de déterminer le format des fichiers qui seront soumis à l'analyse antivirus à l'ouverture, l'exécution et l'enregistrement, ainsi que leur taille et le disque sur lequel ils sont enregistrés.

Afin de simplifier la configuration, tous les fichiers ont été séparés en deux groupes : *simples* et *composés*. Les fichiers simples ne contiennent aucun objet (par exemple, un fichier *txt*). Les fichiers composés peuvent contenir plusieurs objets et chacun de ceux-ci peut à son tour contenir plusieurs pièces jointes. Les exemples ne manquent pas : archives, fichiers contenant des macros, des tableaux, des messages avec des pièces jointes, etc.

N'oubliez pas que l'antivirus de fichiers recherchera la présence éventuelle de virus uniquement dans les fichiers inclus dans la zone de protection. Les fichiers qui ne font pas partie de cette zone seront accessibles sans analyse. Cela augmente le risque d'infection de l'ordinateur !

➡ Afin de modifier la liste des objets à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans la rubrique **Zone de protection** cliquez sur **Ajouter**.
4. Dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajoutés les objets requis, cliquez sur le bouton **OK**.
5. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

➡ Afin de modifier la priorité de la règle, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'affiche, cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le bloc **Type de fichiers** sélectionnez le paramètre requis.

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Anti-Virus compare l'objet décelé aux enregistrements des bases, ce qui vous permet d'obtenir une réponse univoque sur la nature indésirable de l'objet analysé et sur la catégorie de programmes malveillants à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. L'analyse heuristique permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si l'activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus.

Vous pouvez également définir le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

➔ *Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre ouverte sur l'onglet **Productivité** dans le bloc **Méthode de contrôle** cochez la case **Analyse heuristique** et proposez plus bas le niveau de détails du contrôle.

OPTIMISATION DE L'ANALYSE

Pour réduire la durée de l'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus, vous pouvez analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

➔ *Afin d'analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Productivité** cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Les paquets d'installation et les fichiers qui contiennent des objets OLE sont exécutés à l'ouverture, ce qui les rend plus dangereux que des archives. Pour protéger l'ordinateur contre l'exécution de codes malveillants et pour accélérer la vitesse de l'analyse, désactivez l'analyse des archives et activez l'analyse des fichiers de ce type.

Si le fichier qui contient l'objet OLE représente un archive des objets, il sera analysé lors du déballage. Vous pouvez activer l'analyse des archives pour analyser les fichiers avec les objets OLE qui se trouvent en archive avant son déballage. Cependant, cela entraîne une chute de la vitesse d'analyse.

Par défaut, Kaspersky Anti-Virus analyse uniquement les objets OLE joints.

➔ *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.

3. Dans la fenêtre qui s'affiche, sur l'onglet **Productivité** dans la rubrique **Analyse des fichiers composés**, cochez les cases en regard des types d'objets composés qui seront analysés par l'application.

ANALYSE DES OBJETS COMPOSÉS DE GRANDE TAILLE

Lors de l'analyse des fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. Il est possible de réduire cette durée si l'analyse des fichiers est réalisée en arrière-plan. Si un objet malveillant est identifié durant la manipulation d'un fichier de ce genre, Kaspersky Anti-Virus vous le signalera.

Pour réduire le délai d'attente avant de pouvoir accéder aux fichiers, désactiver le décompactage des fichiers dont la taille est supérieure à la taille définie. L'analyse des fichiers aura toujours lieu au moment de l'extraction de l'archive.

► *Pour que l'application décompacte les fichiers de grande taille en arrière-plan, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Productivité**, dans le groupe **Analyse des fichiers composés**, cliquez sur **Options**.
4. Dans la fenêtre **Fichiers complexes** cochez la case **Décompacter les fichiers complexes en arrière-plan** et définissez la valeur de la taille minimale du fichier dans le champ ci-dessous.

► *Afin que l'application ne décompacte pas les fichiers composés de grande taille, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Productivité**, dans le groupe **Analyse des fichiers composés**, cliquez sur **Options**.
4. Dans la fenêtre **Fichiers complexes** cochez la case **Ne pas décompacter les fichiers complexes de grande taille** et définissez la taille maximale du fichier dans le champ du dessous.

MODIFICATION DU MODE D'ANALYSE

Le mode d'analyse désigne la condition de déclenchement d'Antivirus Fichiers. L'application utilise par défaut le mode intelligent dans le quel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Par exemple, en cas de manipulation d'un document Microsoft Office, l'application analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Vous pouvez modifier le mode d'analyse des objets. La sélection du mode dépend du type de fichiers que vous manipulez le plus souvent.

► *Afin de modifier la mode d'analyse des objets, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans la rubrique **Mode d'analyse**, sélectionnez le mode requis.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée par Antivirus Fichiers :

- **iChecker.** Cette technologie permet d'accélérer l'analyse en excluant certains objets. L'exclusion d'un objet de l'analyse est réalisée à l'aide d'un algorithme spécial qui tient compte de la date d'édition des signatures des menaces, de la date de l'analyse antérieure et de la modification des paramètres d'analyse.

Admettons que vous possédiez une archive qui a reçu l'état *non infecté* après l'analyse. Lors de l'analyse suivante, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases de l'application, l'archive sera analysée à nouveau.

La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift.** Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

➡ Afin de modifier la technologie d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologie d'analyse**, sélectionnez la valeur de paramètre souhaitée.

SUSPENSION DU COMPOSANT : PROGRAMMATION

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant pendant un certain temps.

➡ Pour programmer la suspension du composant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration**.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Suspension de la tâche**, cochez la case **Selon la programmation** et cliquez sur le bouton **Programmation**.
4. Dans la fenêtre **Suspension de la tâche**, indiquez l'heure (au format HH:MM) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

SUSPENSION DU COMPOSANT : COMPOSITION DE LA LISTE DES APPLICATIONS

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant lors de l'utilisation de certains programmes.

La configuration de l'arrêt d'Antivirus Fichiers en cas de conflits avec des applications déterminées est une mesure extrême ! En cas de conflit pendant l'utilisation du composant, contactez le service d'assistance technique de Kaspersky Lab (<http://support.kaspersky.com/fr/corporate>). Les experts vous aideront à résoudre le problème de compatibilité entre Kaspersky Anti-Virus et les applications installées sur l'ordinateur.

➔ Pour configurer la suspension du composant pendant l'utilisation des applications indiquées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Au lancement des applications** puis cliquez sur **Liste**.
4. Dans la fenêtre **Programmes**, composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

RESTAURATION DES PARAMÈTRES DE PROTECTION PAR DÉFAUT

Lorsque vous configurez l'Antivirus Fichiers, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Si vous avez modifié la liste des objets repris dans le secteur d'analyse lors de la configuration de l'Antivirus Fichiers, vous aurez la possibilité, lors de la restauration de la configuration initiale, de conserver cette liste pour une utilisation ultérieure.

➔ Pour restaurer les paramètres de protection par défaut tout en conservant la liste des objets repris dans la zone de protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** et cliquez sur **Par défaut**.
3. Dans la fenêtre **Restauration des paramètres**, cochez la case **Zone de protection**.

STATISTIQUES DE LA PROTECTION DES FICHIERS

Toutes les opérations réalisées par l'Antivirus de fichiers sont consignées dans un rapport spécial. Pour consulter les informations relatives au fonctionnement du composant, utilisez le lien **Statistiques**. Ce rapport détaillé contient plusieurs onglets :

- Tous les objets dangereux découverts dans les messages sont repris sur l'onglet **Défectés**. Vous y découvrirez le chemin d'accès complet vers l'emplacement de chaque objet ainsi que le statut que l'Antivirus Fichiers lui aura attribué : si le programme a pu définir exactement le programme malveillant qui a infecté l'objet, il recevra le statut correspondant. Par exemple, virus, cheval de Troie etc. S'il est impossible de définir avec exactitude le type de programme malveillant, l'objet recevra le statut *suspect*. En plus de l'état, le rapport reprend également les informations relatives à l'action exécutée sur l'objet (découvert, introuvable, réparé).

Si vous ne souhaitez pas que cet onglet affiche les informations relatives aux objets réparés, désélectionnez la case **Afficher les objets réparés**.

- La liste complète des événements survenus pendant le fonctionnement de l'Antivirus Fichiers figure sur l'onglet **Événements**. Les événements prévus sont :

- *Informations* (exemple : objet non traité : ignoré en fonction du type).
- *Avertissement* (exemple : découverte d'un virus).
- *Remarque* (exemple : archive protégée par un mot de passe).

En général, les messages à caractère purement informatif n'ont aucun intérêt particulier. Vous pouvez désactiver l'affichage de ce type de message. Pour ce faire, désélectionnez la case **Afficher tous les événements**.

- Les *statistiques* de l'analyse sont reprises sur l'onglet correspondant. Vous y retrouverez le nombre total d'objets analysés ainsi que, dans des colonnes séparées, le nombre d'objets qui étaient des archives, le nombre d'objets dangereux, le nombre d'objets réparés, le nombre d'objets placés en quarantaine, etc.
- Les *paramètres* de fonctionnement de l'Antivirus Fichiers sont repris sur l'onglet du même nom. Pour passer rapidement à la configuration du composant, cliquez sur **Modifier les paramètres**.
- L'onglet affiche la liste des utilisateurs dont l'ordinateur a été bloqué suite à la tentative de copie d'un objet infecté/potentiellement infecté sur le serveur.

REPARATION DIFFEREE DES OBJETS

Dans Kaspersky Anti-Virus for Windows Servers MP4, l'accès aux objets infectés est bloqué aussi bien en cas de réparation, lorsque la réparation a échoué qu'en cas de suppression.

Pour pouvoir à nouveau accéder aux objets bloqués, vous devrez essayer de les réparer. Si la réparation a réussi, vous pourrez à nouveau travailler avec cet objet. S'il est impossible de le réparer vous pourrez choisir entre *supprimer* ou *ignorer*. Dans ce dernier cas, l'accès au fichier sera autorisé. Cela augmente toutefois le risque d'infection du serveur ! Il est vivement conseillé de ne pas ignorer les objets malveillants.

➤ Afin d'obtenir l'accès aux objets bloqués pour les réparer, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Défectés**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces actives**, sélectionnez les objets qui vous intéressent et cliquez sur le lien **Réparer tous**.

VOIR EGALEMENT

Modification de l'action à réaliser sur les objets identifiés [41](#)

RECHERCHE DE VIRUS SUR LE SERVEUR

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 recherche la présence éventuelle de virus aussi bien dans des objets particuliers (fichiers, répertoires, disques, disques amovibles) que dans tout le serveur. La recherche de virus exclut le risque de propagation d'un code malveillant qui n'aurait pas été repéré pour une raison quelconque par l'Antivirus Fichiers.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 propose par défaut les tâches suivantes d'analyse antivirus :

Analyse

Analyse des objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.

Analyse complète

Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.

Analyse rapide

Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres et même programmer le lancement de la tâche.

De plus, vous pouvez rechercher la présence éventuelle de virus dans n'importe quel objet sans devoir créer une tâche particulière. Vous pouvez sélectionner des objets individuels à analyser au départ de l'interface de Kaspersky Anti-Virus ou à l'aide des méthodes Microsoft Windows Server (ex. : dans la fenêtre de **l'Assistant** ou au départ du **Bureau**, etc.). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

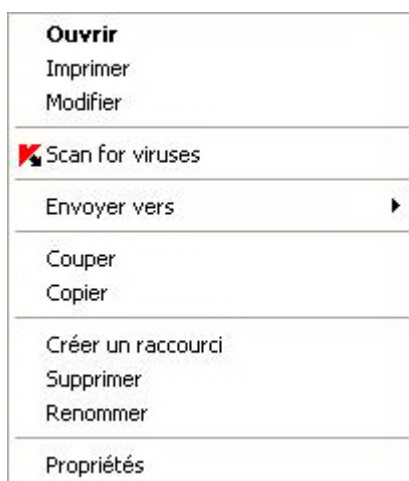


Illustration 7. Menu contextuel de Microsoft Windows

Vous pouvez également accéder au rapport sur l'analyse où vous pourrez voir des informations complètes sur les événements survenus durant l'exécution des tâches.

► Pour modifier les paramètres d'une tâche d'analyse quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.

3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Dans la fenêtre qui s'ouvre, introduisez les modifications nécessaires dans les paramètres de la tâche sélectionnée.

➔ *Pour ouvrir le rapport sur la recherche de virus :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur **Journaux**.

DANS CETTE SECTION

Lancement de la recherche d'éventuels virus.....	50
Composition de la liste des objets à analyser.....	51
Modification du niveau de protection	52
Modification de l'action à exécuter après la découverte d'une menace	53
Modification du type d'objets à analyser	54
Optimisation de l'analyse.....	54
Analyse des fichiers composés	55
Modification de la méthode d'analyse.....	55
Technologie d'analyse.....	56
Performances de l'ordinateur pendant l'exécution des tâches.....	57
Suspension de la tâche : programmation	57
Suspension du composant : composition de la liste des applications	58
Mode de lancement : configuration du compte utilisateur.....	58
Mode de lancement : programmation	58
Particularité du lancement programmé des tâches de l'analyse.....	59
Statistiques de recherche d'éventuels virus.....	59
Définition de paramètres d'analyse uniques pour toutes les tâches	60
Restauration des paramètres d'analyse par défaut	60

LANCEMENT DE LA RECHERCHE D'EVENTUELS VIRUS

Vous pouvez lancer la recherche d'éventuels virus de deux manières :

- le menu contextuel de Kaspersky Anti-Virus ;
- la fenêtre principale de Kaspersky Anti-Virus.

Les informations relatives à l'exécution de la tâche sont affichées dans la fenêtre principale de Kaspersky Anti-Virus.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc.).

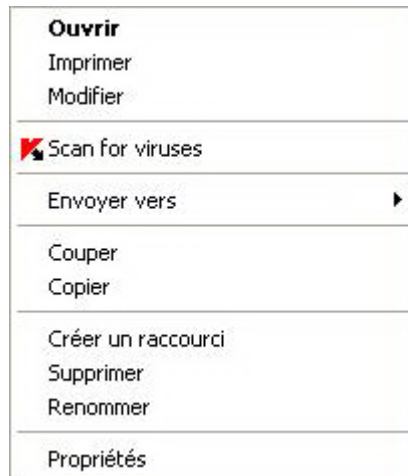


Illustration 8. Menu contextuel de Microsoft Windows

➤ *Pour lancer la recherche d'éventuels virus depuis le menu contextuel :*

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Analyse**. Dans la fenêtre principale de Kaspersky Anti-Virus ainsi ouverte, sélectionnez la tâche **Analyse (Analyse complète, Analyse rapide)**. Le cas échéant, configurez les paramètres de la tâche sélectionnée puis cliquez sur le bouton **Lancer l'analyse**.
3. Dans le menu contextuel, sélectionnez le point **Analyse complète**. L'analyse complète de l'ordinateur sera lancée. La progression de la tâche est illustrée dans la fenêtre principale de Kaspersky Anti-Virus.

➤ *Pour lancer la recherche d'éventuels virus depuis la fenêtre principale de l'application :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le bouton **Lancer l'analyse**. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

➤ *Pour lancer la recherche d'éventuels virus dans un objet sélectionné depuis le menu contextuel de Microsoft Windows, procédez comme suit :*

1. Cliquez avec le bouton droit de la souris sur le nom de l'objet sélectionné.
2. Dans le menu contextuel qui s'ouvre, sélectionnez le point **Rechercher d'éventuels virus**. La progression de la tâche et le résultat sont affichés dans la fenêtre de statistiques.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Une liste d'objets à analyser est associée par défaut à chaque tâche de recherche d'éventuels virus. Afin de consulter cette liste, sélectionnez le nom de la tâche (ex. : **Analyse complète**) dans la section **Analyse** dans la fenêtre principale de l'application. La liste des objets sera reprise dans la partie droite de la fenêtre sous la barre d'état.

La liste des objets à analyser pour la liste des tâches créées par défaut lors de l'installation du logiciel est déjà composée.

Pour faciliter la tâche des utilisateurs, il est possible d'ajouter à la zone d'analyse des catégories telles que des bases de messagerie de l'utilisateur, la mémoire vive, les objets de démarrage, le dossier de sauvegarde du système d'exploitation et les objets qui se trouvent dans le dossier de quarantaine de Kaspersky Anti-Virus.

De plus, lors de l'ajout d'un répertoire contenant des objets, vous pouvez changer la profondeur. Pour ce faire, sélectionnez l'objet dans la liste des objets à analyser puis ouvrez le menu contextuel et sélectionnez le point **Sous-répertoire compris**.

► *Pour composer la liste des objets à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien **Ajouter** pour la rubrique sélectionnée.
4. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajoutés les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci. Afin de supprimer un objet de la liste, sélectionnez-le et cliquez sur le lien **Supprimer**.

MODIFICATION DU NIVEAU DE PROTECTION

Le niveau de protection désigne un ensemble prédéfini de paramètres d'analyse. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. Vous choisissez le niveau en fonction de vos préférences :

- si vous pensez que le risque d'infection de votre ordinateur est très élevé, sélectionnez un niveau de protection élevé.
- le niveau recommandé convient à la majorité des cas et son utilisation est conseillée par les experts de Kaspersky Lab.
- si vous utilisez des applications gourmandes en mémoire vive, sélectionnez le niveau faible car la sélection de fichiers à analyser à ce niveau est moindre.

Si aucun des niveaux proposés ne répond à vos besoins, vous pouvez configurer vous-même les paramètres de fonctionnement. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut de l'analyse, sélectionnez un des niveaux proposés. Par défaut, l'analyse des fichiers s'opère selon les paramètres du niveau **Recommandé**.

► *Afin de modifier le niveau de protection, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Dans la fenêtre qui s'ouvre, dans le groupe **Niveau de protection** déplacez le curseur le long de l'échelle. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité des fichiers analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée. Ou cliquez sur le bouton **Configuration** et configurez les paramètres requis dans la fenêtre qui s'ouvre. Le niveau de protection devient **Utilisateur**.

MODIFICATION DE L'ACTION A EXECUTER APRES LA DECOUVERTE D'UNE MENACE

Si l'analyse d'un objet détermine une infection ou une possibilité d'infection, la suite du fonctionnement du programme dépendra de l'état de l'objet et de l'action sélectionnée.

A la fin de l'analyse, chaque objet peut se voir attribuer l'un des statuts suivants :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*).
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Par défaut, tous les objets infectés sont réparés et tous les objets probablement infectés sont placés en quarantaine.

ACTION CHOISIE	CONSEQUENCE EN CAS DE DECOUVERTE D'UN OBJET MALVEILLANT/PROBABLEMENT INFECTE
<input checked="" type="radio"/> Confirmer à la fin de l'analyse	Le programme reporte le traitement des objets jusque la fin de l'analyse. Les fenêtres demandant la confirmation des actions pour chacun des objets apparaîtront une après l'autre à la fin de l'analyse.
<input checked="" type="radio"/> Confirmer pendant l'analyse	Le programme affiche un message d'avertissement qui reprend les informations relatives au code malveillant source de l'infection (potentielle) et propose l'une des actions suivantes.
<input checked="" type="radio"/> Ne pas confirmer	Le programme consigne les informations relatives aux objets découverts dans le rapport sans les avoir traités ou sans avoir averti l'utilisateur. Ce mode n'est pas recommandé car il ne débarrasse pas votre ordinateur des objets infectés et probablement infectés, ce qui conduira inévitablement à l'infection de celui-ci.
<input checked="" type="radio"/> Ne pas confirmer <input checked="" type="checkbox"/> Réparer	Le programme consigne les informations relatives aux objets découverts dans le rapport sans les avoir traités ou sans avoir averti l'utilisateur. Ce mode n'est pas recommandé car il ne débarrasse pas le serveur des objets infectés et probablement infectés, ce qui conduira inévitablement à l'infection de celui-ci.
<input checked="" type="radio"/> Ne pas confirmer <input checked="" type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer si la réparation est impossible	Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la réparation de l'objet échoue, il sera supprimé. Une copie de l'objet est conservée dans le dossier de sauvegarde.
<input checked="" type="radio"/> Ne pas confirmer <input type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer	Le programme supprimera automatiquement l'objet.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde. Cette copie est placée dans le dossier de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

Si le statut est *potentiellement infecté*, l'objet est placé en quarantaine sans tentative de réparation.

➔ Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :



1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.

4. Saisissez vos modifications dans le groupe **Action** de la fenêtre qui s'ouvre.

MODIFICATION DU TYPE D'OBJETS A ANALYSER

La définition du type d'objet à analyser est la fonction qui vous permet d'indiquer le format et la taille des fichiers qui seront analysés lors de l'exécution de la tâche d'analyse sélectionnée.

Lors de la sélection du type de fichiers, il convient de garder à l'esprit les éléments suivants :

- Il existe toute une série de formats de fichier dans lesquels un code malveillant ne risque pas de s'incruster et dans lesquels son activité sera très réduite (exemple, *txt*). Il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, *exe*, *dll*, *doc*). Le risque d'infection par un code malveillant et d'activation est assez élevé pour ces fichiers.
- Il ne faut pas oublier qu'un individu mal intentionné peut envoyer un virus dans un fichier portant l'extension *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option  **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option  **Fichiers analysés selon le format**, la protection des fichiers et de la mémoire ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier *exe*. Le fichier sera alors soumis à une analyse antivirus minutieuse.

➔ Afin de modifier la priorité de la règle, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le bloc **Type de fichiers** sélectionnez le paramètre requis.

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Il est également possible de limiter la durée de l'analyse. Une fois la durée écoulée, l'analyse des fichiers sera suspendue. Vous pouvez aussi limiter la taille du fichier à analyser. S'il dépasse la valeur définie, il sera exclu de l'analyse.

➔ Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre ouverte sur l'onglet **.Zone d'action** dans le bloc **Optimisation du contrôle** cochez la case **Contrôler seulement les fichiers nouveaux et modifiés**.

➔ Pour définir une restriction temporaire sur la durée de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action**, bloc **Optimisation d'analyse**, cochez la case **Arrêter l'analyse si elle dure plus de**, et définissez la durée d'analyse dans le champ à côté.

➔ *Pour limiter la taille de fichier à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Zones d'action** cliquez sur le bouton **Avancé**.
6. Dans la fenêtre **Fichiers composés** cochez la case **Ne pas décompacter les fichiers composés de plus de** et définissez la taille du fichier dans le champ situé à côté.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour ce faire, cliquez sur le lien situé en regard du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si vous sélectionnez le mode d'analyse uniquement des nouveaux fichiers et des fichiers modifiés, il sera impossible de sélectionner un type de fichier composé.

➔ *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le bloc **Analyse des fichiers composés** sélectionnez les types de fichiers composés à analyser.

MODIFICATION DE LA METHODE D'ANALYSE

Parmi les méthodes d'analyse que vous pouvez utiliser, il y a l'*analyse heuristique*. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si l'activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect.

Vous pouvez également définir le niveau de détail de l'analyse heuristique. Pour ce faire, placez le curseur sur une des positions suivantes : **superficielle**, **moyenne** ou **profonde**.

Outre ces méthodes d'analyse, vous pouvez également utiliser la recherche d'outils de dissimulation d'activité. *Un outil de dissimulation d'activité* est un utilitaire qui permet de dissimuler la présence de programmes malveillants dans le

système d'exploitation. Ces utilitaires s'introduisent dans le système en masquant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité. Lorsque la recherche est activée, vous pouvez définir le niveau de détail d'identification des outils de dissimulation d'activité (Analyse en profondeur). Dans ce cas, une recherche minutieuse de ces programmes sera lancée via l'analyse d'une grande quantité d'objets de divers types.

➔ *Pour utiliser les méthodes d'analyse requises, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le bloc **Méthodes d'analyse** sélectionnez les méthodes d'analyse requis.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée lors de l'analyse :

- **iChecker.** Cette technologie permet d'accélérer l'analyse en excluant certains objets. L'exclusion d'un objet de l'analyse est réalisée à l'aide d'un algorithme spécial qui tient compte de la date d'édition des signatures des menaces, de la date de l'analyse antérieure et de la modification des paramètres d'analyse.

Par exemple, vous disposez d'un fichier archivé que l'antivirus a analysé et auquel il a attribué l'état *non infecté*. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases de l'application, l'archive sera analysée à nouveau.

La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip ou rar).

- **iSwift.** Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

➔ *Afin d'utiliser la technologie d'analyse des objets, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Technologies d'analyse**, activez l'utilisation de la technologie requise.

PERFORMANCES DE L'ORDINATEUR PENDANT L'EXECUTION DES TACHES

Afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky Anti-Virus arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour l'application de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Remarquez que ce paramètre peut être défini individuellement pour chaque tâche de recherche de virus. Dans ce cas, la configuration du paramètre pour une tâche particulière à une priorité supérieure.

► *Pour reporter l'exécution des tâches d'analyse en cas de ralentissement d'autres programmes, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Méthodes d'analyse** cochez la case **Céder les ressources aux autres applications**.

SUSPENSION DE LA TACHE : PROGRAMMATION

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement le fonctionnement des tâches d'analyse. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant pendant un certain temps.

► *Pour programmer la suspension du composant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Dans le menu qui s'ouvre, sélectionnez le point **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet dans le groupe **Suspension de la tâche**, cochez la case **Selon la programmation** et cliquez sur le bouton **Programmation**.
6. Dans la fenêtre **Suspension de la tâche**, indiquez l'heure (au format HH:MM) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

SUSPENSION DU COMPOSANT : COMPOSITION DE LA LISTE DES APPLICATIONS

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement le fonctionnement de la tâche d'analyse. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant lors de l'utilisation de certains programmes.

➔ *Pour configurer la suspension de la tâche pendant l'utilisation des applications indiquées, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Dans le menu qui s'ouvre, sélectionnez le point **Configuration**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Au lancement des applications** puis cliquez sur **Liste**.
6. Dans la fenêtre **Programmes**, composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Vous pouvez définir le compte utilisateur sous les privilèges duquel l'analyse sera réalisée.

➔ *Pour lancer la tâche avec les privilèges d'un autre compte, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Configuration** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre sous l'onglet **Mode d'exécution** dans le bloc **Utilisateur** cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

MODE DE LANCEMENT : PROGRAMMATION

Toutes les tâches liées à la recherche de virus peuvent être lancées manuellement ou selon un horaire défini.

S'agissant des tâches créées lors de l'installation du logiciel, le lancement programmé est désactivé par défaut. La seule exception se situe au niveau de la tâche d'analyse rapide qui est réalisée chaque fois que l'ordinateur est allumé.

Lors de la programmation du lancement des tâches, il est nécessaire d'indiquer l'intervalle selon lequel l'événement doit avoir lieu.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

➤ Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Modifier** de la rubrique **Mode d'exécution** dans la fenêtre qui s'ouvre.
5. Saisissez vos modifications dans la fenêtre **Programmation** qui ouvre.

➤ Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Modifier** de la rubrique **Mode d'exécution** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre **Programmation** qui s'ouvre, dans le groupe **Configuration de la programmation** cochez la case **Lancer la tâche ignorée**.

PARTICULARITE DU LANCEMENT PROGRAMME DES TACHES DE L'ANALYSE

Toutes les tâches liées à la recherche de virus peuvent être lancées manuellement ou selon un horaire défini.

Pour les tâches, lancées selon la programmation, vous pouvez utiliser la possibilité complémentaire : *suspendre l'analyse selon la programmation si l'écran de veille est actif ou l'ordinateur est débloqué*. Cette possibilité permet de reporter le lancement de la tâche jusqu'à ce que l'utilisateur ne termine pas son travail sur l'ordinateur. Ainsi, la tâche d'analyse ne va pas occuper les ressources de l'ordinateur pendant son fonctionnement.

➤ Pour lancer l'analyse une fois que l'utilisateur terminera son travail, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse complète, Analyse rapide**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Dans la fenêtre qui s'ouvre, dans le bloc **Mode d'exécution**, cochez la case **Suspendre l'analyse selon la programmation si l'écran de veille est actif ou l'ordinateur est débloqué**.

STATISTIQUES DE RECHERCHE D'EVENTUELS VIRUS

Les informations globales sur le fonctionnement de chacune des tâches d'analyse sont reprises dans la fenêtre de statistique. Vous pouvez consulter le nombre d'objets soumis à l'analyse, le nombre d'objets malveillants découverts et le nombre d'objets qui doivent être traités. La synthèse affiche également l'heure de début et de fin de la dernière exécution de l'analyse et sa durée.

Les informations principales relatives aux résultats de l'analyse sont reprises sur les onglets suivants :

- *Détections* - contient tous les objets dangereux, découverts suite à l'exécution de la tâche ;

- *Événements* - contient la liste complète des événements survenus pendant l'exécution de la tâche ;
- *Statistiques* - contient des statistiques relatives au nombre d'objets analysés ;
- *Paramètres* - contient les paramètres qui définissent le fonctionnement de la tâche.

Si des erreurs surviennent pendant l'analyse, essayez de relancer la tâche. Si cette tentative se solde par un échec, enregistrez le rapport avec les résultats de l'exécution de la tâche dans un fichier t à l'aide du bouton **Enregistrer sous**. Envoyez ensuite le rapport au service d'assistance technique. Les experts de Kaspersky Lab répondront à vos questions.

➤ *Afin de parcourir les statistiques d'exécution de la tâche de recherche d'éventuels virus, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse (Analyse complète, Analyse rapide)**, formez une tâche de recherche et lancez-la. La progression de la tâche est illustrée dans la fenêtre principale. Cliquez sur le lien **Détails**, afin de passer à la fenêtre des statistiques.

DEFINITION DE PARAMETRES D'ANALYSE UNIQUES POUR TOUTES LES TACHES

Chaque tâche d'analyse s'exécute en fonction de ses paramètres. Les tâches créées lors de l'installation du programme sur l'ordinateur sont exécutées par défaut selon les paramètres recommandés par les experts de Kaspersky Lab.

Vous pouvez configurer des paramètres d'analyse uniques pour toutes les tâches. La sélection de paramètres utilisée pour la recherche de virus dans un objet particulier servira de base.

➤ *Pour définir des paramètres d'analyse uniques pour toutes les tâches, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Dans la partie droite de la fenêtre, dans le groupe **Paramètres des autres tâches**, cliquez sur le bouton **Appliquer**. Confirmez les paramètres uniques dans la boîte de dialogue de confirmation.

RESTAURATION DES PARAMETRES D'ANALYSE PAR DEFAUT

Lorsque vous configurez les paramètres d'exécution d'une tâche, vous avez toujours la possibilité de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

➤ *Pour restaurer les paramètres de protection des fichiers par défaut, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Cliquez sur le lien portant le nom du niveau de protection sélectionné pour le composant Antivirus Fichiers.
4. Cliquez sur le bouton **Par défaut** de la rubrique **Niveau de protection** dans la fenêtre qui s'ouvre.

MISE A JOUR DE L'APPLICATION

L'actualité de la protection est le garant de la sécurité. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillant apparaissent. Il est donc primordial de s'assurer que vos données sont bien protégées.

Lors de la mise à jour de l'application, les éléments suivants sont téléchargés et installés sur le serveur :

- **Les bases de l'application**

La protection des données est garantie par l'utilisation de bases de l'application. Elles sont utilisées par l'Antivirus Fichiers pour rechercher les objets dangereux sur le serveur et les neutraliser. Ces bases sont enrichies toutes les heures des définitions des nouvelles menaces et des moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

- **Les modules de l'application**

En plus des bases de Kaspersky Anti-Virus, vous pouvez actualiser les modules logiciels. Ces paquets de mise à jour suppriment des vulnérabilités de l'application, ajoutent de nouvelles fonctions ou améliorent les fonctions existantes.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour de Kaspersky Anti-Virus.

Pour réussir à télécharger les mises à jour depuis les serveurs, il faut que votre ordinateur soit connecté à Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres du serveur proxy ne sont pas définis automatiquement, configurez les paramètres de connexion à ce dernier.

Au cours du processus, les modules logiciels et les bases installés sur le serveur sont comparés à ceux de la source de mises à jour. Si les bases et les composants installés sur le serveur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les bases et les modules diffèrent, la partie manquante de la mise à jour sera installée sur le serveur. La copie des bases et des modules complets n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

Avant de lancer la mise à jour des bases, Kaspersky Anti-Virus réalise une copie des signatures installées au cas où vous souhaiteriez à nouveau l'utiliser pour une raison quelconque.

La possibilité d'annuler est indispensable, par exemple si les bases que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

Parallèlement à la mise à jour, vous pouvez copier les mises à jour obtenues dans une source locale. Ce service permet d'actualiser les bases antivirus et les modules logiciels sur les ordinateurs du réseau en réduisant le trafic Internet.

Vous pouvez également configurer le mode de lancement automatique de la mise à jour.

La section **Mise à jour** reprend les informations relatives à l'état actuel des bases de l'application.

Vous pouvez passer au rapport sur les mises à jour qui reprend les informations complètes relatives aux événements survenus lors de l'exécution de la tâche de mises à jour (bouton Journaux). Vous pouvez également prendre connaissance de l'activité virale sur le site www.kaspersky.com/fr (lien **Suivre l'activité virale**).

► *Pour modifier les paramètres d'une tâche de mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.

4. Dans la fenêtre qui s'ouvre, introduisez les modifications nécessaires dans les paramètres de la tâche sélectionnée.

➤ *Pour passer au rapport sur les mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Journaux**.

DANS CETTE SECTION

Lancement de la mise à jour	62
Annulation de la dernière mise à jour	63
Sélection de la source de mises à jour	63
Paramètres régionaux	64
Utilisation du serveur proxy	64
Mode de lancement : configuration du compte utilisateur.....	65
Mode de lancement : programmation	65
Sélection de l'élément à actualiser	66
Modification du mode de lancement de la tâche de mise à jour	66
Mise à jour depuis un répertoire local.....	67
Statistiques de la mise à jour.....	68
Problèmes possibles lors de la mise à jour	68

LANCEMENT DE LA MISE A JOUR

Vous pouvez lancer la mise à jour du logiciel à n'importe quel moment. Celle-ci sera réalisée au départ de la source de la mise à jour que vous aurez choisie.

La mise à jour de Kaspersky Anti-Virus peut être lancée de deux façons :

- au départ du menu contextuel ;
- au départ de la fenêtre principale du logiciel.

Les informations relatives au processus sont affichées dans la fenêtre principale de l'application.

N'oubliez pas que la copie des mises à jour dans une source locale aura lieu en même temps que l'exécution de la mise à jour, pour autant que ce service ait été activé.

➤ *Pour lancer la mise à jour de Kaspersky Anti-Virus depuis le menu contextuel, procédez comme suit :*

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.

2. Dans le menu qui s'ouvre, sélectionnez le point **Mise à jour**.

► *Pour lancer la mise à jour de Kaspersky Anti-Virus depuis la fenêtre principale du logiciel, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Lancer la Mise à jour**. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

ANNULATION DE LA DERNIERE MISE A JOUR

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Anti-Virus crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau les bases antérieures après une mise à jour ratée.

La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si une partie de la base est corrompue. Les bases locales peuvent être corrompues par l'utilisateur ou par un programme malveillant, ce qui est possible uniquement lorsque l'autodéfense de l'application est désactivée. Vous pouvez ainsi revenir aux bases antérieures et tenter de les actualiser à nouveau ultérieurement.

► *Pour revenir à l'utilisation de la version précédente des bases, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien **Restaurer les mises à jours précédentes**.

SELECTION DE LA SOURCE DE MISES A JOUR

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules de Kaspersky Anti-Virus.

Vous pouvez choisir parmi les sources de mises à jour suivantes :

- *Serveur d'administration* : entrepôt centralisé des mises à jour situé sur le serveur d'administration de Kaspersky Administration Kit (pour de plus amples informations, consultez le manuel de l'administrateur de "Kaspersky Administration Kit").
- *Serveurs de mise à jour de Kaspersky Lab* : sites Web spéciaux qui accueillent les mises à jour des signatures des menaces et des modules de l'ensemble des logiciels de Kaspersky Lab.
- *Serveurs HTTP ou FTP, répertoires locaux ou de réseau* : serveur ou répertoire local contenant l'ensemble des mises à jour.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 (495) 797 87 00 ou au +7 (495) 645-79-39 pour obtenir l'adresse d'un partenaire de Kaspersky Lab qui pourra vous donner la mise à jour sur disquette ou sur CD-ROM dans un fichier zip.

Les mises à jour obtenues sur un disque amovible peuvent être par la suite placées sur un site FTP ou HTTP ou dans un répertoire local ou de réseau.

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir la mise à jour des modules de l'application.

Si en guise de source de mises à jour vous avez sélectionné une ressource située hors de l'intranet, vous devrez être connecté à Internet pour télécharger la mise à jour.

Si plusieurs ressources ont été sélectionnées en guise de sources de mise à jour, le logiciel les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible.

➤ *Pour sélectionner la source de la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Cliquez sur le bouton **Configuration** de la rubrique **Paramètres de la mise à jour** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'affiche, sous l'onglet **Source des mises à jour** cliquez sur le bouton **Ajouter**.
6. Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le site FTP ou HTTP ou saisissez son adresse IP, son nom symbolique ou son adresse URL.

PARAMETRES REGIONAUX

Si vous utilisez les serveurs de Kaspersky Lab en guise de serveur de mise à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Les serveurs de Kaspersky Lab sont répartis entre plusieurs pays. En choisissant le serveur situé le plus proche de vous géographiquement, vous pouvez augmenter la vitesse de la mise à jour et du téléchargement de celle-ci.

➤ *Pour sélectionner le serveur le plus proche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Cliquez sur le bouton **Configuration** de la rubrique **Paramètres de la mise à jour** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Source des mises à jour**, dans le groupe **Paramètres régionaux**, sélectionnez l'option **Choisir dans la liste** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

Si vous choisissez l'option **Déterminer automatiquement**, la mise à jour utilisera les informations sur la région définie dans la base de registre du système d'exploitation.

UTILISATION DU SERVEUR PROXY

Si vous vous connectez à Internet via un serveur proxy, il faudra le configurer.

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

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Cliquez sur le bouton **Configuration** de la rubrique **Paramètres de la mise à jour** dans la fenêtre qui s'ouvre.

- Dans la fenêtre qui s'ouvre, sur l'onglet **Paramètres du proxy**, configurez les paramètres du serveur proxy.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Kaspersky Anti-Virus permet de lancer la mise à jour du logiciel au nom d'un autre compte utilisateur. Ce service est désactivé par défaut et les tâches sont lancées au nom du compte utilisateur en session (le compte sous lequel vous êtes enregistré dans le système).

Dans la mesure où la mise à jour peut être réalisée depuis une source à laquelle vous n'avez pas accès (par exemple, le répertoire de réseau de mise à jour) ou via un serveur proxy pour lequel vous n'avez pas d'autorisation, ce service vous permet de lancer la mise à jour au nom d'un autre utilisateur qui possède ces privilèges.

N'oubliez pas que sans l'utilisation de l'exécution avec les privilèges, la mise à jour programmée sera réalisée selon les privilèges du compte en session. Si aucun utilisateur n'est en session à ce moment et que le lancement de la mise à jour avec les privilèges d'un autre utilisateur n'a pas été configuré et que la mise à jour est programmée, l'actualisation sera lancée avec les privilèges SYSTEM.

➤ *Pour lancer la tâche avec les privilèges d'un autre compte, procédez comme suit :*

- Ouvrez la fenêtre principale de l'application.
- Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
- Cliquez sur le lien du mode de lancement défini.
- Cliquez sur le bouton **Configuration** de la rubrique **Paramètres de la mise à jour** dans la fenêtre qui s'ouvre.
- Dans la fenêtre qui s'ouvre sous l'onglet **Avancé** dans le bloc **Mode d'exécution** cochez la case **Lancer la tâche avec les privilèges de l'utilisateur**. Indiquez ensuite le compte utilisateur sous lequel la tâche sera exécutée : nom de compte et mot de passe.

MODE DE LANCEMENT : PROGRAMMATION

Toutes les tâches liées à la recherche de virus peuvent être lancées manuellement ou selon un horaire défini.

Lors de la programmation du lancement des tâches, il est nécessaire d'indiquer l'intervalle selon lequel l'événement doit avoir lieu.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

➤ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

- Ouvrez la fenêtre principale de l'application.
- Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
- Cliquez sur le lien du mode de lancement défini.
- Cliquez sur le bouton **Modifier** de la rubrique **Mode d'exécution** dans la fenêtre qui s'ouvre.
- Saisissez vos modifications dans la fenêtre **Programmation** qui ouvre.

➤ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

- Ouvrez la fenêtre principale de l'application.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Cliquez sur le bouton **Modifier** de la rubrique **Mode d'exécution** dans la fenêtre qui s'ouvre.
5. Dans la fenêtre **Programmation** qui s'ouvre, dans le groupe **Configuration de la programmation** cochez la case **Lancer la tâche ignorée**.

SELECTION DE L'ELEMENT A ACTUALISER

Les objets de la mise à jour désignent les objets qui seront actualisés :

- Les bases de l'application ;
- Les modules de l'application.

Les bases de l'application de sont toujours mises à jour tandis que les modules d'application le sont en fonction de la configuration.

Si une mise à jour des modules de l'application est présente à ce moment dans la source, Kaspersky Anti-Virus recevra les mises à jour requises et les appliquera après le redémarrage de l'ordinateur. Les mises à jour téléchargées ne seront pas installées tant que l'ordinateur ne sera pas redémarré.

Si la mise à jour suivante se produit avant le redémarrage de l'ordinateur et l'installation des mises à jour antérieure des modules de l'application, seule la mise à jour des signatures des menaces aura lieu.

► *Pour copier et installer les mises à jour des modules de l'application pendant la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Cochez la case **Actualiser les modules de l'application** dans le group **Paramètres de la mise à jour** de la fenêtre qui s'ouvre.



MODIFICATION DU MODE DE LANCEMENT DE LA TACHE DE MISE A JOUR

Le mode de lancement de la tâche de mise à jour de Kaspersky Anti-Virus est sélectionné lors du fonctionnement de l'Assistant de configuration de l'application (cf. section "Configuration de la mise à jour" à la page [27](#)). Il est possible de modifier le mode de lancement sélectionné.

L'exécution de la tâche de mise à jour peut se dérouler selon un des modes suivants :

- **Automatique**. Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source de la mise à jour. Si le logiciel découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode de mise à jour est activé par défaut.

Kaspersky Anti-Virus tentera de réaliser la mise à jour selon un intervalle défini lors de la mise à jour antérieure. Cela permet de régler automatiquement la fréquence des mises à jour en cas d'épidémie de virus ou d'autres situations dangereuses. Le logiciel recevra en temps opportuns les versions les plus récentes des bases et des modules de l'application, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

-  **Selon la programmation** (l'intervalle peut changer en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini.
-  **Manuel**. Vous lancez vous-même la procédure de mise à jour du logiciel. Kaspersky Anti-Virus vous avertira de la nécessité de réaliser la mise à jour.

➔ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Dans la fenêtre qui s'ouvre, dans le groupe **Mode d'exécution** sélectionnez le mode d'exécution de la tâche de mise à jour. Si vous avez choisi l'option Programmé, définissez l'horaire.

MISE A JOUR DEPUIS UN REPERTOIRE LOCAL

La procédure de récupération des mises à jour depuis un répertoire local est organisée de la manière suivante :

1. Un des ordinateurs du réseau récupère les mises à jour pour l'application et les signatures des menaces sur les serveurs de Kaspersky Lab ou sur tout autre serveur en ligne proposant les mises à jour les plus récentes. Les mises à jour ainsi obtenues sont placées dans un dossier partagé.
2. Les autres ordinateurs du réseau accèdent à ce dossier partagé afin d'obtenir les mises à jour.

Kaspersky Anti-Virus 6.0 ne récupère que les paquets indispensables à propre mise à jour depuis les serveurs de mise à jour de Kaspersky Lab. Nous vous conseillons de copier les mises à jour des autres applications Kaspersky Lab à l'aide de Kaspersky Administration Kit.

➔ *Pour activer le mode de copie des mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Dans la fenêtre qui s'affiche, cliquez sur **Configuration**.
5. Dans la fenêtre ouverte, onglet **Avancé**, bloc **Diffusion des mises à jour**, cochez la case **Copier les mises à jour dans le dossier**, et dans le champ ci-dessous définissez le chemin vers les dossiers communs, où les mises à jour seront placées. De plus, le chemin peut être sélectionné dans la fenêtre ouverte à l'aide du bouton **Parcourir**.

➔ *Afin que la mise à jour de l'application soit réalisée depuis le répertoire partagé sélectionné, réalisez les opérations suivantes sur tous les ordinateurs du réseau :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le lien du mode de lancement défini.
4. Dans la fenêtre qui s'affiche, cliquez sur **Configuration**.
5. Dans la fenêtre qui s'affiche, sous l'onglet **Source des mises à jour** cliquez sur le bouton **Ajouter**.

- Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le répertoire ou saisissez son chemin d'accès complet dans le champ **Source**.
- Dans l'onglet **Source des mises à jour**, désélectionnez la case **Serveurs de mise à jour de Kaspersky Lab**.

STATISTIQUES DE LA MISE A JOUR

Les informations globales sur le fonctionnement des tâches d'analyse sont reprises dans la fenêtre de statistique. Ici, vous pouvez voir les événements, qui se sont produits lors de l'exécution de la tâche (l'onglet *Evénements*) et parcourir la liste des paramètres selon lesquels la tâche s'exécute (l'onglet *Paramètres*).

Si des erreurs surviennent pendant l'analyse, essayez de relancer la tâche. Si cette tentative se solde par un échec, enregistrez le rapport avec les résultats de l'exécution de la tâche dans un fichier t à l'aide du bouton **Enregistrer sous**. Envoyez ensuite le rapport au service d'assistance technique. Les experts de Kaspersky Lab répondront à vos questions.

Une synthèse des statistiques de la mise à jour est reprise dans la partie inférieure de la fenêtre de statistique et contient la taille des mises à jour téléchargées et installées, la vitesse de la mise à jour, la durée de la procédure, etc.

➤ *Afin de parcourir les statistiques d'exécution de la tâche de recherche d'éventuels virus, procédez comme suit :*

- Ouvrez la fenêtre principale de l'application.
- Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**, formez une tâche de mise à jour et lancez-la. La progression de la tâche est illustrée dans la fenêtre principale. Le lien [détails](#) permet d'accéder à la fenêtre des statistiques.

PROBLEMES POSSIBLES LORS DE LA MISE A JOUR

Des erreurs liées à la mauvaise configuration des mises à jour, à des problèmes de connexion, etc. peuvent survenir lors de la mise à jour des modules de Kaspersky Anti-Virus ou des signatures des menaces. Cette section est consacrée à ces erreurs et aux moyens de les rectifier. Si vous êtes confronté à une erreur qui n'est pas décrite dans l'aide et si vous souhaitez obtenir des informations détaillées sur la manière de résoudre le problème adressez-vous au service d'assistance technique via le formulaire de contact en ligne.

ERREURS DE CONFIGURATION

Les erreurs de ce groupe sont généralement provoquées par une installation incorrecte de l'application ou par une modification de la configuration qui nuit au fonctionnement du logiciel.

Recommandations d'ordre général :

Lorsqu'une erreur de ce type se produit, il est conseillé de tenter de lancer à nouveau la mise à jour. Si l'erreur se reproduit, contactez le service d'assistance technique.

Si l'erreur est imputable à une installation incorrecte de l'application, il est conseillé de la réinstaller.

Aucune source de mise à jour n'est indiquée

Aucune des sources ne contient des fichiers pour la mise à jour. Il se peut qu'aucune source de mise à jour ne soit définie dans les paramètres. Vérifiez l'exactitude des paramètres de mise à jour et réessayez.

Erreur de vérification de la licence

Cette erreur se produit lorsque la clé de licence utilisée par l'application est bloquée ou lorsqu'elle figure dans la liste noire des licences.

Erreur de réception des paramètres de mise à jour

Erreur interne lors de la réception des paramètres de la mise à jour. Vérifiez l'exactitude des paramètres de mise à jour et réessayez.

Privilèges insuffisants pour la mise à jour

Cette erreur se produit lorsque le compte utilisé pour lancer la mise à jour ne jouit pas des privilèges d'accès à la source ou au répertoire contenant les mises à jour. Il est conseillé de vérifier si le compte jouit des privilèges nécessaires.

Cette erreur se produit également lors de la tentative de copie des fichiers de mise à jour dans un dossier qui ne peut être créé.

Erreur interne

Erreur interne de la logique de fonctionnement de la tâche de mise à jour. Vérifiez l'exactitude des paramètres de mise à jour et réessayez.

Erreur de vérification de la mise à jour

Cette erreur se produit lorsque les fichiers téléchargés depuis la source de mise à jour n'ont pas subi la vérification interne. Veuillez retenter la mise à jour plus tard.

ERREURS LIÉES A L'UTILISATION DES REPERTOIRES ET DES FICHIERS

Les erreurs de ce groupe surviennent lorsque les privilèges du compte au nom duquel la mise à jour est lancée ne permettent pas l'accès à la source de la mise à jour ou au répertoire contenant les mises à jour.

Recommandations d'ordre général :

Si vous êtes confronté à des erreurs de ce type, il est conseillé de vérifier si le compte utilisateur jouit des privilèges d'accès aux fichiers et répertoires indiqués.

Impossible de créer un répertoire

Cette erreur survient lorsqu'il est impossible de créer un répertoire lors de l'exécution de la mise à jour.

Privilèges insuffisants pour l'exécution d'opérations sur le fichier

Cette erreur survient si le compte utilisateur employé pour lancer la mise à jour ne jouit pas des privilèges suffisants pour exécuter des opérations sur les fichiers.

Fichier ou répertoire introuvable

Cette erreur survient lorsqu'un fichier ou un répertoire indispensable à la mise à jour est introuvable. Il est conseillé de vérifier si le fichier ou le répertoire indiqué existe et qu'il est accessible.

Erreur d'opération sur les fichiers

Cette erreur est une erreur interne de la logique de fonctionnement du module de mise à jour lors de l'exécution d'une opération sur les fichiers.

ERREURS DE RESEAU

Les erreurs de ce groupe sont le résultat de problèmes de communication ou d'une configuration incorrecte des paramètres de connexion.

Recommandations d'ordre général :

Si vous êtes confronté à une erreur de ce type, vérifiez si votre ordinateur est connecté au réseau, assurez-vous de l'exactitude des paramètres et confirmez la disponibilité de la source de la mise à jour. Ensuite, retentez la mise à jour. En cas de nouvel échec, contactez le service d'assistance technique.

Erreur de réseau

Une erreur s'est produite lors de la réception des fichiers de la mise à jour. Lorsque cette erreur se produit, vérifiez si votre ordinateur est bien connecté au réseau.

Déconnexion

Cette erreur se produit si pour une raison quelconque la connexion à la source de mise à jour est coupée.

Délai d'attente de l'opération de réseau écoule

Le délai d'attente pour la connexion à la source de la mise à jour est écoule. Au moment de la configuration des paramètres de la mise à jour, vous avez peut-être défini un délai d'attente trop court pour la connexion. Si l'ordinateur ne parvient pas à établir la connexion au serveur ou au répertoire de mise à jour dans ce délai, l'erreur se produit. Il est conseillé dans ce cas de vérifier l'exactitude des paramètres de la mise à jour ainsi que la disponibilité de la source de la mise à jour.

<p><i>Erreur d'autorisation sur le serveur FTP</i></p> <p>Cette erreur se produit si une faute a été commise lors de la saisie des paramètres d'autorisation pour l'accès au serveur FTP faisant office de source de la mise à jour. Vérifiez que les paramètres du serveur FTP autorisent le téléchargement de fichier pour ce compte utilisateur.</p>
<p><i>Erreur d'autorisation sur le serveur proxy</i></p> <p>Cette erreur se produit si une faute a été commise lors de la saisie du nom d'utilisateur ou du mot de passe dans la configuration de la connexion via un serveur proxy ou si le compte utilisateur utilisé pour la mise à jour ne dispose pas des privilèges d'accès suffisants à la source de la mise à jour. Corrigez les paramètres d'autorisation et retentez la mise à jour.</p>
<p><i>Erreur de résolution du nom DNS</i></p> <p>Cette erreur se produit lorsqu'aucune source de mise à jour n'a pu être identifiée. Il se peut que l'adresse n'ait pas été correctement saisie, que les paramètres de connexion au réseau soient erronés ou que le serveur DNS ne soit pas accessible. Il est conseillé de vérifier les paramètres de la mise à jour, la disponibilité de la source de mise à jour et de retenter l'opération.</p>
<p><i>Impossible d'établir la connexion avec la source de la mise à jour</i></p> <p>Cette erreur indique qu'il n'y a pas de connexion avec la source de mise à jour. Vérifiez l'exactitude de l'adresse de la source de mise à jour et réessayez.</p>
<p><i>Impossible d'établir la connexion avec le serveur proxy</i></p> <p>Cette erreur signifie que les paramètres de connexion au serveur proxy sont incorrects. Pour résoudre ce problème, vérifiez les paramètres et/ou la disponibilité du serveur proxy et retentez l'opération.</p>
<p><i>Erreur de résolution du nom DNS du serveur proxy</i></p> <p>Cette erreur se produit lorsque le serveur proxy est introuvable. Vérifiez l'exactitude des paramètres de connexion au serveur proxy et/ou la disponibilité du serveur DNS.</p>
<p>ERREURS LIEES A LA CORRUPTION DES BASES</p> <p>Les erreurs de ce groupe sont provoquées par la présence de fichiers corrompus dans la source de la mise à jour.</p> <p><u>Recommandations d'ordre général :</u></p> <p>Si vous tentez de réaliser la mise à jour depuis les serveurs de Kaspersky Lab, réessayez plus tard. En cas de nouvel échec, contactez le service d'assistance technique.</p> <p>Si vous réalisez la mise à jour au départ d'une autre source (par exemple, depuis un répertoire local), actualisez son contenu depuis un serveur de Kaspersky Lab. Si l'erreur se reproduit, contactez le service d'assistance technique.</p>
<p><i>Le fichier n'existe pas dans la source de mise à jour</i></p> <p>Tous les fichiers qui doivent être téléchargés et installés sur votre ordinateur au cours de la mise à jour sont repris dans un fichier spécial inclus dans le paquet. Cette erreur se produit lorsqu'un fichier quelconque figure dans la liste des fichiers à mettre à jour mais qu'il n'est pas présent physiquement sur la source.</p>
<p><i>Erreur de vérification de la signature</i></p> <p>Cette erreur peut être produite par l'application lorsque la signature numérique du paquet téléchargé est corrompue ou lorsqu'elle ne correspond pas à la signature de Kaspersky Lab.</p>
<p><i>L'index est corrompu ou manquant</i></p> <p>Cette erreur survient lorsque l'index au format xml, qui commande la mise à jour, est corrompu ou absent.</p>

ERREURS LIEES A LA MISE A JOUR DEPUIS LE SERVEUR D'ADMINISTRATION KASPERSKY ADMINISTRATION KIT
<p>Les erreurs de cette famille sont liées aux problèmes de mise à jour de l'application via le serveur d'administration Kaspersky Administration Kit.</p> <p><u>Recommandations d'ordre général :</u></p> <p>Tout d'abord, assurez-vous que Kaspersky Administration Kit et ses composants (serveur d'administration et agent d'administration) sont installés et en exécution. Réessayez la mise à jour. En cas de nouvel échec, relancez le serveur d'administration et l'agent d'administration et essayez à nouveau de réaliser la mise à jour. Si le problème persiste, contactez le service d'assistance technique.</p>
<p><i>Erreur de connexion au serveur d'administration</i></p> <p>Cette erreur survient si la connexion au serveur d'administration Kaspersky Administration Kit est impossible. Il est conseillé de s'assurer que l'agent d'administration est bien installé et qu'il tourne.</p>
<p><i>Erreur d'enregistrement dans l'agent d'administration</i></p> <p>Si cette erreur se manifeste, suivez les recommandations générales applicables aux erreurs de cette catégorie. Si l'erreur se reproduit, récupérez le fichier de rapport détaillé de la mise à jour et de l'agent d'administration sur cet ordinateur et envoyez-le au service d'assistance technique via le formulaire en ligne en décrivant la situation.</p>
<p><i>Impossible d'établir une connexion. Le serveur d'administration est surcharge et il ne peut répondre à la requête</i></p> <p>Dans ce cas, Kaspersky recommande de tenter la mise à jour plus tard.</p>
<p><i>Impossible d'établir la connexion avec le serveur d'administration / avec le serveur d'administration principale / l'agent d'administration, erreur physique / erreur inconnue</i></p> <p>Si vous êtes confronté à ce genre d'erreurs, retentez la mise à jour plus tard. En cas de nouvel échec, contactez le service d'assistance technique.</p>
<p><i>Erreur de réception du fichier du serveur d'administration, argument incorrect pour le transport</i></p> <p>Si cette erreur se reproduit ultérieurement, contactez le service d'assistance technique.</p>
<p><i>Erreur de réception du fichier du serveur d'administration</i></p> <p>Si vous êtes confronté à ce genre d'erreurs, retentez la mise à jour plus tard. En cas de nouvel échec, contactez le service d'assistance technique.</p>
CODES DIVERS
<p>Ce groupe reprend les erreurs qui n'appartiennent à aucune des catégories citées ci-dessus.</p>
<p><i>Les fichiers pour la remise à l'état antérieur manquent</i></p> <p>Cette erreur se produit si une tentative de remise à l'état antérieur est réalisée après la remise à l'état antérieur à la mise à jour sans qu'une mise à jour ait été réalisée entre les deux. La deuxième remise à l'état antérieur est impossible tant qu'une mise à jour n'aura pas été exécutée et à la suite de laquelle la sélection de sauvegarde des fichiers aura été restaurée.</p>

CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de l'application vous permet d'accéder rapidement aux paramètres principaux de Kaspersky Anti-Virus 6.0.

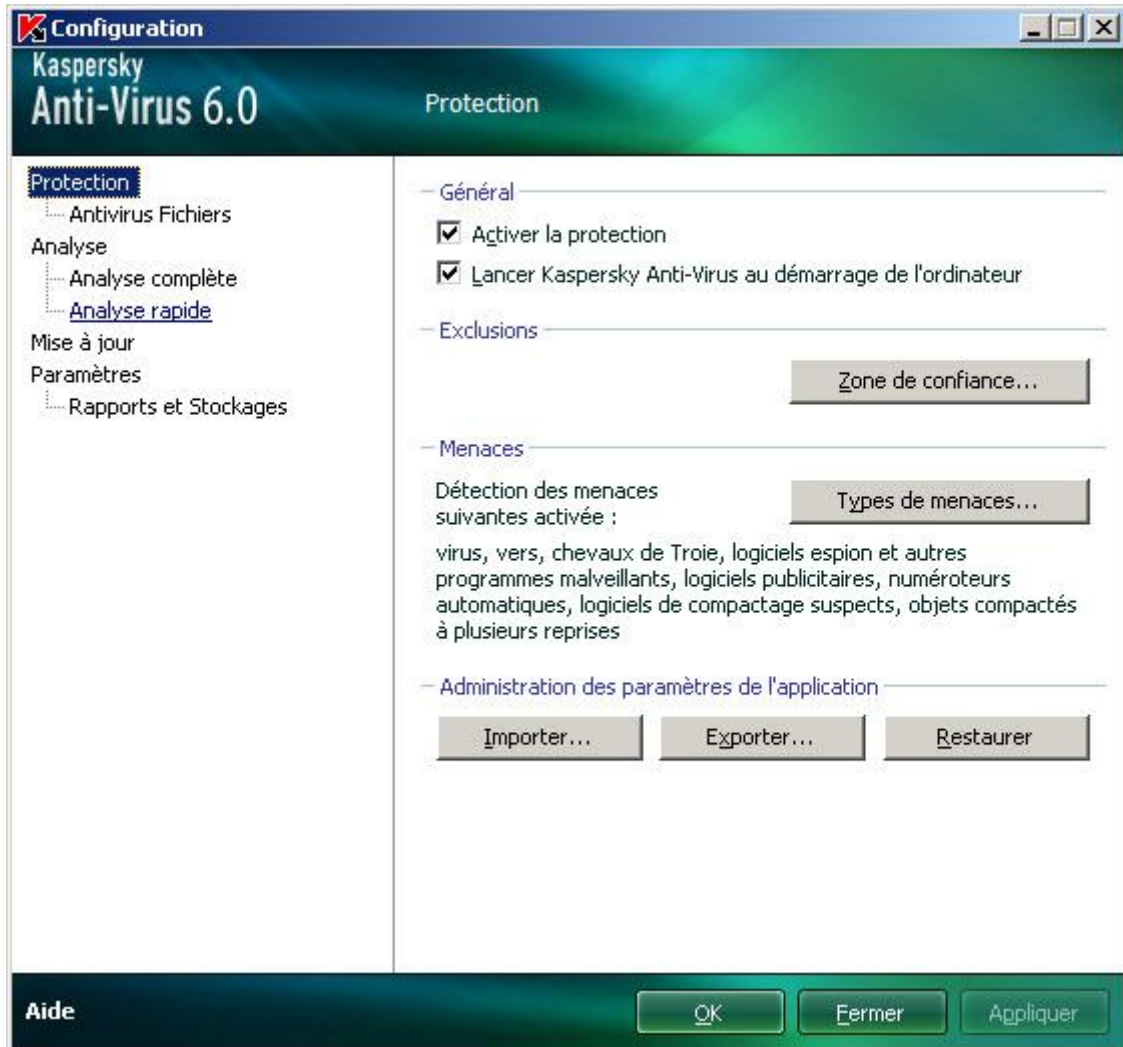


Illustration 9. Fenêtre de configuration des paramètres de l'application

La fenêtre contient deux parties :

- la partie gauche permet d'accéder à l'Antivirus Fichiers, aux tâches de recherche de virus, à la mise à jour, etc. ;
- la partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionnés dans la partie gauche.

Vous pouvez ouvrir la fenêtre d'une des manières suivantes :

- Au départ de la fenêtre principale du logiciel. Pour ce faire, cliquez sur le bouton **Configuration** dans la partie supérieure de la fenêtre.

- Au départ du menu contextuel. Pour ce faire, sélectionnez l'élément **Configuration** dans le menu contextuel de l'application.



Illustration 10. Menu contextuel

DANS CETTE SECTION

Protection	73
Antivirus Fichiers	80
Analyse.....	80
Mise à jour.....	81
Paramètres.....	81
Rapports et Stockages	87

PROTECTION

La fenêtre **Protection** vous permet d'utiliser les fonctions complémentaires suivantes de Kaspersky Anti-Virus :

- Désactivation / activation de la protection de l'application (cf. page [74](#)).
- Lancement de l'application au démarrage du système d'exploitation (cf. page [74](#)).
- Sélection des catégories de menaces identifiées (cf. page [74](#)).
- Constitution de la zone de confiance (cf. page [75](#)) :
 - création d'une règle d'exclusion (cf. page [75](#)) ;
 - composition de la liste des applications de confiance (cf. page [78](#)) ;
 - exportation / importation des composants de la zone de confiance (cf. page [78](#)).
- Exportation / importation des paramètres de fonctionnement de l'application (cf. page [79](#)).
- Restauration des paramètres de fonctionnement de l'application par défaut (cf. page [79](#)).

DESACTIVATION/ACTIVATION DE LA PROTECTION DE L'ORDINATEUR

Kaspersky Anti-Virus est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. L'Antivirus Fichiers fonctionne.

Vous pouvez désactiver complètement la protection offerte par l'Antivirus Fichiers.

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection** car cela pourrait entraîner l'infection du serveur et la perte de données.

Cette action entraînera l'arrêt du fonctionnement de l'Antivirus Fichiers. La désactivation du fonctionnement de composant n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Anti-Virus.

➤ *Pour désactiver complètement la protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Désélectionnez la case **Activer la protection**.

LANCEMENT DE L'APPLICATION AU DEMARRAGE DU SYSTEME D'EXPLOITATION.

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Anti-Virus, sélectionnez le point **Quitter** dans le menu contextuel du programme. Celui-ci sera déchargé de la mémoire vive. Ce qui signifie que l'ordinateur ne sera plus protégé à partir de ce moment.

Pour activer à nouveau la protection de l'ordinateur, vous pourrez charger l'application depuis le menu **Démarrer** → **Programmes** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**.

Il est possible également de lancer la protection automatiquement après le redémarrage du système d'exploitation.

➤ *Pour activer le mode de lancement de l'application au démarrage du système d'exploitation, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Cochez la case **Lancer Kaspersky Anti-Virus au démarrage de l'ordinateur**.

SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Kaspersky Anti-Virus vous protège contre divers types de programmes malveillants. Quels que soient les paramètres définis, l'application recherche toujours et neutralise les virus et les chevaux de Troie. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

➤ *Pour sélectionner les catégories de menaces à identifier, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Dans le bloc **Menaces** cliquez sur **Types de menaces**.

4. Dans la fenêtre **Types de menaces** qui s'ouvre, cochez les cases pour les catégories de menaces contre lesquelles vous souhaitez protéger votre ordinateur.

CONSTITUTION DE LA ZONE DE CONFIANCE

La *Zone de confiance* est en réalité une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par Kaspersky Anti-Virus. En d'autres termes, il s'agit des éléments exclus de la protection offerte par le programme.

Cette zone de confiance peut être définie par l'utilisateur sur la base des particularités des objets qu'il manipule et des programmes installés sur l'ordinateur. La constitution de cette liste d'exclusions peut s'avérer utile si Kaspersky Anti-Virus bloque l'accès à un objet / un programme quelconque alors que vous êtes convaincu que celui-ci est tout à fait sain.

Il est possible d'exclure des fichiers d'un certain format, des fichiers selon un masque, certains secteurs (par exemple, un répertoire ou un programme), des processus ou des objets en fonction d'un verdict (état attribué à l'objet par Kaspersky Anti-Virus suite à l'analyse).

Les objets exclus ne sont pas analysés lors de l'analyse du disque ou du dossier où ils se trouvent. Toutefois, en cas de sélection de l'analyse de cet objet précis, la règle d'exclusion ne sera pas appliquée.

► Pour constituer la liste des exclusions de la protection, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Cliquez sur le bouton **Zone de confiance** dans le groupe **Exclusions**.
4. Dans la fenêtre qui s'ouvre, configurez les règles d'exclusion pour les objets (cf. page [75](#)) et composez également une liste d'applications de confiance (cf. page [78](#)).

VOIR ÉGALEMENT

Création d'une règle d'exclusion.....	75
Masques autorisés pour l'exclusion des fichiers.....	76
Masques d'exclusion autorisés selon le classement de l'encyclopédie des virus.....	77
Composition de la liste des applications de confiance	78
Exportation / importation des composants de la zone de confiance.....	78

CREATION D'UNE REGLE D'EXCLUSION

Les *règles d'exclusions* sont des ensembles de conditions qui permettent à Kaspersky Anti-Virus de savoir qu'il ne doit pas analyser un objet.

Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus logiciels ou des objets selon un verdict.

Type de menace – est l'état assigné par Kaspersky Anti-Virus à un objet au cours de l'analyse. Le type de menace est rendu sur la base du classement des programmes malveillants et des riskwares présentés dans l'encyclopédie des virus de Kaspersky Lab.

Les programmes présentant un risque potentiel n'ont aucune fonction malicieuse mais ils pourraient être exploités par un individu mal intentionné en guise de soutien à un programme malicieux en raison des failles ou des erreurs qu'il contient. Cette catégorie regroupe par exemple les programmes d'administration à distance, les clients IRC, les serveurs FTP,

tous les utilitaires pour l'arrêt des processus ou la dissimulation de leur activité, les enregistreurs de frappes, les programmes d'identification des mots de passe, les numéroteurs automatiques vers des sites payants etc. Ces programmes ne sont pas considérés comme un virus (not-a-virus) mais ils peuvent être répartis en différentes catégories telles que les adwares, les jokewares, les riskwares ; etc. (pour obtenir de plus amples informations sur les programmes malveillants découverts par Kaspersky Anti-Virus, consultez l'Encyclopédie des virus à l'adresse www.viruslist.com/fr (<http://www.viruslist.com/fr/virus/encyclopedia>)). Ces programmes peuvent être bloqués suite à l'analyse. Et vu que certains d'entre eux sont largement utilisés, il est possible de les exclure de l'analyse. Pour ce faire, il faut ajouter à la zone de confiance le nom ou le masque de la menace selon le classement de l'Encyclopédie des virus.

Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'un système d'accès à distance qui permet de travailler sur un ordinateur distant. Kaspersky Anti-Virus considère ce type d'activité logicielle comme potentiellement dangereuse et peut donc la bloquer. Afin d'éviter le blocage de l'application, il faut composer une règle d'exclusion pour laquelle le verdict sera Remote Admin.

L'ajout d'une exclusion s'accompagne de la création d'une règle qui pourra être exploitée par l'Antivirus Fichiers et lors de l'exécution des tâches d'analyse antivirus.

➤ *Pour créer une règle d'exclusion, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Cliquez sur le bouton **Zone de confiance** dans le groupe **Exclusions**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur **Ajouter**.
5. Dans la fenêtre **Règle d'exclusion** qui apparaît, sélectionnez le type d'exclusion dans la section **Paramètres**. Ensuite, dans le groupe **Description** associez des valeurs aux types d'exclusion sélectionnés et définissez les composants de Kaspersky Anti-Virus qui exploiteront la règle ainsi créée.

➤ *Pour créer une règle d'exclusion au départ de la fenêtre du rapport, procédez comme suit :*

1. Sélectionnez dans le rapport l'objet que vous souhaitez ajouter aux exclusions.
2. Pour cet objet, dans le menu contextuel, sélectionnez le point **Ajouter à la zone de confiance**.
3. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, vérifiez si tous les paramètres vous conviennent. Les champs reprenant le nom de l'objet et le type de menace attribué sont remplis automatiquement sur la base des renseignements qui figurent dans la notification. Afin de créer une règle, cliquez sur **OK**.

MASQUES AUTORISÉS POUR L'EXCLUSION DES FICHIERS

Voici des exemples de masques autorisés que vous pouvez utiliser dans la composition de la liste des fichiers à exclure :

1. Masques sans chemins d'accès aux fichiers :
 - ***.exe** : tous les fichiers avec extension *exe* ;
 - **tous les fichiers *.exe** - tous les fichiers avec extension *ex?*, où ? peut représenter tout caractère singulier ;
 - **test** : tous les fichiers avec le nom *test*.
2. Masques avec chemins d'accès absolus aux fichiers :
 - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** : tous les fichiers du répertoire *C:\dir* ;
 - **C:\dir*.exe** : tous les fichiers avec l'extension *exe* dans le répertoire *C:\dir* ;
 - **C:\dir*.ex?** : tous les fichiers portant l'extension *ex?* dans le répertoire *C:\dir*, où ? peut représenter tout caractère singulier ;

- **C:\dir\test** : uniquement le fichier *C:\dir\test*.

Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case **Sous-répertoire compris** lors de la définition du masque.

3. Masques de chemins d'accès aux fichiers :

- **dir*.*** ou **dir*** ou **dir** : tous les fichiers dans tous les répertoires *dir* ;
- **dir\test** : tous les fichiers *test* dans les répertoires *dir* ;
- **dir*.exe** : tous les fichiers portant l'extension *exe* dans tous les répertoires *dir* ;
- **dir*.ex?** : tous les fichiers portant l'extension *ex?* dans tous les répertoires *dir*, où ? peut représenter tout caractère singulier.

Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case **Sous-répertoire compris** lors de la définition du masque.

L'utilisation des masques d'exclusion ***.*** ou ***** est admissible uniquement lors de l'indication de la classification des menaces exclues selon l'Encyclopédie des virus. Dans ce cas, la menace indiquée ne sera pas décelée dans tous les objets. L'utilisation de ces masques sans indication de la classification revient à désactiver la protection. Il n'est pas recommandé de sélectionner, en tant qu'exclusion, le chemin d'accès appartenant au disque virtuel, généré à la base du catalogue du système de fichiers par la commande *subst*, aussi qu'au disque qui est l'image du dossier de réseau. Il se fait que différents utilisateurs peuvent attribuer le même nom à différentes ressources, ce qui va entraîner des erreurs au niveau de l'application des règles d'exclusion.

VOIR ÉGALEMENT

Masques d'exclusion autorisés selon le classement de l'encyclopédie des virus [77](#)

MASQUES D'EXCLUSION AUTORISÉS SELON LE CLASSEMENT DE L'ENCYCLOPÉDIE DES VIRUS

Pour ajouter des menaces d'un verdict particulier (conforme au classement de l'encyclopédie des virus) en guise d'exclusion, vous pouvez indiquer les données suivantes :

- le nom complet de la menace, tel que repris dans l'encyclopédie des virus sur www.viruslist.com/fr (<http://www.viruslist.com/fr/viruses/encyclopedia>) (par exemple, **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**) ;
- Le nom de la menace selon un masque, par exemple :
 - **not-a-virus*** - exclut de l'analyse les logiciels licites mais potentiellement dangereux, ainsi que les jokewares ;
 - ***Riskware.*** - exclut de l'analyse tous les types de logiciels présentant un risque potentiel de type Riskware ;
 - ***RemoteAdmin.*** : exclut de l'analyse toutes les versions de logiciel d'administration à distance.

VOIR ÉGALEMENT

Masques autorisés pour l'exclusion des fichiers [76](#)

COMPOSITION DE LA LISTE DES APPLICATIONS DE CONFIANCE

Vous pouvez créer une liste d'applications de confiance dont l'activité, y compris les activités suspectes, les activités de fichiers, les activités de réseau et les requêtes adressées à la base de registre système ne sera pas contrôlée.

Par exemple, vous estimez que les objets utilisés par le programme **Bloc-notes** de Microsoft Windows sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance aux processus de ce programme. Afin d'exclure de l'analyse les objets utilisés par ce processus, ajoutez le programme **Bloc-notes** à la liste des applications de confiance. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

De plus, certaines actions considérées comme dangereuses sont en réalité normales dans le cadre du fonctionnement de divers programmes. Par exemple, l'interception du texte que vous saisissez à l'aide du clavier est tout à fait normale dans le cadre des logiciels qui permutent automatiquement la disposition du clavier en fonction de la langue (Punto Switcher, etc.). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

L'exclusion de ces applications de confiance peut également résoudre de possibles conflits de compatibilité entre Kaspersky Anti-Virus et d'autres applications (par exemple, le trafic réseau depuis un autre ordinateur, déjà analysé par l'application antivirus) et accélérer le rendement de l'ordinateur, ce qui est spécialement important lorsqu'on utilise des applications serveur.

Par défaut, Kaspersky Anti-Virus analyse les objets ouverts, exécutés ou enregistrés par tous les processus logiciels, il surveille l'activité ainsi que le trafic réseau généré par tous les programmes.

► *Pour ajouter une application à la liste des applications de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Cliquez sur le bouton **Zone de confiance** dans le groupe **Exclusions**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Applications de confiance**, cliquez sur **Ajouter**.
5. Dans la fenêtre **Application de confiance** qui s'ouvre, sélectionnez l'application à l'aide du bouton **Parcourir**. Cette action entraîne l'affichage d'un menu contextuel qui vous permettra au départ du point **Parcourir** de passer à la boîte de dialogue standard de sélection des fichiers et d'indiquer le chemin d'accès au fichier exécutable ou de consulter la liste des applications ouvertes à l'instant au départ du point **Applications** et de sélectionner l'application souhaitée. Pour l'application sélectionnée, indiquez les paramètres nécessaires.

EXPORTATION / IMPORTATION DES COMPOSANTS DE LA ZONE DE CONFIANCE

A l'aide d'exportation et importation, vous pouvez transférer les règles d'exclusions déjà créées et les listes des applications de confiance aux autres ordinateurs.

► *Afin de copier les règles d'exclusion créées, exécutez l'opération suivante :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Cliquez sur le bouton **Zone de confiance** dans le groupe **Exclusions**.
4. Dans la fenêtre ouverte, sous l'onglet **Règles d'exclusion** utilisez les boutons **Exporter** et **Importer**, afin d'exécuter les actions nécessaires pour la copie des règles.

► *Pour copier la liste composée des applications de confiance, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.

3. Cliquez sur le bouton **Zone de confiance** dans le groupe **Exclusions**.
4. Dans la fenêtre ouverte, sous l'onglet **Applications de confiance** utilisez les boutons **Exporter** et **Importer**, afin d'exécuter les actions nécessaires pour la copie de la liste.

EXPORTATION ET IMPORTATION DES PARAMÈTRES DE FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus offre la possibilité d'exporter et d'importer les paramètres.

Cela est utile si vous avez installé le logiciel sur un ordinateur chez vous et au bureau. Vous pouvez configurer le logiciel selon un mode qui vous convient pour le travail à domicile, conserver ces paramètres sur le disque et à l'aide de la fonction d'importation, les importer rapidement sur votre ordinateur au travail. Les paramètres sont enregistrés dans un fichier de configuration spécial.

➤ *Pour exporter les paramètres actuels de fonctionnement de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Exporter**.
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

➤ *Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Importer**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky Anti-Virus.

RESTAURATION DES PARAMÈTRES PAR DEFAUT

Vous pouvez toujours revenir aux paramètres recommandés de Kaspersky Anti-Virus. Ces paramètres sont les paramètres optimaux recommandés par les experts de Kaspersky Lab. La restauration s'opère à l'aide de l'Assistant de configuration initiale du logiciel.

La fenêtre qui s'ouvre vous permet de définir les paramètres que vous souhaitez conserver en même temps que le rétablissement du niveau de sécurité recommandé.

Lorsque vous aurez quitté l'Assistant, tous les composants de la protection fonctionneront selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidés de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

➤ *Pour restaurer les paramètres de protection, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Restaurer**.
4. Dans la fenêtre qui s'ouvre, cochez les cases pour les paramètres qui doivent être enregistrés. Cliquez sur **Suivant**. L'Assistant de configuration initiale sera lancé. Suivez ses instructions.

ANTIVIRUS FICHIERS

Cette fenêtre regroupe les paramètres du composant **Antivirus Fichiers** (cf. section "Protection antivirus du système de fichiers de l'ordinateur" à la page [39](#)). En modifiant les valeurs des paramètres, vous pouvez :

- modifier le niveau de protection (cf. page [41](#)) ;
- modifier l'action à appliquer aux objets identifiés (cf. page [41](#)) ;
- constituer la couverture de protection (cf. page [42](#)) ;
- optimiser l'analyse (cf. page [44](#)) ;
- configurer l'analyse des fichiers composés (cf. page [44](#)) ;
- modifier le mode d'analyse (cf. page [45](#)) ;
- utiliser l'analyse heuristique (cf. page [43](#)) ;
- suspendre le composant (cf. page [46](#)) ;
- sélectionner la technologie d'analyse (cf. page [46](#)) ;
- restaurer les paramètres de protection par défaut (cf. page [47](#)), pour autant qu'ils aient été modifiés.

➔ *Pour passer à la configuration des paramètres d'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Antivirus Fichiers**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres d'Antivirus Fichiers.

ANALYSE

L'ensemble de paramètres définis pour chaque tâche détermine le mode d'exécution de l'analyse des objets sur l'ordinateur.

Les experts de Kaspersky Lab ont défini plusieurs tâches d'analyse antivirus. Notamment :

Analyse

Analyse des objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.

Analyse complète

Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.

Analyse rapide

Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

La boîte de dialogue de configuration des tâches vous offre la possibilité de :

- sélectionner le niveau de protection (cf. page [52](#)), pour l'exécution de la tâche ;
- sélectionner l'action (cf. page [53](#)), qui sera exécutée en cas de découverte d'un objet infecté ou probablement infecté ;
- programmer le lancement automatique (cf. page [58](#)) de la tâche ;
- définir les types de fichiers (cf. page [54](#)), soumis à l'analyse antivirus ;
- définir les paramètres d'analyse des fichiers composés (cf. page [55](#)) ;
- sélectionner les méthodes et les technologies d'analyse (cf. page [56](#)) ;
- définir des paramètres d'analyse uniques pour toutes les tâches (cf. page [60](#)).

➔ *Pour passer à la configuration des paramètres de la tâche, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse (Analyse complète, Analyse rapide)**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection requis, la réaction face à la menace et définissez le mode d'exécution. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres des tâches. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut**.

MISE A JOUR

La mise à jour de Kaspersky Anti-Virus s'exécute selon les paramètres qui définissent :

- la source (cf. page [63](#)) d'où les fichiers de la mise à jour de l'application seront copiés avant d'être installés ;
- le mode de lancement (cf. page [66](#)) du processus de mise à jour de l'application et les éléments actualisés ;
- la fréquence d'exécution de la mise à jour si l'exécution programmée (cf. page [65](#)) a été définie ;
- le compte utilisateur (cf. page [65](#)) avec les privilèges duquel la mise à jour sera exécutée ;
- la nécessité de copier les mises à jour téléchargées dans une source locale (cf. page [67](#)) ;
- utilisation du serveur proxy (cf. page [64](#)).

➔ *Pour passer à la configuration des paramètres de la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans la partie droite de la fenêtre, sélectionnez le mode de lancement requis. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres de la tâche.

PARAMETRES

La fenêtre **Paramètres** vous permet d'utiliser les fonctions complémentaires suivantes de Kaspersky Anti-Virus :

- Autodéfense du logiciel (cf. page [82](#)).
- Restriction de l'accès à l'application (cf. page [82](#)).

- Restriction de taille des fichiers iSwift (cf. page [83](#)).
- Performance des serveurs dotés de plusieurs processeurs (cf. page [83](#)).
- Notifications relatives aux événements de Kaspersky Anti-Virus (cf. page [84](#)) :
 - sélection du type d'événement et de mode d'envoi des notifications (cf. page [85](#)) ;
 - configuration de l'envoi des notifications par courrier électronique (cf. page [85](#)) ;
 - configuration des paramètres du journal des événements (cf. page [86](#)).
- Éléments actifs de l'interface (cf. page [86](#)).

AUTODEFENSE DU LOGICIEL

Kaspersky Anti-Virus protège les ordinateurs contre les programmes malveillants et pour cette raison, elle constitue une cible de choix pour les programmes malveillants qui tentent de le bloquer ou de le supprimer de l'ordinateur.

Pour garantir la stabilité du système de sécurité de votre ordinateur, l'application prévoit des mécanismes d'auto-défense et de protection contre les actions externes.

Sous la version 64 bits de Microsoft Windows Server 2008 (sans Service Pack) et de Microsoft Windows Server 2003, seule la protection contre les modifications ou la suppression des fichiers de l'application sur le disque et des entrées de la base de registres système est accessible.

En cas d'utilisation de la protection contre l'interaction à distance, il faut donner l'accès à l'application à un programme d'administration à distance (par exemple, RemoteAdmin). Pour cette raison, il est indispensable d'ajouter ces programmes dans la liste des applications de confiance et d'activer pour ceux-ci le paramètre **Autoriser l'interaction avec l'interface de l'application**.

► Afin d'activer l'utilisation des mécanismes d'autodéfense du logiciel, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le groupe **Autodéfense**, cochez la case **Activer l'autodéfense** pour activer le mécanisme de protection du programme contre la modification ou la suppression de ces propres fichiers sur le disque, des processus en mémoire et des enregistrements dans la base de registre système.

Dans le groupe **Autodéfense**, cochez la case **Désactiver la possibilité d'administration externe du service système** pour bloquer toute tentative d'administration à distance des services de l'application.

Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la zone de notification de la barre des tâches de Microsoft Windows en cas de tentative d'exécution des actions citées (pour autant que le service n'ait pas été désactivé par l'utilisateur).

RESTRICTION DE L'ACCES A L'APPLICATION

Un ordinateur personnel peut être utilisé par plusieurs personnes, qui ne possèdent pas toutes les mêmes connaissances en informatique. L'accès ouvert au logiciel et à ces paramètres peut considérablement réduire le niveau de la protection globale de l'ordinateur.

Pour renforcer la sécurité de l'ordinateur, imposez un mot de passe pour l'accès à Kaspersky Anti-Virus. Vous pouvez bloquer toutes les actions, à l'exception des notifications en cas de découverte d'objets dangereux ou interdire l'une des actions suivantes :

- modification des paramètres de fonctionnement de l'application ;

- arrêt de l'application ;
- désactivation du fonctionnement d'Antivirus Fichiers ou des tâches d'analyse ;
- désactivation de la stratégie (en cas d'utilisation de l'application via Kaspersky Administration Kit) ;
- suppression de l'application.

Chacune de ces actions entraîne une réduction du niveau de protection de votre ordinateur, aussi vous devez faire confiance aux personnes à qui vous confiez ces tâches.

➔ *Pour protéger l'accès à l'application à l'aide d'un mot de passe, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le groupe **Protection par mot de passe**, cochez la case **Activer la protection par mot de passe** puis cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Protection par un mot de passe** qui s'ouvre, saisissez le mot de passe et définissez le domaine d'application des restrictions. Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions que vous avez sélectionnées, il devra saisir le mot de passe.

RESTRICTION DE TAILLE DES FICHIERS ISWIFT

Les fichiers iSwift – ce sont les fichiers qui contiennent l'information sur les objets déjà analysés du système fichier NTFS sur la présence de virus (technologie iSwift). La présence de ces fichiers permet d'accélérer l'analyse des objets, puisque Kaspersky Anti-Virus analyse seulement les fichiers qui ont été modifiés depuis la dernière analyse. Avec le temps les fichiers iSwift deviennent assez volumineux. Il est conseillé de définir une limite sur la taille de ces fichiers. Le fichier iSwift sera purgé dès que la limite sera atteinte.

➔ *Pour limiter la taille des fichiers iSwift, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Ressources** cochez la case **Remettre la base iSwift à zéro quand elle atteint** et dans le champ d'à côté, saisissez la taille de base en Mo.

POSTE SERVEUR MULTIPROCESSEUR

Lors de l'utilisation d'une configuration multiprocesseur du serveur, vous pouvez configurer la Performance du serveur, en utilisant les procédés suivants :

- Définir le nombre de copies du moteur antivirus chargées au lancement de Kaspersky Anti-Virus sur le serveur (c.-à-d. le nombre des processus antivirus lancés parallèlement sur le serveur).

Plus le nombre de copies du moteur de l'antivirus est grand, et plus les opérations antivirus sont traitées rapidement. Cependant, ceci affecte le rendement général du serveur. Les dérangements de fonctionnement d'Antivirus Fichiers sont possibles quand la capacité de la mémoire RAM est insuffisante et un grand nombre de copies du moteur de l'antivirus est en exécution.

En outre, l'exécution de nombreux processus antivirus simultanés sur le serveur garantit que le serveur restera toujours protégé dans le cas où l'un des moteurs subit une erreur.

- Régler la charge du serveur : par exemple réserver une partie des processeurs au traitement antivirus et l'autre, aux tâches directes du serveur.

Les experts de Kaspersky Lab recommandent de réserver au moins un processeur dans les systèmes multiprocesseurs aux tâches du serveur.

➔ *Afin de définir le nombre de copies du moteur antivirus, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Performance** cliquez sur le bouton **Détails**.
4. Dans la fenêtre **Configuration multi-processeurs** qui s'ouvre, dans le bloc **Paramètres**, indiquez le nombre de copies du moteur antivirus.

➔ *Afin d'équilibrer la charge sur le serveur, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section Paramètres.
3. Dans le bloc Performance cliquez sur le bouton Détails.
4. Dans la fenêtre **Configuration multi-processeurs** qui s'ouvre, dans le bloc **Processeurs utilisés** décochez les cases en regard du processeur à réserver exclusivement au travail du serveur.

NOTIFICATIONS RELATIVES AUX EVENEMENTS DE KASPERSKY ANTI-VIRUS

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus. Elles peuvent avoir un caractère purement informatif ou présenter des informations cruciales. Par exemple, la notification peut signaler la réussite de la mise à jour ou signaler une erreur dans le fonctionnement d'un composant qu'il faudra rectifier au plus vite.

Pour rester au courant des événements qui surviennent dans le fonctionnement de Kaspersky Anti-Virus, utilisez le service de notifications.

La notification peut être réalisée de l'une des manières suivantes :

- messages contextuels au-dessus de l'icône de l'application dans la barre des tâches ;
- notification sonore ;
- messages électroniques ;
- enregistrement des informations dans le journal d'événements.

➔ *Pour activer le service de notification, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Apparence**, cochez la case **Activer les notifications sur les événements** et cliquez sur **Configuration**.
4. Dans la fenêtre **Configuration des notifications** qui s'ouvre, définissez le type d'événements de Kaspersky Anti-Virus au sujet desquels vous souhaitez être averti, ainsi que le mode de notification.

VOIR ÉGALEMENT

Sélection du type d'événement et de mode d'envoi des notifications	85
Configuration de l'envoi des notifications par courrier électronique.....	85
Configuration des paramètres du journal des événements	86

SELECTION DU TYPE D'ÉVÉNEMENT ET DE MODE D'ENVOI DES NOTIFICATIONS

Pendant les opérations de Kaspersky Anti-Virus, les types d'événement suivants peuvent se produire :

- **Événements critiques.** Événements critiques au sujet desquels il est vivement conseillé d'être averti car ils indiquent un problème dans le fonctionnement du logiciel ou une vulnérabilité dans la protection de l'ordinateur. Par exemple, *les bases sont fortement dépassées* ou *la durée de validité de la licence est écoulée*.
- **Refus de fonctionnement.** Événements entraînant le non-fonctionnement de l'application. Par exemple, *les bases sont manquantes ou corrompues*.
- **Événements importants.** Événements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le fonctionnement du logiciel. Par exemple, *les bases sont dépassées* ou *la durée de validité de la licence arrive à échéance*.
- **Événements informatifs.** Événements à caractère purement informatif qui ne contiennent aucune information cruciale. Par exemple, *objet placé en quarantaine*.

➔ Afin d'indiquer les événements au sujet desquels vous souhaitez être averti et de quelle manière, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Apparence**, cochez la case **Activer les notifications sur les événements** et cliquez sur **Configuration**.
4. Dans la fenêtre **Configuration des notifications** qui s'ouvre, cochez les cases pour les événements au sujet desquels vous souhaitez être averti, et les moyens d'envoi des notifications pour eux.

CONFIGURATION DE L'ENVOI DES NOTIFICATIONS PAR COURRIER ÉLECTRONIQUE

Après avoir sélectionné les événements (cf. section "Sélection du type d'événement et de mode d'envoi des notifications" à la page [85](#)) au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications.

➔ Pour configurer les paramètres d'envoi des notifications par courrier électronique, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Apparence**, cochez la case **Activer les notifications sur les événements** et cliquez sur **Configuration**.

4. Dans la fenêtre **Configuration des notifications** qui s'ouvre, cochez les cases pour les événements nécessaires, dans la colonne **Email** et cliquez sur le bouton **Configuration d'email**.
5. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre, saisissez les valeurs nécessaires des paramètres. Pour être averti des événements après un certain temps, programmez la diffusion des messages d'informations en cliquant sur le bouton **Modifier**. Saisissez vos modifications dans la fenêtre **Programmation** qui ouvre.

CONFIGURATION DES PARAMETRES DU JOURNAL DES EVENEMENTS

Kaspersky Anti-Virus a la possibilité d'enregistrer des informations sur les événements apparus pendant l'exécution du programme, soit dans le journal générique de Microsoft Windows (**Application**) soit dans un journal spécialisé de Kaspersky Anti-Virus (**Kaspersky Event Log**).

La consultation du journal s'opère dans la fenêtre standard **Observateur d'événements** de Microsoft Windows que vous pouvez ouvrir à l'aide de la commande **Démarrer/Paramètres/Panneau de configuration/Administration/Observateur d'événements**.

➔ *Pour configurer les paramètres du journal des événements, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Dans le bloc **Apparence**, cochez la case **Activer les notifications sur les événements** et cliquez sur **Configuration**.
4. Dans la fenêtre **Configuration des notifications** qui s'ouvre, cochez les cases pour les événements nécessaires, dans la colonne **Journal** et cliquez sur le bouton **Configuration du journal**.
5. Dans la fenêtre **Paramètres du journal des événements** qui s'ouvre, sélectionnez le journal, dans lequel l'information sur les événements sera enregistrée.

ELEMENTS ACTIFS DE L'INTERFACE

Les possibilités suivantes de Kaspersky Anti-Virus s'entendent par les éléments actifs de l'interface :

Animer l'icône dans la zone de notification de la barre des tâches.

L'icône de l'application dans la barre des tâches varie en fonction de l'opération exécutée. Par exemple, lors de l'analyse du courrier, une image représentant une lettre apparaît sur le fond de l'icône. L'icône est animée par défaut. Dans ce cas, l'icône indiquera uniquement l'état de la protection de l'ordinateur : lorsque la protection est activée, l'icône est en couleur, lorsque la protection est suspendue ou désactivée, l'icône est grisée.

Afficher "Protected by Kaspersky Lab" sur l'écran de bienvenue de Microsoft Windows.

Par défaut, cet indicateur apparaît dans le coin supérieur droit de l'écran au démarrage de Kaspersky Anti-Virus. Il indique que votre ordinateur est protégé contre tout type de menace.

➔ *Pour configurer les éléments actifs de l'interface, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Paramètres**.
3. Cochez les cases requises dans le groupe **Apparence**.

RAPPORTS ET STOCKAGES

Cette rubrique reprend les paramètres qui régissent l'utilisation des fichiers de données de l'application.

Les fichiers de données du programme - sont les objets placés en quarantaine ou dans le dossier de sauvegarde pendant l'utilisation de Kaspersky Anti-Virus ainsi que les rapports des différents composants de l'application.

Dans cette section, vous pouvez :

- configurer les paramètres de création et de conservation des rapports ;
- configurer les paramètres de la quarantaine et du dossier de sauvegarde ;
- purger les rapports sauvegardés ainsi que le contenu du dossier de quarantaine et du dossier de sauvegarde.

➤ *Pour purger le contenu de ces dossiers, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Rapports et Stockages**.
3. Dans la fenêtre qui s'affiche, cliquez sur **Purger**.
4. Dans la fenêtre **Fichiers de données** qui s'ouvre, cochez les objets dont les sauvegardes doivent être supprimées.

VOIR ÉGALEMENT

Principes d'utilisation des rapports	87
Quarantaine pour les objets potentiellement infectés	88
Manipulation des objets en quarantaine	89
Copie de sauvegarde des objets dangereux	89
Manipulation des copies de sauvegarde	90

PRINCIPES D'UTILISATION DES RAPPORTS

Le fonctionnement l'Antivirus Fichiers et l'exécution de chaque tâche d'analyse et de la mise à jour est consignée dans un rapport.

➤ *Pour consulter les rapports, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur **Journaux**.

➤ *Pour voir tous les événements consignés dans le rapport et relatifs au fonctionnement du composant ou à l'exécution d'une tâche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Journaux**.
2. Dans la fenêtre ouverte, sous l'onglet **Rapports** sélectionnez le nom du composant ou de la tâche et cliquez sur le bouton **Détails**. Cette action entraîne l'ouverture d'une fenêtre contenant des informations détaillées sur le fonctionnement l'Antivirus Fichiers de la tâche sélectionné. Les statistiques sont reprises dans la partie

supérieure de la fenêtre tandis que les détails apparaissent sur divers onglets de la partie centrale. En fonction du rapport sélectionné (pour l'Antivirus Fichiers ou pour la tâche), la composition des onglets peut varier.

➔ *Pour importer le rapport dans le fichier texte, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Journaux**.
2. Dans la fenêtre ouverte, sous l'onglet **Journaux** sélectionnez le nom du composant ou de la tâche et cliquez sur le bouton **Détails**.
3. La fenêtre ouverte contient les informations détaillées sur le fonctionnement du composant ou de la tâche sélectionné. Cliquez sur **Enregistrer sous** et indiquez où vous souhaitez enregistrer le fichier.

CONFIGURATION DES PARAMETRES DU RAPPORT

Vous pouvez définir les paramètres suivants de constitution et de conservation des rapports :

- Consigner ou non les événements à caractère informatif. En règle générale, ces événements ne jouent pas un rôle crucial dans la protection (la case **Consigner les événements non critiques**).
- Activer la conservation dans le rapport uniquement des événements survenus depuis le dernier lancement de la tâche. Cela permet de gagner de l'espace sur le disque en diminuant la taille du rapport (la case **Conserver uniquement les événements courants**). Si la case est cochée, les informations reprises dans le rapport seront actualisées à chaque redémarrage de la tâche. Cependant, seules les informations non critiques seront écrasées.
- Définissez le délai de conservation des rapports (la case **Supprimer les rapports après**). Par défaut, ce délai est établi à 30 jours. Les rapports sont supprimés à l'issue des 30 jours. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.
- Définir la taille maximale du rapport (la case **Taille maximale**). Par défaut, la taille maximale est limitée à 250 Mo. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

➔ *Afin de configurer les paramètres de constitution et de conservation des rapports, procédez comme suit :*

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Rapports et Stockages**.
3. Dans le bloc **Rapports** cochez les cases nécessaires et, si nécessaire, établissez le délai de conservation des rapports et indiquez la taille maximale du rapport.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La **quarantaine** est un dossier spécial dans lequel on retrouve les objets qui ont peut être été infectés par des virus.

Les **objets potentiellement infectés** sont des objets qui ont peut-être été infectés par des virus ou leur modification.

Pourquoi parle-t-on d'objets *potentiellement infectés*? Il n'est pas toujours possible de définir si un objet est infecté ou non. Il peut s'agir des raisons suivantes :

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

Les bases de l'application contiennent les menaces qui ont été étudiées par les experts de Kaspersky Lab. Si le programme malveillant a été modifié et que ces modifications ne figurent pas encore dans les bases, Kaspersky Anti-Virus considère l'objet comme étant infecté par une modification d'un programme malveillant et le classe comme objet potentiellement infecté. Il indique obligatoirement à quelle menace cette infection ressemble.

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

Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Anti-Virus la classe comme un objet potentiellement infecté.

L'analyseur heuristique de code détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

L'objet potentiellement infecté peut-être identifié et mis en quarantaine pendant l'analyse antivirus ou par l'Antivirus Fichiers.

Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

VOIR EGALEMENT

Manipulation des objets en quarantaine[89](#)

MANIPULATION DES OBJETS EN QUARANTAINE

Vous pouvez réaliser les opérations suivantes sur les objets en quarantaine :

- mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- analyser et réparer à l'aide de la version actuelle des bases de l'application tous les objets potentiellement infectés qui se trouvent en quarantaine ;
- restaurer les fichiers dans un répertoire choisi par l'utilisateur ou dans le répertoire d'origine où ils se trouvaient avant d'être mis en quarantaine ;
- supprimer n'importe quel objet ou groupe d'objets de la quarantaine.

➔ *Pour réaliser une action quelconque sur les objets en quarantaine, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Défectés**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Quarantaine**, exécutez les actions requises.

COPIE DE SAUVEGARDE DES OBJETS DANGEREUX

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

La copie de sauvegarde est une copie de l'objet dangereux original qui est créée lors de la première réparation ou suppression de l'objet en question et qui est conservée dans le dossier de sauvegarde.

Le dossier de sauvegarde est un dossier spécial qui contient les copies des objets dangereux traités ou supprimés. La fonction principale du dossier de sauvegarde est de permettre à n'importe quel moment la restauration de l'objet original. Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger.

VOIR EGALEMENT

Manipulation des copies de sauvegarde[90](#)

MANIPULATION DES COPIES DE SAUVEGARDE

Vous pouvez réaliser les actions suivantes sur les objets de la sauvegarde :

- restaurer les copies sélectionnées ;
- supprimer les objets.

➔ Pour réaliser une action quelconque sur les objets de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le bouton **Menaces détectées**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Dossier de sauvegarde**, exécutez les actions requises.

CONFIGURATION DE LA QUARANTAINE ET DU DOSSIER DE SAUVEGARDE

Vous pouvez configurer les paramètres suivants de fonctionnement de la quarantaine et de la sauvegarde :

- Définir le mode d'analyse automatique des objets en quarantaine après chaque mise à jour des bases de l'application (la case **Analyser les fichiers en quarantaine après mise à jour**).

Kaspersky Anti-Virus ne peut analyser les objets en quarantaine directement après la mise à jour des bases de l'application si vous utilisez la quarantaine à ce moment.

- Définir la durée de conservation maximum des objets en quarantaine et des copies des objets dans le dossier de sauvegarde (la case **Supprimer les objets après**). Par défaut, la durée de conservation des objets est 90 jours, après lesquels ils seront supprimés. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.
- Indiquer la taille maximale de la quarantaine (case **Taille maximale**). Par défaut, la taille maximale est limitée à 1000 Mo. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

➔ Pour configurer les paramètres de la quarantaine ou de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Rapports et Stockages**.
3. Dans le groupe **Quarantaine et sauvegarde**, cochez les cases requises et, le cas échéant, définissez la taille limite du dossier où seront conservées les données.

DISQUE DE DEPANNAGE

Kaspersky Anti-Virus propose la création d'un disque de dépannage.

Le disque de dépannage est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il est utilisé lors de tel degré d'infection, quand il n'est pas possible de réparer l'ordinateur par les applications antivirus ou par les utilitaires de réparation (par exemple, Kaspersky AVPTool), lancés sous le système d'exploitation. Avec cela, l'efficacité de réparation est augmentée grâce au fait que les programmes malveillants dans le système ne reçoivent pas d'administration pendant le démarrage du système d'exploitation.

Le disque de dépannage est créé à la base du noyau du système d'exploitation Linux et représente le fichier .iso qui inclut :

- les fichiers de système et de configuration Linux ;
- un ensemble d'utilitaires pour le diagnostic du système d'exploitation ;
- l'ensemble d'utilitaires auxiliaires (le gestionnaire de fichiers, etc.) ;
- les fichiers Kaspersky Rescue Disk ;
- les fichiers contenant les bases de l'application.

Le démarrage de l'ordinateur avec le système d'exploitation endommagé peut être effectué de deux manières :

- *localement*, du périphérique CD/DVD-ROM. Pour cela le périphérique correspondant doit être installé sur l'ordinateur.
- *à distance*, du poste administrateur ou d'un autre ordinateur du réseau.

L'installation à distance est possible seulement dans le cas, si l'ordinateur soutient la technologie Intel® vPro™ ou Intel® Active Management.

➔ Afin de créer le disque de dépannage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur **Disque de dépannage** afin de lancer l'assistant de création de disque (cf. page [91](#)).
3. Suivez les consignes de l'Assistant.
4. A l'aide du fichier obtenu à la fin de l'Assistant, créez un CD/DVD de dépannage. Vous pouvez utiliser pour ce faire un des programmes d'enregistrement de CD/DVD tel que Nero par exemple.

VOIR ÉGALEMENT

Création d'un disque de dépannage	91
Démarrage de l'ordinateur à l'aide du disque de dépannage	93

CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier .iso) à partir des bases actuelles de l'application ainsi que des fichiers de configuration.

L'image du disque de départ, en fonction de laquelle le nouveau fichier est généré, peut être téléchargée du serveur de Kaspersky Lab, ou copiée depuis une source locale.

Le fichier de l'image, généré par l'Assistant, est sauvegardé dans le dossier "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk1*" ("*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk1*" : pour Microsoft Vista) avec le nom *rescuecd.iso*. Si l'Assistant a découvert le fichier de l'image, créé précédemment, dans le dossier, alors, en cochant la case **Utiliser l'image existante**, vous pouvez l'utiliser en guise de l'image du disque de départ, et passez tout d'un coup à l'étape 3 : mise à jour de l'image (cf. page [92](#)). Si l'Assistant n'a pas découvert le fichier de l'image, alors cette case n'existe pas.

La création du disque de dépannage s'opère à l'aide d'un assistant spécial qui contient une succession de fenêtres (étape) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Pour terminer le travail de l'assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

VOICI, EN DETAILS, LES ETAPES DE L'ASSISTANT :

Etape 1. Sélection de la source de l'image du disque	92
Etape 2. Copie (téléchargement) de l'image du disque	92
Etape 3. Mise à jour de l'image du disque	92
Etape 4. Chargement de l'ordinateur distant	93
Etape 5. Fin de l'Assistant	93

ETAPE 1. SELECTION DE LA SOURCE DE L'IMAGE DU DISQUE

Si dans la fenêtre précédente de l'Assistant vous avez coché la case **Utiliser l'image existante**, alors cette étape n'est pas présentée.

Cette étape vous oblige à sélectionner une source du fichier de l'image parmi les options proposées :

- Sélectionnez l'option **Copier l'image du CD/DVD ou du réseau local**, si vous possédez déjà un CD/DVD contenant l'image du disque de dépannage ou si cette image a déjà été préparée et qu'elle se trouve sur l'ordinateur ou sur une ressource du réseau local.
- Sélectionner l'option **Télécharger l'image du serveur de Kaspersky Lab**, si vous n'avez une copie du fichier d'image, vous pouvez le télécharger depuis le serveur de Kaspersky Lab (le fichier pèse environ 100 Mo).

ETAPE 2. COPIE (TELECHARGEMENT) DE L'IMAGE DU DISQUE

Si à l'étape précédente vous avez sélectionné l'option de copie de l'image de la source locale (**Copier l'image du CD/DVD ou du réseau local**), alors à cette étape il vous faut indiquer le chemin d'accès à lui. Pour ce faire, cliquez sur **Parcourir**. La fenêtre suivante illustrera la progression de la copie du fichier.

Si vous aviez choisi l'option **Télécharger l'image du serveur de Kaspersky Lab**, alors la progression du téléchargement s'affichera à la fois.

ETAPE 3. MISE A JOUR DE L'IMAGE DU DISQUE

La procédure d'actualisation du fichier d'image prévoit :

- la mise à jour des bases de l'application ;
- la mise à jour des fichiers de configuration.


Les fichiers de configuration définissent le moyen d'application du disque de dépannage : sur l'ordinateur local ou distant, c'est pourquoi il vous faut sélectionner l'option nécessaire parmi les options proposées avant la mise à jour du fichier de l'image :

- **Chargement de l'ordinateur distant**, si vous prévoyez le chargement de l'ordinateur distant.

N'oubliez qu'en cas de chargement de l'ordinateur distant, celui-ci doit être compatible avec la technologie Intel® vPro™ ou Intel® Active Management.

Si l'accès à l'Internet s'effectue de l'ordinateur distant via le serveur proxy, alors la mise à jour sera inaccessible


lors de l'utilisation du disque de dépannage. En ce cas, il est préalablement recommandé d'actualiser Kaspersky Anti-Virus.

-  **Chargement du système depuis un CD/DVD** si l'image du disque créée sera enregistré plus tard sur un CD ou un DVD.

Une fois que vous aurez fait votre choix, appuyez sur le bouton **Suivant**. La fenêtre suivante de l'Assistant illustrera la progression de la mise à jour.

Si l'option **Chargement de l'ordinateur distant** est sélectionnée, l'image créée ne pourra pas être enregistrée sur CD/DVD afin de charger le système. Pour charger le système depuis un CD/DVD, exécutez à nouveau l'assistant et, à cette étape, sélectionnez **Chargement du système du disque CD/DVD**.

ETAPE 4. CHARGEMENT DE L'ORDINATEUR DISTANT

Cette étape de l'Assistant apparaît uniquement dans le cas, si à l'étape précédente vous avez sélectionné l'option  **Chargement de l'ordinateur distant**.

Saisissez les données relatives à l'ordinateur :

- **Adresse IP ou nom de l'ordinateur** dans le réseau ;
- Données du compte utilisateur avec les privilèges d'administrateur : **Nom d'utilisateur** et **Mot de passe**.

La fenêtre suivante de l'Assistant propose la console iAMT permettant de gérer le processus de démarrage de l'ordinateur (cf. page [93](#)).

ETAPE 5. FIN DE L'ASSISTANT

Cette fenêtre de l'assistant vous informe de la réussite de la création du disque de dépannage.

DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Pour charger le système d'exploitation, il vous faut absolument un fichier d'image (.iso) de disque de dépannage. Vous pouvez charger (cf. page [92](#)) le fichier depuis le serveur de Kaspersky Lab ou actualiser (cf. page [92](#)) le fichier existant.

Examinons en détails le fonctionnement du disque de dépannage. Les opérations suivantes se déroulent durant le chargement du disque :

1. Identification automatique de la configuration matérielle de l'ordinateur.
2. Recherche de systèmes de fichiers sur les disques durs. Les systèmes de fichiers trouvés sont identifiés par un nom commençant par C.

Les noms attribués aux disques durs et aux disques amovibles peuvent ne pas correspondre à la dénomination dans le système d'exploitation.

Si le système d'exploitation d'ordinateur démarré est en mode de veille, ou son système de fichiers est en mode *unclean*, en conséquence de l'arrêt incorrect du fonctionnement, il vous sera proposé de prendre une décision sur l'assemblage du système de fichiers ou de redémarrer l'ordinateur.

L'assemblage du système de fichiers peut amener à sa panne.

3. Recherche d'un fichier de téléchargement Microsoft Windows *pagefile.sys*. Si ce fichier n'existe pas, la taille de la mémoire virtuelle est limitée par la taille de la mémoire vive.
4. Choix de la langue de la version. Si durant une certaine période de temps, aucune sélection n'a eu lieu, alors la langue anglaise est prise par défaut.

Lors du démarrage de l'ordinateur distant cette étape n'existe pas.

5. Recherche (création) des dossiers pour le placement des bases antivirus, des rapports, de la quarantaine et des fichiers auxiliaires. Les répertoires de l'application de Kaspersky Lab installée sur l'ordinateur infectés sont utilisés par défaut (*ProgramData/Kaspersky Lab/AVP8* – pour Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – pour les versions antérieures de Microsoft Windows). Si les répertoires de l'application sont introuvables, une tentative de création sera réalisée. Si les dossiers n'ont pas été découverts et il n'a pas été possible de les créer, le dossier *kl.files* se crée sur un des disques.
6. La tentative de configurer les connexions de réseau en fonction des données, découvertes dans les fichiers de système de l'ordinateur démarré.
7. Le téléchargement du sous-système graphique et le lancement de Kaspersky Rescue Disk (dans le cas du démarrage de l'ordinateur du CD/DVD).

Dans le cas du démarrage de l'ordinateur distant, la ligne de commande s'affiche dans la console iAMT. Les commandes pour l'utilisation de Kaspersky Anti-Virus au départ de la ligne de commande (cf. page 95) ont été utilisées pour administrer les tâches.


En mode de restauration, seules la recherche de virus et la mise à jour des bases depuis une source locale sont accessibles, aussi que l'annulation des mises à jour et la consultation des statistiques.

► Pour charger le système d'exploitation d'un ordinateur infecté depuis un CD/DVD, procédez comme suit :

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).
2. Introduisez le disque contenant l'image du disque de dépannage dans le lecteur d'un ordinateur infecté.
3. Redémarrez l'ordinateur.
4. Le chargement est alors exécuté conformément à l'algorithme décrit ci-dessus.

► Pour lancer le système d'exploitation d'un ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur afin de lancer l'assistant de création de disque (cf. page 91). Suivez les consignes de l'Assistant.

N'oubliez pas, qu'à l'étape de la mise à jour (cf. page 92) de l'image du disque, il faut sélectionner l'option  **Chargement de l'ordinateur distant**.

Le chargement est alors exécuté conformément à l'algorithme décrit ci-dessus.

UTILISATION DE KASPERSKY RESCUE DISK AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Rescue Disk à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- analyse des objets sélectionnés ;
- mise à jour des signatures des menaces et des modules de l'application ;
- annulation de la dernière mise à jour ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;

Syntaxe de la ligne de commande :

<commande> [paramètres]

Où instruction peut être remplacé par:

HELP	aide sur la syntaxe de la commande ou la liste des commandes.
SCAN	analyse antivirus des objets
UPDATE	lancement de la tâche de mise à jour
ROLLBACK	annulation de la dernière mise à jour réalisée
EXIT	arrêt de Kaspersky Rescue Disk

DANS CETTE SECTION

Recherche de virus.....	96
Mise à jour de Kaspersky Anti-Virus.....	97
Annulation de la dernière mise à jour	97
Consultation de l'aide	98

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>] [<paramètres du rapport>]
```

Description des paramètres.

<p><objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant.</p> <p>Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.</p>	
<files>	<p>Liste des chemins d'accès aux fichiers et / ou aux répertoires à analyser.</p> <p>La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace.</p> <p>Remarques :</p> <ul style="list-style-type: none"> • Mettre le nom de l'objet entre guillemets s'il contient un espace; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/discs/	Analyse de tous les disques.
/discs/<disc_name>:/<folder>	Analyse du disque spécifié, ou <disc_name> – nom du disque et <folder> – chemin vers le répertoire analysé.
<p><action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur -i8.</p>	
-i0	Aucune action n'est exécutée, seules les informations sont consignées dans le rapport.
-i1	Réparer les objets infectés, si la réparation est impossible, les ignorer.
-i2	Réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx).
-i3	Réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
-i4	Supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
-i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
-i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.
<p>Le paramètre <types de fichiers> définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.</p>	
-fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
-fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.

-fa	Analyser tous les fichiers.
Le paramètre <exclusions> définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque.
-e:<secondes>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <secondes> .
-es:<taille>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre <size> .

Exemples :

- Lancer l'analyse du répertoire Documents and Settings et du disque <D> :

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

MISE A JOUR DE KASPERSKY ANTI-VIRUS

L'instruction pour la mise à jour des modules de Kaspersky Anti-Virus et des bases de l'application possède la syntaxe suivante :

```
UPDATE [<source_des_mises_à_jour>] [-R[A]:<fichier_de_rapport>]
```

Description des paramètres.

<source_de_la_mise_à_jour>	Serveur HTTP, serveur FTP pour répertoire de réseau pour le chargement de la mise à jour. Ce paramètre peut prendre comme valeur le chemin d'accès complet à la source de la mise à jour ou l'URL. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de Kaspersky Anti-Virus.
-R[A]:<fichier_de_rapport>	<p>-R:<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants.</p> <p>-RA:<fichier_de_rapport> : consigner tous les événements dans le rapport.</p> <p>Les chemins absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.</p>

Exemples :

- Actualiser les bases et consigner tous les éléments dans le rapport :

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

ROLLBACK [-R[A]:<fichier_de_rapport>]

Description des paramètres.

<p>-R[A]:<fichier_de_rapport></p>	<p>-R:<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants.</p> <p>-RA:<fichier_de_rapport> : consigner tous les événements dans le rapport.</p> <p>Les chemins absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.</p>
--	---

Exemple :

ROLLBACK -RA:/discs/C:/rollback.txt

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

[-? | HELP]

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

<commande> -?

HELP <commande>


VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY ANTI-VIRUS

Une fois que vous aurez installé et configuré Kaspersky Anti-Virus, vous pourrez vérifier si la configuration des paramètres est optimale à l'aide du virus d'essai et de ses modifications. La vérification doit être réalisée séparément pour chaque composant de la protection / protocole.

DANS CETTE SECTION

Virus d'essai "EICAR" et ses modifications	99
Vérification de l'exactitude de la configuration d'Antivirus Fichiers	100
Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus	101

VIRUS D'ESSAI "EICAR" ET SES MODIFICATIONS

Ce "virus" d'essai a été développé spécialement par l'organisation  (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le virus d'essai N'EST PAS UN VIRUS et il ne contient pas de code qui pourrait nuire à votre ordinateur. Toutefois, la majorité des logiciels antivirus le considère comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus !

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

Avant de lancer le téléchargement, il faut absolument désactiver la protection antivirus car le fichier *anti_virus_test_file.htm* sera identifié et traité par l'application comme un objet infecté transmis par le protocole HTTP. N'oubliez pas de réactiver la protection antivirus dès que le téléchargement du virus d'essai sera terminé.

L'application identifie le fichier téléchargé depuis le site de la société **EICAR** comme un objet infecté par un virus **qui ne peut être neutralisé** et exécute l'action définie pour ce genre d'objet.

Vous pouvez également utiliser une modification du virus d'essai standard afin de vérifier le bon fonctionnement de l'application. Pour ce faire, il faut modifier le contenu du virus standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le **Bloc-Notes de Microsoft** ou **UltraEdit32**, etc.

Vous pouvez vérifier le bon fonctionnement de votre logiciel antivirus à l'aide d'une modification du virus EICAR uniquement si vous possédez des bases antivirus dont la date de publication est postérieure au 24 octobre 2003 (mise à jour cumulée, octobre 2003).

La première colonne du tableau contient les préfixes qu'il faut ajouter en tête de la ligne du virus d'essai traditionnel. La deuxième colonne reprend toute les valeurs possibles de l'état attribué par l'antivirus à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de l'application.

Après avoir ajouté le préfixe au virus d'essai, enregistrez le fichier, par exemple sous le nom : *eicar_dele.com*. Nommez tous les virus modifiés selon le même principe.

Tableau 1. Modifications du virus d'essai

Préfixe	Etat de l'objet	Informations relatives au traitement de l'objet
Pas de préfixe, "virus" d'essai standard.	Infecté. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée.
CORR-	Corrompu.	L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application.
WARN-	Suspect. L'objet contient le code d'un virus inconnu. Réparation impossible.	L'analyseur heuristique attribue l'état suspect à l'objet. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
SUSP-	Suspect. L'objet contient le code modifié d'un virus connu. Réparation impossible.	L'application a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
ERRO-	Erreur d'analyse.	Une erreur s'est produite lors de l'analyse de l'objet. L'application ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application.
CURE-	Infecté. L'objet contient le code d'un virus connu. Réparable.	L'objet contient un virus qui peut être réparé. L'application répare l'objet et le texte du corps du " virus " est remplacé par CURE. Vous serez averti de la découverte d'un tel objet.
DELE-	Infecté. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée. Vous serez averti de la découverte d'un tel objet.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION D'ANTIVIRUS FICHIERS

➡ Pour vérifier l'exactitude de la configuration de l'Antivirus Fichiers, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation EICAR (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.
2. Autorisez la consignation de tous les événements afin que le rapport reprenne les données sur les objets corrompus ou les objets qui n'ont pas été analysés suite à un échec.
3. Exécutez le fichier du virus d'essai ou une de ses modifications.

Antivirus Fichiers intercepte la requête adressée au fichier, la vérifie et exécute l'action définie dans les paramètres. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Les informations complètes sur les résultats du fonctionnement d'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE ANTIVIRUS

► Pour vérifier l'exactitude de la configuration de la tâche d'analyse, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.
2. Créez une nouvelle tâche d'analyse antivirus et en guise d'objet à analyser sélectionnez le dossier, contenant la sélection de virus d'essai.
3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec.
4. Lancez la tâche d'analyse antivirus.

Lors de l'analyse, les actions définies dans les paramètres de la tâche seront exécutées au fur et à mesure que des objets suspects ou infectés sont découverts. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Toutes les informations relatives aux résultats de l'exécution de la tâche d'analyse sont consultables dans le rapport de fonctionnement du composant.

TYPES DE MESSAGE

Lorsqu'un événement se produit pendant l'utilisation de Kaspersky Anti-Virus, vous verrez apparaître un message spécial. En fonction du niveau de gravité de l'événement (du point de vue de la sécurité de l'ordinateur), le message peut appartenir à l'une des catégories suivantes :

- **Alertes.** Un événement critique s'est produit, par exemple un objet malveillant ou une activité dangereuse a été découvert dans le système. Il faut immédiatement décider de la suite des événements. Ce type de message est de couleur rouge.
- **Attention.** Un événement qui présente un risque potentiel s'est produit, par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système. Il faut prendre une décision en fonction du danger que représente la menace à vos yeux. Ce type de message est de couleur jaune.
- **Informations.** Ce message vous signale un événement qui n'est pas critique. Les messages à caractère informatif ont une couleur bleue.

DANS CETTE SECTION

Un objet suspect a été détecté	102
La réparation de l'objet est impossible	103
Un objet suspect a été détecté	103

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers ou une tâche d'analyse découvre un objet malveillant, un message spécial apparaît.

Celui-ci contient :

- Le type de menace (par exemple : *virus, cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Réparer** : tentative de réparation de l'objet malveillant. Une copie de sauvegarde est créée avant la suppression au cas où il faudrait restaurer l'objet ou le scénario de l'infection.
- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Afin d'appliquer l'action sélectionnée à tous les objets possédant un statut identique et découverts au cours de cette session du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas similaires**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou

jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusque sa fin.

LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet malveillant. Par exemple, si l'objet est corrompu à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer. De plus il existe certains types d'objets malicieux comme les chevaux de Troie qui ne peuvent pas être réparés.

Dans ce cas, un message spécial contenant les informations suivantes s'affiche :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusque sa fin.

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers ou la recherche d'éventuels virus découvre un objet qui contient le code d'un virus inconnu ou le code modifié d'un virus connu, un message spécial s'affiche.

Celui-ci contient :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : place l'objet en quarantaine. Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme un objet infecté et réparé à l'aide des bases actualisées. Ou l'objet n'est pas *infecté* et il peut être restauré.

- **Supprimer** : supprime l'objet. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Afin d'appliquer l'action sélectionnée à tous les objets possédant un statut identique et découverts au cours de cette session du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas similaires**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusque sa fin.

Si vous êtes certain que l'objet découvert ne présente aucun danger, ajoutez-le à la zone de confiance pour éviter de devoir à nouveau le traiter lors des analyses ultérieures.

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Anti-Virus à l'aide de la ligne de commande.

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation de Kaspersky Anti-Virus ou en indiquant le chemin d'accès complet à avp.com.

En tant que <commande> vous pouvez utiliser :

- **HELP** – aide sur la syntaxe de la commande ou la liste des commandes.
- **SCAN** – analyse des objets sur la présence de virus.
- **UPDATE** – lance la mise à jour de l'application.
- **ROLLBACK** – annulation de la dernière mise à jour réalisée (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus).
- **START** – lancement du composant ou de la tâche.
- **STOP** – arrêt du composant ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus).
- **STATUS** – affichage de l'état actuel du composant ou de la tâche.
- **STATISTICS** – affichage des statistiques du composant ou de la tâche.
- **EXPORT** – exporte les paramètres de la protection de l'application.
- **IMPORT** – importation des paramètres de protection de Kaspersky Anti-Virus (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application).
- **ACTIVATE** – activation de Kaspersky Anti-Virus via Internet à l'aide du code d'activation.
- **ADDKEY** – activation du programme à l'aide du fichier de la clé de licence (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application).
- **RESTORE** – restauration du fichier de la quarantaine.
- **EXIT** – quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mot de passe défini via l'interface de l'application).
- **TRACE** – obtention du fichier de trace.

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

DANS CETTE SECTION

Consultation de l'aide	106
Recherche de virus.....	106
Mise à jour de l'application	108
Annulation de la dernière mise à jour	109
Lancement / arrêt d'Antivirus Fichiers ou d'une tâche	109
Statistiques du fonctionnement du composant ou de la tâche.....	110
Exportation des paramètres de protection.....	111
Importation des paramètres de protection	111
Activation de l'application	111
Restauration du fichier de la quarantaine	112
Arrêt de l'application	112
Obtention du fichier de trace	112
Codes de retour de la ligne de commande.....	113

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
avp.com [ /? | HELP ]
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
avp.com <commande> /?
```

```
avp.com HELP <commande>
```

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<paramètres du rapport>] [< paramètres complémentaires >]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Anti-Virus.

Description des paramètres.

<objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace :

- **<files>** – liste des chemins d'accès aux fichiers et / ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques :
 - mettre le nom de l'objet entre guillemets s'il contient un espace ;
 - lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
- **/ALL** – analyse complète de l'ordinateur.
- **/MEMORY** – objets de la mémoire vive.
- **/STARTUP** – objets de démarrage.
- **/MAIL** – bases de données de messagerie.
- **/REMDRIVES** – tous les disques amovibles.
- **/FIXDRIVES** – tous les disques locaux.
- **/NETDRIVES** – tous les disques de réseau.
- **/QUARANTINE** – objets en quarantaine.
- **/@:<filelist.lst>** – chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi avec guillemets, s'il contient un espace.

<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i2**. Les valeurs suivantes sont possibles :

- **/i0** – aucune action n'est exécutée, seules les informations sont consignées dans le rapport.
- **/i1** – réparer les objets infectés, si la réparation est impossible, les ignorer.
- **/i2** – réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx). Cette action est utilisée par défaut.
- **/i3** – réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
- **/i4** – supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
- **/i8** – confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
- **/i9** – confirmer l'action auprès de l'utilisateur à la fin de l'analyse.

Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu. Les valeurs suivantes sont possibles :

- **/fe** – analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
- **/fi** – analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
- **/fa** – analyser tous les fichiers.

Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.

- **/e:a** – ne pas analyser les archives
- **/e:b** – ne pas analyser les bases de messagerie.
- **/e:m** – ne pas analyser les messages électroniques au format plain text.
- **/e:<mask>** – ne pas analyser les objets en fonction d'un masque.
- **/e:<seconds>** – ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<seconds>**.

Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

- **/R:<report_file>** – consigner uniquement les événements importants dans le fichier indiqué.
- **/RA:<report_file>** – consigner tous les événements dans le rapport.

<paramètres complémentaires> – paramètres qui définissent l'utilisation de technologies de recherche de virus et l'utilisation du fichier de configuration des paramètres :

- **/iChecker=<on|off>** – activer / désactiver l'utilisation de la technologie iChecker.
- **/iSwift=<on|off>** – activer / désactiver l'utilisation de la technologie iSwift.
- **/C:<nom_du_fichier_de_configuration>** – le paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.

Exemples :

- *Exécuter l'analyse de la mémoire vive, des objets de démarrage automatique, des bases de données de messagerie électronique et des répertoires My Documents, Program Files dans le test.exe :*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_setting.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

MISE A JOUR DE L'APPLICATION

La commande de mise à jour des modules de Kaspersky Anti-Virus et des bases de l'application possède la syntaxe suivante:

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/APP=<on|off>] [<paramètres_de_rapport>]
[<paramètres_complémentaires>]
```

Description des paramètres.

<source_de_la_mise_à_jour> – serveur HTTP, serveur FTP ou répertoire de réseau pour le chargement de la mise à jour. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.

/APP=<on|off> – active / désactive la mise à jour des modules de l'application.

Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

- **/R:<report_file>** – consigner uniquement les événements importants dans le fichier indiqué.
- **/RA:<report_file>** – consigner tous les événements dans le rapport.

<paramètres complémentaires> – paramètre qui définit l'utilisation du fichier de configuration des paramètres.

/C:<nom_du_fichier_de_configuration> – le paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.

Exemples :

➤ *Actualiser les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➤ *Mettre à jour les modules de Kaspersky Anti-Virus en utilisant les paramètres du fichier de configuration updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
avp.com ROLLBACK </password=<mot_de_passe>> [<paramètres_de_rapport>]
```

Description des paramètres.

</password=<mot_de_passe>> – mot de passe défini via l'interface de l'application. La commande ROLLBACK ne peut être exécutée sans la saisie préalable du mot de passe.

<paramètres du rapport> – le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

- **/R:<report_file>** – consigner uniquement les événements importants dans le fichier indiqué.
- **/RA:<report_file>** – consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

Exemple

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

LANCEMENT / ARRET D'ANTIVIRUS FICHIERS OU D'UNE TACHE

Syntaxe de la commande START :

```
avp.com START <profil|nom_de_la_tâche> [<paramètres_de_rapport>]
```

Syntaxe de la commande STOP :

```
avp.com STOP <profil|nom_de_la_tâche> </password=<mot de passe>>
```

Description des paramètres.

</password=<mot_de_passe>> – mot de passe défini via l'interface de l'application. La commande STOP ne peut être exécutée sans la saisie préalable du mot de passe.

<paramètres du rapport> – le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

- **/R:<report_file>** – consigner uniquement les événements importants dans le fichier indiqué.
- **/RA:<report_file>** – consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

<profil|nom_de_la_tâche> – attribuez une des valeurs suivantes :

- **Protection (RTP)** – tous les composants de la protection ;
- **File_Monitoring (FM)** – Antivirus Fichiers ;
- **Scan_My_Computer** – la tâche d'analyse complète de l'ordinateur ;
- **Scan_Objects** – analyse des objets ;
- **Scan_Quarantine** – analyse de la quarantaine ;
- **Scan_Startup (STARTUP)** – analyse des objets de démarrage ;
- **Updater** – tâche de mise à jour ;
- **Rollback** – tâche d'annulation d'une mise à jour.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples :

➤ *Pour activer l'Antivirus Fichiers, saisissez dans la ligne de commande :*

```
avp.com START FM
```

➤ *Pour arrêter la tâche d'analyse complète, saisissez dans la ligne de commande :*

```
avp.com STOP SCAN_MY_COMPUTER /password=<votre_mot_de_passe>
```

STATISTIQUES DU FONCTIONNEMENT DU COMPOSANT OU DE LA TÂCHE

Syntaxe de la commande STATUS :

```
avp.com STATUS <profil|nom_de_la_tâche>
```

Syntaxe de la commande STATISTICS :

```
avp.com STATISTICS <profil|nom_de_la_tâche>
```

Description des paramètres.

<profil|nom_de_la_tâche> – une des valeurs citées dans la commande START / STOP (cf. page [109](#)) s'indique.

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com EXPORT <profil|nom_de_la_tâche> <nom_du_fichier>
```

Description des paramètres.

<profil|nom_de_la_tâche> – une des valeurs citées dans la commande START / STOP (cf. page [109](#)) s'indique.

<nom_du_fichier> – chemin d'accès au fichier vers lequel sont exportés les paramètres de l'application. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple

```
avp.com EXPORT RTP RTP_settings.dat - format binaire
avp.com EXPORT FM FM_settings.txt - format texte
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com IMPORT <nom_du_fichier> </password=<votre_mot_de_passe>>
```

Description des paramètres.

<nom_du_fichier> – chemin d'accès au fichier duquel sont importés les paramètres de l'application. Vous pouvez indiquer un chemin relatif ou absolu.

</password=<votre_mot_de_passe>> – mot de passe défini via l'interface de l'application.

Exemple

```
avp.com IMPORT settings.dat
```

ACTIVATION DE L'APPLICATION

L'activation de Kaspersky Anti-Virus peut se dérouler de deux manières :

- Via Internet à l'aide du code d'activation (commande ACTIVATE) ;
- Via le fichier de clé de licence (commande ADDKEY).

Syntaxe de la commande :

```
avp.com ACTIVATE <code_d'activation> </password=<mot_de_passe>>
avp.com ADDKEY <nom_du_fichier > </password=<mot_de_passe>>
```

Description des paramètres.

<code d'activation> – code d'activation : xxxxx-xxxxx-xxxxx-xxxxx.

<nom_du_fichier> – nom de la clé du fichier de licence avec l'extension .key : xxxxxxxx.key.

</password=<mot de passe>> – mot de passe défini via l'interface de l'application.

Exemple

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<mot de passe>>
```

RESTAURATION DU FICHIER DE LA QUARANTAINE

Syntaxe de la commande :

```
avp.com RESTORE [/REPLACE] <nom_du_fichier>
```

Description des paramètres.

/REPLACE – remplacement du fichier existant.

<nom_du_fichier> – nom du fichier à restaurer.

Exemple

```
avp.com REPLACE C:\eicar.com
```

ARRÊT DE L'APPLICATION

Syntaxe de la commande :

```
avp.com EXIT </password=<mot_de_passe>>
```

Description des paramètres.

</password=<mot_de_passe>> – mot de passe défini via l'interface de l'application. La commande ne peut être exécutée sans la saisie préalable du mot de passe.

OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de Kaspersky Anti-Virus. Il permettra aux spécialistes du service d'assistance technique de poser un diagnostic plus précis.

Syntaxe de la commande :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

Description des paramètres.

[on|off] – active / désactive la création d'un fichier de trace.

[file] – recevoir la trace dans un fichier.

<niveau_de_trace> – pour ce paramètre, il est possible de saisir un chiffre compris entre 100 (niveau minimum, uniquement les événements critiques) et 600 (niveau maximum, tous les messages).

Lorsque vous contactez le service d'assistance technique, l'expert doit vous préciser le niveau qu'il souhaite. Si ce niveau n'a pas été indiqué, il est conseillé d'utiliser la valeur 500.

Exemples :

➡ *Désactiver la constitution de fichiers de trace :*

```
avp.com TRACE file off
```


- *Créer un fichier de trace avec le niveau 500 :*

avp.com TRACE file on 500

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

Codes de retour généraux :

- 0 – opération réussie ;
- 1 – valeur de paramètre invalide ;
- 2 – erreur inconnue ;
- 3 – erreur d'exécution de la tâche ;
- 4 – annulation de l'exécution de la tâche.

Codes de retour des tâches d'analyse antivirus :

- 101 – tous les objets dangereux ont été traités ;
- 102 – des objets dangereux ont été découverts.

MODIFICATION, REPARATION OU SUPPRESSION DE L'APPLICATION

Vous pouvez supprimer l'application à l'aide d'un des moyens suivants :

- à l'aide de l'assistant d'installation de l'application ;
- au départ de la ligne de commande (cf. section "Procédure de suppression de l'application via la ligne de commande" à la page [116](#)) ;
- la suite logicielle Kaspersky Administration Kit (cf. "Guide de déploiement de Kaspersky Administration Kit") ;
- via les stratégies de domaine de groupe de Microsoft Windows Server 2000/2003 (cf. section "Suppression de l'application" à la page [23](#)).

DANS CETTE SECTION

Modification, réparation ou suppression du logiciel à l'aide d'assistant d'installation.....	114
Procédure de suppression de l'application via la ligne de commande.....	116

MODIFICATION, REPARATION OU SUPPRESSION DU LOGICIEL A L'AIDE D'ASSISTANT D'INSTALLATION

La réparation du logiciel est utile si vous êtes confrontés à certaines erreurs de fonctionnement suite à une mauvaise configuration ou à la corruption des fichiers de l'application.

► *Pour passer à la restauration de l'état d'origine du logiciel ou à l'installation de composants de Kaspersky Anti-Virus qui n'avaient pas été installés à l'origine ainsi que pour supprimer l'application :*

1. Introduisez le cédérom d'installation dans le lecteur de CD/DVD-ROM pour autant que vous ayez installé le logiciel à l'aide de ce cédérom. Si vous aviez procédé à l'installation au départ d'une autre source (dossier partagé, répertoire du disque dur, etc.), assurez que le fichier d'installation se trouve toujours dans cette source et que vous y avez accès.
2. Sélectionnez **Démarrez** → **Programmes** → **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** → **Modification, réparation ou suppression**.

Cette action entraîne le lancement du programme d'installation qui se présente sous la forme d'un Assistant. Examinons les étapes de la réparation ou de la modification de la composition du logiciel ou de sa suppression.

ETAPE 1. FENETRE D'ACCUEIL DU PROGRAMME D'INSTALLATION

Si vous avez réalisé toutes les tâches nécessaires à la réparation ou à la modification de la composition du programme, la fenêtre d'accueil du programme d'installation de Kaspersky Anti-Virus s'affichera. Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 2. SÉLECTION DE L'OPERATION

Vous devez définir à cette étape le type d'opération que vous souhaitez exécuter sur le logiciel: vous pouvez soit modifier la composition du logiciel, soit restaurer l'état d'origine des composants installés ou supprimer certains composants ou l'application complète. Pour exécuter l'action que vous voulez, il suffit de cliquer sur le bouton correspondant. La suite de l'Assistant dépend de l'action que vous avez choisie.

La modification de la composition de l'application est similaire à l'installation personnalisée qui vous permet de sélectionner les composants que vous voulez installer ou supprimer.

La réparation de l'application s'opère sur la base de la composition actuelle. Tous les fichiers des composants installés seront actualisés et pour chacun d'entre eux, c'est le niveau de protection **Recommandé** qui sera appliqué.

Lors d'une désinstallation à distance de Kaspersky Anti-Virus 6.0, le redémarrage automatique du serveur ne s'effectue pas. Toutefois, pour une suppression intégrale des composants de l'application et pour le fonctionnement suivant de l'ordinateur, il est recommandé de redémarrer l'ordinateur manuellement.

Lors de la suppression de l'application, vous devrez sélectionner les données créées et utilisées par le programme que vous souhaitez sauvegarder. Pour supprimer toutes les données de Kaspersky Anti-Virus, sélectionnez l'option **Supprimer complètement l'application**. Pour sauvegarder les données, vous devrez sélectionner l'option **Enregistrer les objets de l'application** et précisez quels objets exactement :

- *Informations relatives à l'activation* : fichier de licence indispensable au fonctionnement de l'application.
- *Bases de l'application* : toutes les signatures des programmes dangereux, des virus et des autres menaces qui datent de la dernière mise à jour.
- *Objets du dossier de sauvegarde* : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure.
- *Objets de la quarantaine* : objets qui sont peut-être modifiés par des virus ou leur modification. Ces objets contiennent un code semblable au code d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des signatures des menaces.
- *Paramètres de la protection* : valeurs des paramètres de fonctionnement de tous les composants du logiciel.
- *Données iSwift* : base contenant les informations relatives aux objets analysés dans le système de fichiers NTFS. Elle permet d'accélérer l'analyse des objets. Grâce à cette base, Kaspersky Anti-Virus analyse uniquement les objets qui ont été modifiés depuis la dernière analyse.

Si un laps de temps important s'écoule entre la suppression d'une version de Kaspersky Anti-Virus et l'installation d'une autre, il n'est pas conseillé d'utiliser la base iSwift de l'installation précédente. En effet, pendant cet intervalle, un programme dangereux peut s'infiltrer et ses actions pourraient ne pas être identifiées à l'aide de cette base, ce qui entraînerait l'infection de l'ordinateur.

Pour exécuter l'action sélectionnée, cliquez sur **Suivant**. La copie des fichiers nécessaires ou la suppression des composants et des données sélectionnés est lancée.

ETAPE 3. FIN DE LA REPARATION, DE LA MODIFICATION OU DE LA SUPPRESSION DU LOGICIEL

La progression de la réparation, de la modification ou de la suppression sera illustrée et vous serez averti dès que l'opération sera terminée.

En règle générale, la suppression requiert le redémarrage de l'ordinateur, indispensable pour tenir compte des modifications dans le système. La boîte de dialogue vous invitant à redémarrer l'ordinateur s'affichera. Cliquez sur **Oui** pour redémarrer immédiatement. Si vous souhaitez redémarrer l'ordinateur manuellement plus tard, cliquez sur **Non**.

PROCEDURE DE SUPPRESSION DE L'APPLICATION VIA LA LIGNE DE COMMANDE

- Pour supprimer Kaspersky Anti-Virus for Windows Servers MP4 au départ de la ligne de commande, saisissez :

```
msiexec /x <nom_du_paquet>
```

Cette action lancera l'Assistant d'installation qui vous permettra de supprimer l'application.

- Pour supprimer l'application en mode non interactif sans redémarrage de l'ordinateur (le redémarrage devra être réalisé manuellement après l'installation), saisissez :

```
msiexec /x <nom_du_paquet> /qn
```

- Pour supprimer l'application en mode non interactif avec redémarrage de l'ordinateur, saisissez :

```
msiexec /x <nom_du_paquet> ALLOWREBOOT=1 /qn
```

Si un mot de passe contre la suppression avait été défini lors de l'installation, il faudra absolument saisir ce mot de passe sans quoi la suppression ne pourra avoir lieu.

- Pour supprimer l'application confirmant le privilège de suppression de l'application, saisissez :

```
msiexec /x <nom_du_paquet> KLUNINSTPASSWD=***** : supprime l'application en mode interactif ;
```

```
msiexec /x <nom_du_paquet> KLUNINSTPASSWD=***** /qn – supprime l'application en mode non interactif.
```

ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit – est un système qui permet d'exécuter, de manière centralisée, les principales tâches d'administration de la sécurité des ordinateurs du réseau d'une entreprise. Il repose sur les applications faisant partie de la suite Kaspersky Business Optimal et Kaspersky Corporate Suite. Kaspersky Administration Kit prend en charge toutes les configurations réseau utilisant le protocole TCP/IP.

Kaspersky Administration Kit est un outil pour administrateurs de réseaux d'entreprise et pour responsables de sécurité antivirale.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 est un des logiciels de Kaspersky Lab qui peut être administré directement via l'interface, via la ligne de commande (cette méthode est décrite ci-dessus dans la documentation) ou via Kaspersky Administration Kit (pour autant que l'ordinateur soit inclus dans le système d'administration centralisée à distance).

Afin d'administrer Kaspersky Anti-Virus via Kaspersky Administration Kit, procédez comme suit :

- déployez le *Serveur d'administration* dans le réseau ;
- installez la *Console d'administration* sur le poste de travail de l'administrateur (pour de plus amples informations, consultez le "Manuel de déploiement de Kaspersky Administration Kit") ;
- installez l'*Agent d'administration* sur les ordinateurs du réseau (fait partie de Kaspersky Administration Kit). Pour de plus amples informations sur l'installation à distance de Kaspersky Anti-Virus sur les ordinateurs du réseau, consultez le "Manuel de déploiement de Kaspersky Administration Kit".

Avant d'actualiser la version du module externe d'administration de Kaspersky Anti-Virus via Kaspersky Administration Kit, il est nécessaire de quitter la Console d'administration.

L'administration de l'application via Kaspersky Administration Kit s'opère grâce à la Console d'administration (cf. ill. ci-après). Cette console 'se présente sous la forme d'une interface standard intégrée au MMC. Grâce à elle, l'administrateur peut exécuter les tâches suivantes :

- installer et supprimer à distance Kaspersky Anti-Virus et l'*Agent d'administration* sur les ordinateurs du réseau ;
- configurer à distance Kaspersky Anti-Virus sur les ordinateurs du réseau ;
- actualiser les bases et les modules de Kaspersky Anti-Virus ;
- administrer les licences d'utilisation de Kaspersky Anti-Virus sur les ordinateurs du réseau ;

- consulter les informations relatives à l'activité de l'application sur les ordinateurs clients.

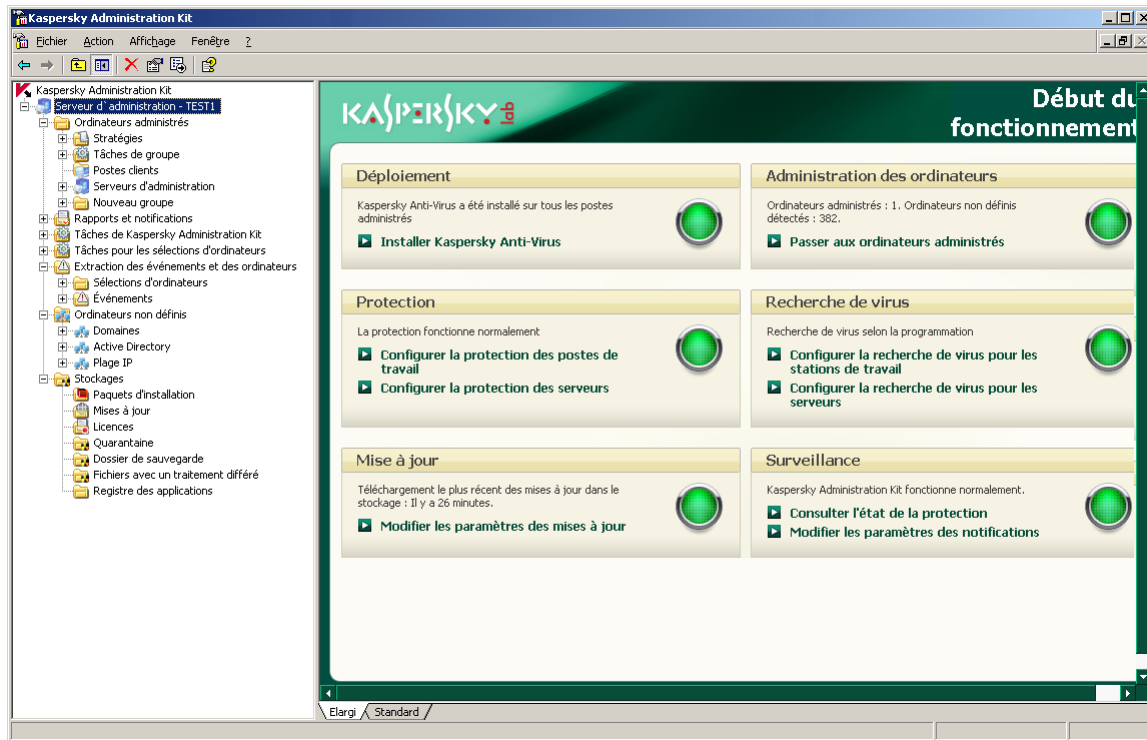


Illustration 11. Ouvrez la console d'administration de Kaspersky Administration Kit

L'apparence de la fenêtre principale de Kaspersky Administration Kit peut varier en fonction du système d'exploitation de l'ordinateur.

En cas d'utilisation de Kaspersky Administration Kit, l'administration s'opère selon les paramètres des stratégies, les paramètres des tâches et les paramètres de l'application définis par l'administrateur.

Une action portant un nom et exécutée par l'*application* s'appelle une tâche. Fonctionnellement, les tâches sont catégorisées en plusieurs *types*: tâche de recherche de virus, tâche de mise à jour de l'application, annulation d'une mise à jour, tâche d'installation du fichier clé.

A chaque tâche correspond un groupe de paramètres que le programme applique à l'exécution de la tâche. Les paramètres communs à tous les types de tâche sont appelés les *paramètres de l'application*. Les paramètres spécifiques à chaque type de tâche s'intitulent les *paramètres de tâche*. Aucun conflit n'est possible entre les paramètres de l'application et les paramètres de tâche.

Parmi les particularités de l'administration centralisée, citons la répartition des ordinateurs distants en groupe et l'administration des paramètres via la création et la définition de stratégies de groupe.

La stratégie – est un ensemble de paramètres de fonctionnement de l'application dans le groupe ainsi qu'un ensemble de restrictions sur la redéfinition des paramètres lors de la configuration de l'application et des tâches sur un ordinateur client distant. La stratégie inclut les paramètres permettant de configurer toutes les fonctionnalités de l'application, à l'exception de paramètres spécifiques à certains modèles de tâche. Il peut notamment s'agir des paramètres de programmation.

La stratégie comprend par exemple les paramètres :

- communs à tous les types de tâche, à savoir les paramètres de l'application ;
- communs à tous les modèles de tâche d'un type donné, à savoir la majeure partie des paramètres de tâche.

En d'autres termes, la stratégie de Kaspersky Anti-Virus, dont font partie les tâches de protection et de recherche de virus, comprend tous les paramètres utilisés par l'ensemble des tâches exécutées mais n'inclut pas la programmation de ces tâches, les paramètres définissant la zone d'analyse, etc.

DANS CETTE SECTION

Administration du logiciel.....	119
Analyse antivirus des fichiers	124
Administration des stratégies	129

ADMINISTRATION DU LOGICIEL

Kaspersky Administration Kit offre la possibilité d'effectuer à distance les actions suivantes: lancer et arrêter Kaspersky Anti-Virus sur un poste client, configurer les paramètres de l'application, activer ou désactiver la protection de l'ordinateur et configurer les rapports et dossiers.

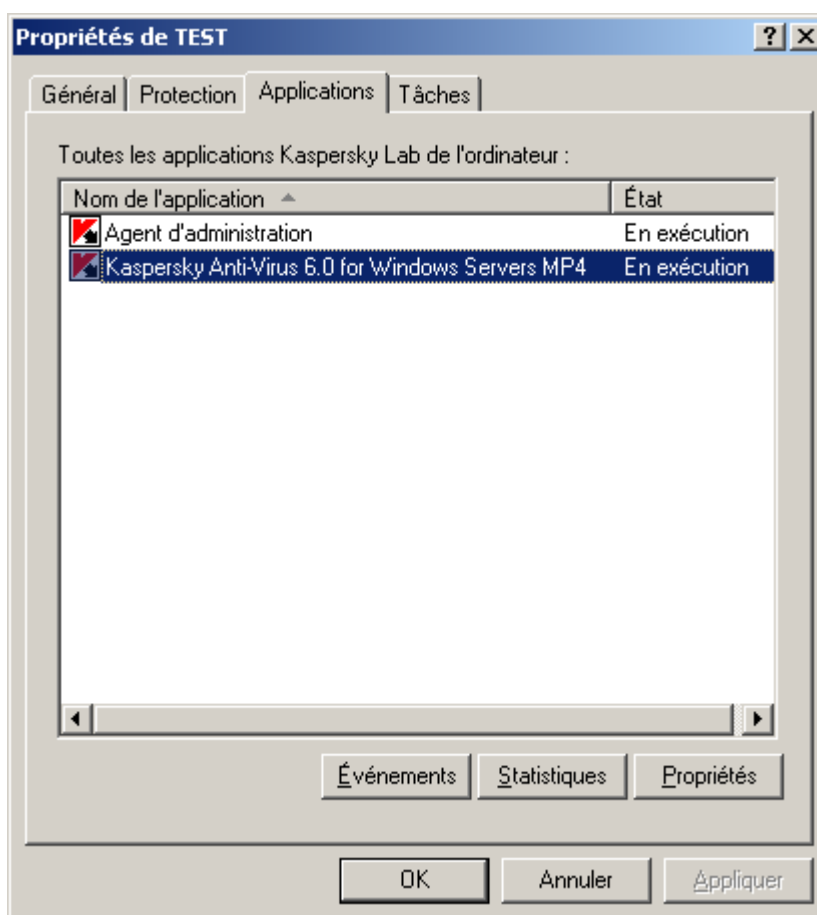


Illustration 12. Fenêtre des propriétés de l'ordinateur client. Onglet **Applications**

➔ Pour accéder à l'administration des paramètres de l'application, procédez comme suit :

1. Ouvrez la console d'administration de Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe dont fait partie le poste client.

3. Sous le groupe sélectionné, ouvrez le dossier **Ordinateurs** et choisissez dans le panneau des résultats l'ordinateur dont vous souhaitez modifier les paramètres de l'application.
4. Sélectionnez l'option **Propriétés** dans le menu contextuel ou dans le menu **Action** de manière à ouvrir la fenêtre des propriétés du poste client.
5. L'onglet **Applications** de la fenêtre des propriétés de l'ordinateur client reprend la liste complète de toutes les applications Kaspersky Lab installées sur l'ordinateur client. Sélectionnez l'application **Kaspersky Anti-Virus 6.0 for Windows Servers MP4**.

En bas de la liste des applications, vous verrez un ensemble de boutons qui vous permettront de :

- consulter la liste des événements survenus dans l'application au niveau de l'ordinateur client et enregistrés sur le Serveur d'administration ;
- consulter les statistiques actuelles sur l'activité de l'application ;
- configurer les paramètres de l'application (cf. page [121](#)).

LANCEMENT ET ARRÊT DE L'APPLICATION

La gestion de l'arrêt et du lancement de Kaspersky Anti-Virus 6.0 sur le poste distant s'effectue depuis la fenêtre des propriétés de l'application (cf. ill. ci-dessous).

La partie supérieure de la fenêtre indique le nom de l'application installée, les informations sur la version, la date d'installation, son état (application en exécution ou non sur l'ordinateur local) ainsi que les informations sur l'état des bases de l'application.

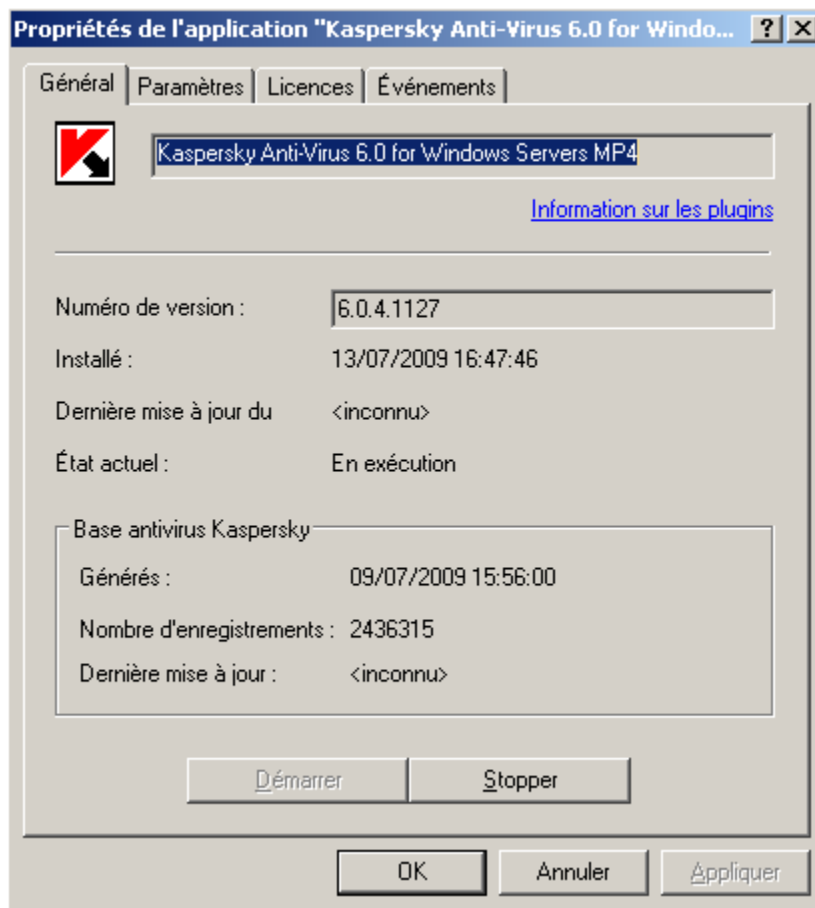


Illustration 13. Fenêtre des propriétés de l'application. Onglet **Général**

➤ Pour arrêter ou lancer une application sur un ordinateur distant, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client souhaité (cf. page 119) et sélectionnez l'onglet **Applications**.
2. Sélectionnez l'application **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** et cliquez sur le bouton **Propriétés**.
3. Dans l'onglet **Général** de la fenêtre des propriétés de l'application, cliquez sur le bouton **Arrêter** pour arrêter l'application ou sur **Démarrer** pour la démarrer.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

Pour afficher ou modifier les paramètres de l'application, utilisez l'onglet **Paramètres** de la fenêtre des propriétés de l'application (cf. ill. ci-dessous). Les autres onglets sont des onglets standards de l'application Kaspersky Administration Kit. Vous trouverez leur description détaillée dans le manuel de référence correspondant.

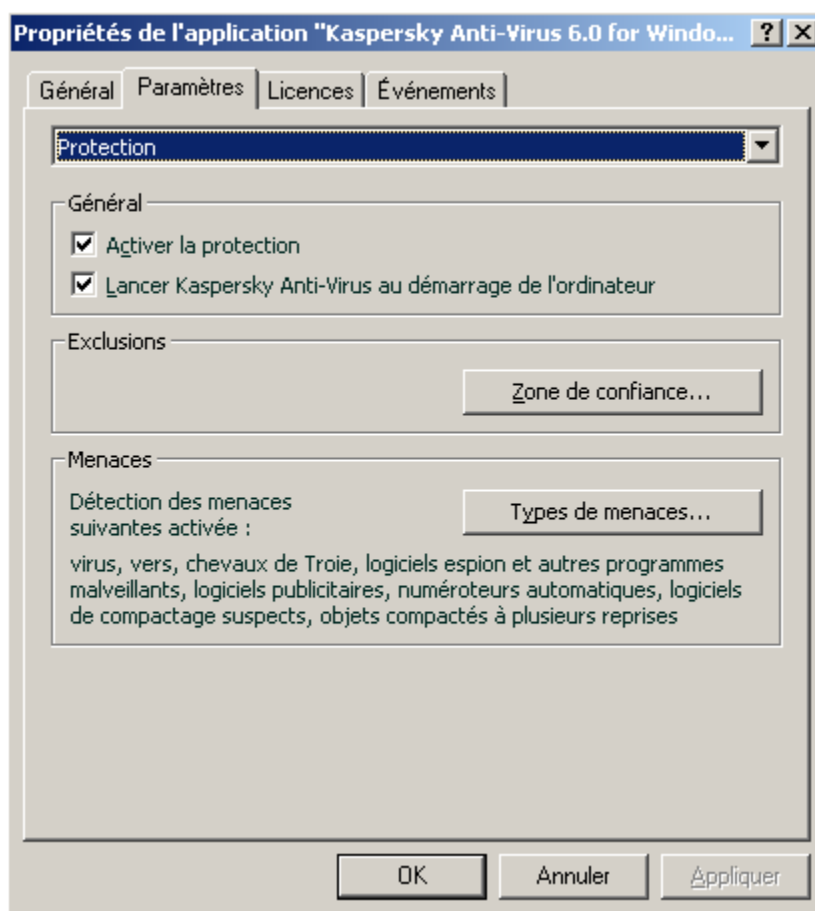


Illustration 14. Fenêtre des propriétés de l'application. Onglet **Paramètres**

Si une stratégie (cf. page 130), interdisant la modification de certains paramètres a été créée pour l'application, la modification de la configuration de l'application sera impossible.

➤ Pour consulter et modifier les paramètres de l'application, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client souhaité (cf. page 119) et sélectionnez l'onglet **Applications**.
2. Sélectionnez l'application **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** et cliquez sur le bouton **Propriétés**.

3. Dans la fenêtre ouverte des propriétés de l'application sous l'onglet **Paramètres** vous pouvez configurer les paramètres généraux de Kaspersky Anti-Virus, les rapports et dossiers ainsi que les paramètres réseaux. Pour ce faire, il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure.

VOIR EGALEMENT

Lancement de l'application au démarrage du système d'exploitation.....74

Sélection des catégories de menaces identifiées.....74

Constitution de la zone de confiance.....75

Configuration de l'envoi des notifications par courrier électronique.....85

CONFIGURATION DES PARAMETRES SPECIFIQUES

Lorsque vous gérez Kaspersky Anti-Virus par le biais de Kaspersky Administration Kit, vous avez la possibilité d'activer ou désactiver l'interaction avec l'utilisateur, de configurer la visibilité externe de l'application, les paramètres de protection par mot de passe et de modifier les informations d'assistance technique. Ces paramètres sont modifiables dans l'écran des propriétés de l'application (cf. ill. ci-dessous).

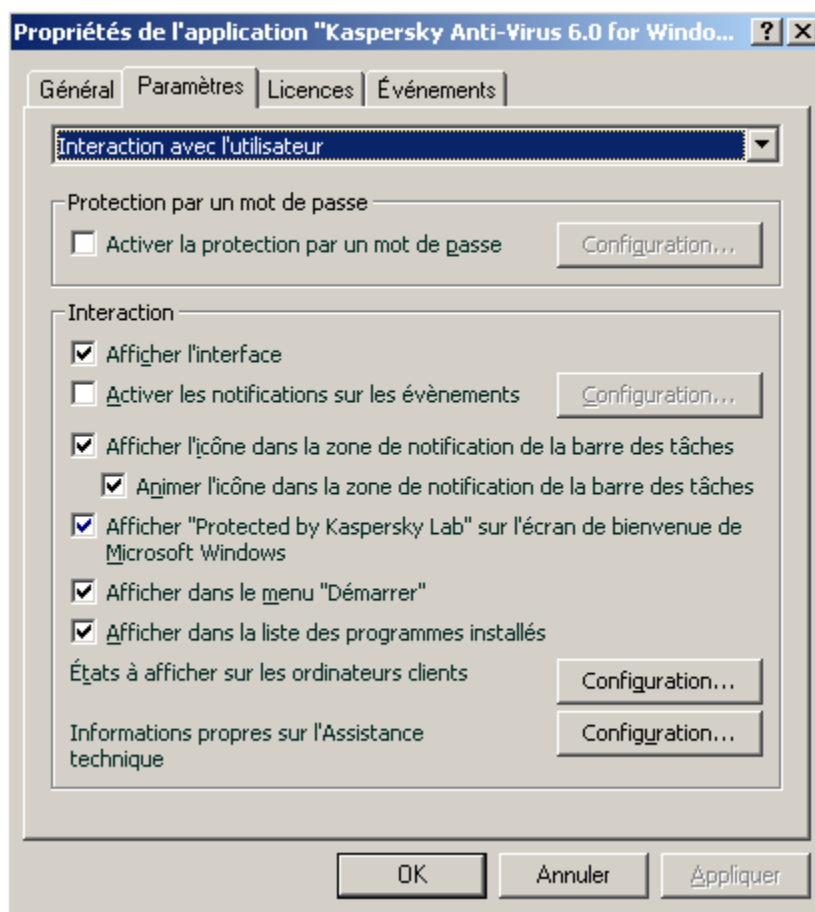


Illustration 15. Fenêtre des propriétés de l'application. Configuration des paramètres spécifiques

Pour protéger l'accès à Kaspersky Anti-Virus par un mot de passe, cochez la case Activer la protection par mot de passe dans le bloc **Protection par un mot de passe**. Indiquez le mot de passe et la zone restreinte d'accès dans la fenêtre ouverte lorsque vous cliquez sur **Configuration**.

Pour protéger le système contre la suppression non autorisée de l'application sur l'ordinateur local, cochez la case **Activer la protection contre la suppression**. Dans la fenêtre qui s'ouvre après que vous aurez cliqué sur **Configuration**, indiquez le mot de passe pour le supprimer ou confirmer.

Pour protéger l'accès à Kaspersky Anti-Virus par un mot de passe, cochez la case **Activer la protection par mot de passe**. Indiquez le mot de passe et la zone restreinte d'accès dans la fenêtre ouverte lorsque vous cliquez sur **Configuration**.

Pour protéger le système contre la suppression non autorisée de l'application sur l'ordinateur local, cochez la case **Activer la protection contre la suppression**. Dans la fenêtre qui s'ouvre après que vous aurez cliqué sur **Configuration**, indiquez le mot de passe pour le supprimer ou confirmer.

Le groupe **Interaction** vous permet de spécifier les paramètres d'interaction entre l'utilisateur et l'interface de Kaspersky Anti-Virus :

- Si la case **Interdire interaction entre l'utilisateur et l'interface** est sélectionnée, un utilisateur travaillant sur un ordinateur distant qui voit s'afficher l'icône de Kaspersky Anti-Virus et les messages pourra prendre des décisions conformément aux actions proposées par les fenêtres de notification concernant les événements qui surgissent. Cochez la case pour empêcher le mode interactif de l'application. Pour cacher à l'utilisateur le fait que l'application est installée sur son ordinateur, cochez la case **Cacher entièrement la présence de l'application installée**.
- Dans la fenêtre **Apparence** qui s'ouvre après que vous aurez cliqué sur **Configuration** vous permet de modifier les informations concernant le service d'assistance technique présentes dans la section Informations relatives au service d'assistance technique de Kaspersky Anti-Virus, sous l'entrée **Assistance technique** sur l'ordinateur distant.

Pour modifier la zone supérieure, saisissez les informations d'assistance technique fournies. Dans la zone inférieure, vous pouvez modifier les hyperliens s'affichant dans la section **Liens utiles** de la fenêtre **Assistance technique**, accessible via le lien **Assistance technique** dans la fenêtre principale de Kaspersky Anti-Virus.

Pour composer la liste, utilisez les boutons **Ajouter**, **Modifier**, **Supprimer**. Kaspersky Anti-Virus ajoutera un nouveau lien en début de liste. Pour modifier l'ordre des liens dans la liste, utilisez les boutons **Monter** et **Descendre**.

Si la fenêtre ne contient pas de données, les informations par défaut sur l'assistance technique ne pourront pas être modifiées.

Le groupe **États de l'application** vous permet de spécifier les statuts de l'application qui seront affichés dans la fenêtre principale de Kaspersky Anti-Virus. Pour ce faire, cliquez sur **Configuration** et dans la fenêtre qui s'ouvre, cliquez sur à côté des états requis. Cette fenêtre vous permet de configurer le contrôle de validité des bases de l'application.

Le groupe **Apparence** vous permet de configurer le mode d'interaction de Kaspersky Anti-Virus sur l'ordinateur distant: affichage de la notification de protection sur le bureau Microsoft Windows, affichage de l'icône de Kaspersky Anti-Virus dans le panneau de configuration, l'envoi de notifications d'événements (par exemple, détection d'un objet dangereux).

Si une stratégie (cf. page 130), interdisant la modification de certains paramètres a été créée pour l'application, la modification de la configuration de l'application sera impossible.

➔ Pour afficher ou modifier les paramètres spécifiques de l'application, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client souhaité (cf. page 119) et sélectionnez l'onglet **Applications**.
2. Sélectionnez l'**application Kaspersky Anti-Virus 6.0 for Windows Servers MP4** et cliquez sur le bouton Propriétés.
3. Dans la fenêtre ouverte des propriétés de l'application, sous l'onglet **Paramètres**, sélectionnez le point **Interaction avec l'utilisateur** dans la liste déroulante et configurez les paramètres.

ANALYSE ANTIVIRUS DES FICHIERS

Cette rubrique est consacrée à l'administration de tâches pour Kaspersky Anti-Virus. Pour de plus amples informations concernant la gestion des tâches via Kaspersky Administration Kit, référez-vous au Guide de l'administrateur correspondant.

Un ensemble de tâches système est créé pour chaque ordinateur du réseau lors de l'installation. Cette liste contient les tâches de protection (Antivirus Fichiers) et les tâches d'analyse antivirus (Analyse complète, Analyse rapide) et les tâches de mise à jour (la mise à jour des bases et des modules de l'application, annulation de la dernière mise à jour).

Vous pouvez administrer le lancement des tâches système et en configurer les paramètres. Il est toutefois impossible de les supprimer.

Vous pouvez également créer des tâches spécifiques (cf. page [125](#)), par exemple des tâches d'analyse, de mise à jour de l'application, d'annulation des mises à jour ou d'installation de fichier de licence.

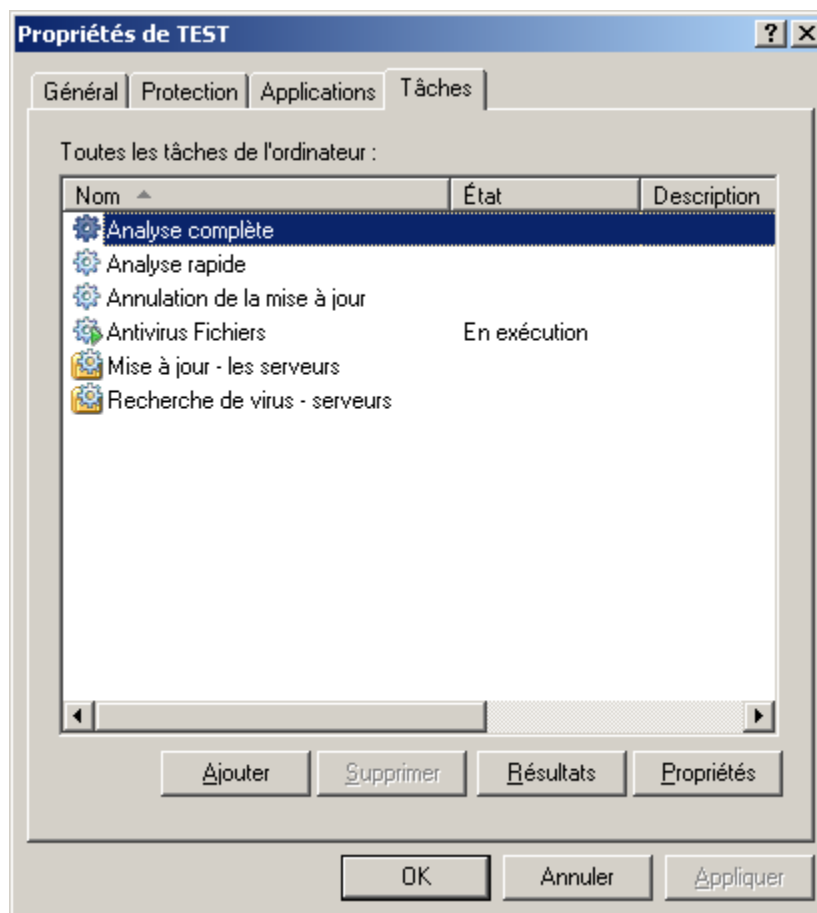


Illustration 16. Fenêtre des propriétés de l'ordinateur client. Onglet **Tâches**

➤ Pour ouvrir la liste des tâches créées sur le poste client, procédez comme suit :

1. Ouvrez la console d'administration de Kaspersky Administration kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe dont fait partie le poste client.
3. Sous le groupe sélectionné, ouvrez le dossier **Ordinateurs clients** et choisissez dans le panneau des résultats l'ordinateur dont vous souhaitez modifier les paramètres de l'application.
4. Sélectionnez l'option **Propriétés** dans le menu contextuel ou dans le menu **Action** de manière à ouvrir la fenêtre des propriétés du poste client.

- Dans la fenêtre des propriétés du poste client, sélectionnez l'onglet **Tâches** dans lequel est présentée la liste complète des tâches créées sur l'ordinateur.

LANCEMENT ET ARRÊT DES TACHES

Le lancement d'une tâche sur l'ordinateur est possible uniquement si l'application correspondante est lancée (cf. page [120](#)). En cas d'arrêt de l'application, l'exécution des tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide de la commande du menu contextuel) ou depuis la fenêtre d'examen des paramètres de la tâche. Vous pouvez suspendre l'exécution d'une tâche puis la reprendre.

➤ *Afin de lancer, arrêter, interrompre ou reprendre manuellement une tâche, procédez comme suit :*

- Ouvrez la fenêtre des propriétés du poste client et sélectionnez l'onglet **Tâches**.
- Sélectionnez la tâche souhaitée et ouvrez son menu contextuel. Sélectionnez le point **Lancer** pour lancer la tâche ou le point **Arrêter** – pour son arrêt. Vous pouvez aussi utiliser les points similaires dans le menu **Action**.

Le menu contextuel ne permet pas de suspendre et de reprendre la tâche.

ou

Sélectionnez la tâche souhaitée dans la liste et cliquez sur le bouton **Propriétés**. Dans l'onglet **Général** de la fenêtre des propriétés de la tâche, vous trouverez des boutons permettant de lancer, arrêter, suspendre ou reprendre la tâche.

CREATION D'UNE TACHE

Lorsque vous gérez Kaspersky Anti-Virus via Kaspersky Administration Kit, vous avez la possibilité de créer les types de tâches suivantes:

- des tâches locales, définies pour un ordinateur client distinct ;
- des tâches de groupe, définies pour les ordinateurs appartenant à un groupe d'administration donné ;
- des tâches pour une sélection d'ordinateurs, définies pour certains ordinateurs d'un groupe d'administration donné ;
- des tâches Kaspersky Administration Kit, dédiées au Serveur de mise à jour: tâches de mise à jour, tâches de copie de sauvegarde et tâches d'envoi de rapports.

Les tâches pour une sélection d'ordinateurs ne sont exécutées que sur les ordinateurs faisant partie de la sélection. La tâche d'installation à distance définie pour les ordinateurs d'un groupe ne sera pas appliquée aux nouveaux ordinateurs clients qui seraient ajoutés à ce groupe. Il faudra donc créer une nouvelle tâche ou modifier comme il se doit les paramètres de la tâche existante.

Les tâches peuvent être associées aux actions suivantes :

- configurez les paramètres de la tâche ;
- surveillance de l'exécution de la tâche ;
- copie et transfert d'une tâche depuis un groupe vers un autre et suppression d'une tâche par le biais des options **Copier / Coller, Couper / Coller et Supprimer** du menu contextuel ou du menu **Action**.

- importation et exportation de tâches.

Pour de plus amples informations concernant le fonctionnement des tâches, référez-vous au Manuel de référence de Kaspersky Administration Kit.

➤ *Pour créer une tâche locale, procédez comme suit :*

1. Ouvrez la fenêtre des propriétés du poste client et sélectionnez l'onglet **Tâches**.
2. Cliquez sur le bouton **Ajouter**.
3. Cette action entraînera l'ouverture de l'assistant pour la création d'une tâche (cf. page [126](#)). Suivez les instructions.

➤ *Pour créer une tâche de groupe, procédez comme suit :*

1. Ouvrez la console d'administration Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe souhaité.
3. Dans le groupe sélectionné, ouvrez le sous-dossier **Tâches de groupe** dans lequel seront présentées l'ensemble des tâches créées pour ce groupe.
4. Cliquez sur le lien **Créer une nouvelle tâche** dans le panneau des tâches pour lancer l'assistant de création d'une nouvelle tâche. Pour de plus amples informations sur la création des tâches de groupe, référez-vous au Manuel de référence de Kaspersky Administration Kit.

➤ *Pour créer une tâche destinée à une sélection d'ordinateurs (tâche Kaspersky Administration Kit), procédez comme suit :*

1. Ouvrez la console d'administration de Kaspersky Administration Kit.
2. Sélectionnez le dossier **Tâches pour une sélection d'ordinateurs (Tâches Kaspersky Administration Kit)**.
3. Cliquez sur le lien **Créer une nouvelle tâche** dans le panneau des tâches pour lancer l'assistant de création d'une nouvelle tâche. Pour de plus amples informations sur la création de tâches Kaspersky Administration Kit et de tâches destinées à une sélection d'ordinateurs, référez-vous au Manuel de référence de Kaspersky Administration Kit.

ASSISTANT POUR LA CREATION D'UNE TACHE LOCALE

L'Assistant pour la création d'une tâche locale peut être lancé depuis le menu contextuel ou la fenêtre des propriétés du poste client.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter le programme à n'importe quelle étape, cliquez sur **Annuler**.

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA TACHE

La première fenêtre de l'Assistant nécessite l'encodage du nom de la tâche (champ **Nom**).

ETAPE 2. SELECTION DE L'APPLICATION ET DU TYPE DE TACHE

Au cours de cette étape, vous devez préciser l'application pour laquelle vous créez la tâche : Kaspersky Anti-Virus 6.0 for Windows Servers MP4 ou Agent d'administration. Outre cela, il est nécessaire de sélectionner le type de tâche. Les tâches suivantes peuvent être créées pour Kaspersky Anti-Virus 6.0 :

- *Recherche de virus* – tâche permettant de rechercher des virus dans les zones spécifiées par l'utilisateur.

- *Mise à jour* – tâche permettant de télécharger et d'installer des mises à jour pour l'application.
- *Annulation d'une mise à jour* – tâche permettant d'annuler la dernière mise à jour de l'application.
- *Installation d'un fichier de licence* – tâche permettant d'installer le fichier de licence d'une nouvelle licence nécessaire au fonctionnement de l'application.

ETAPE 3. CONFIGURATION DES PARAMETRES DU TYPE DE TACHE SELECTIONNE

Selon le type de tâche sélectionné lors de l'étape précédente, le contenu de la fenêtre des paramètres varie.

Pour une tâche de recherche de virus, il faut indiquer l'action (cf. page 53) que Kaspersky Anti-Virus doit effectuer en présence d'un objet dangereux, et créer la liste des objets à analyser (cf. page 51).

Pour une tâche de mise à jour des bases et des modules de l'application, il faut spécifier la source à partir de laquelle seront téléchargées les mises à jour (cf. page 63). Les mises à jour sont téléchargées par défaut depuis le serveur de mise à jour de l'application Kaspersky Administration Kit.

Une tâche d'annulation de mises à jour ne présente aucun paramètre spécifique.

Pour une tâche d'installation d'un fichier clé, utilisez le bouton **Parcourir** pour spécifier l'emplacement du fichier clé. Pour ajouter le fichier clé d'une licence complémentaire, cochez la case correspondante . Une licence complémentaire devient active lorsque la clé active arrive à échéance.

Des informations relatives à la licence spécifiée (numéro de licence, type et date de fin) sont affichées dans le champ inférieur.

ETAPE 4. CONFIGURATION DE LA PROGRAMMATION

Une fois que vous aurez configuré la tâche, vous aurez la possibilité de programmer son lancement automatique.

Pour ce faire, utilisez la liste déroulante de l'écran de configuration de la programmation pour sélectionner la périodicité de lancement de la tâche et spécifiez les paramètres de programmation dans la partie inférieure de l'écran.

ETAPE 5. FIN DE LA CREATION D'UNE TACHE

La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche.

CONFIGURATION DES TACHES

La configuration des tâches de l'application via Kaspersky Administration Kit est identique à la configuration via l'interface locale de Kaspersky Anti-Virus. La seule différence réside au niveau des paramètres définis individuellement pour cette tâche tels que la programmation du lancement de la tâche d'analyse, ou les paramètres spécifiques à Kaspersky Administration Kit, par exemple les paramètres autorisant (interdisant) l'utilisateur à gérer une tâche locale d'analyse.

Si une stratégie (cf. page 130), interdisant la modification de certains paramètres a été créée, la modification de la configuration de la tâche sera impossible.

Tous les onglets de la fenêtre des propriétés de la tâche, excepté celui intitulé **Paramètres** (cf. ill. ci-dessous) sont des onglets standards de Kaspersky Administration Kit. Vous trouverez leur description détaillée dans le manuel de référence correspondant. L'onglet **Paramètres** contient des paramètres spécifiques à Kaspersky Anti-Virus. Son contenu varie en fonction du type de tâche sélectionné.

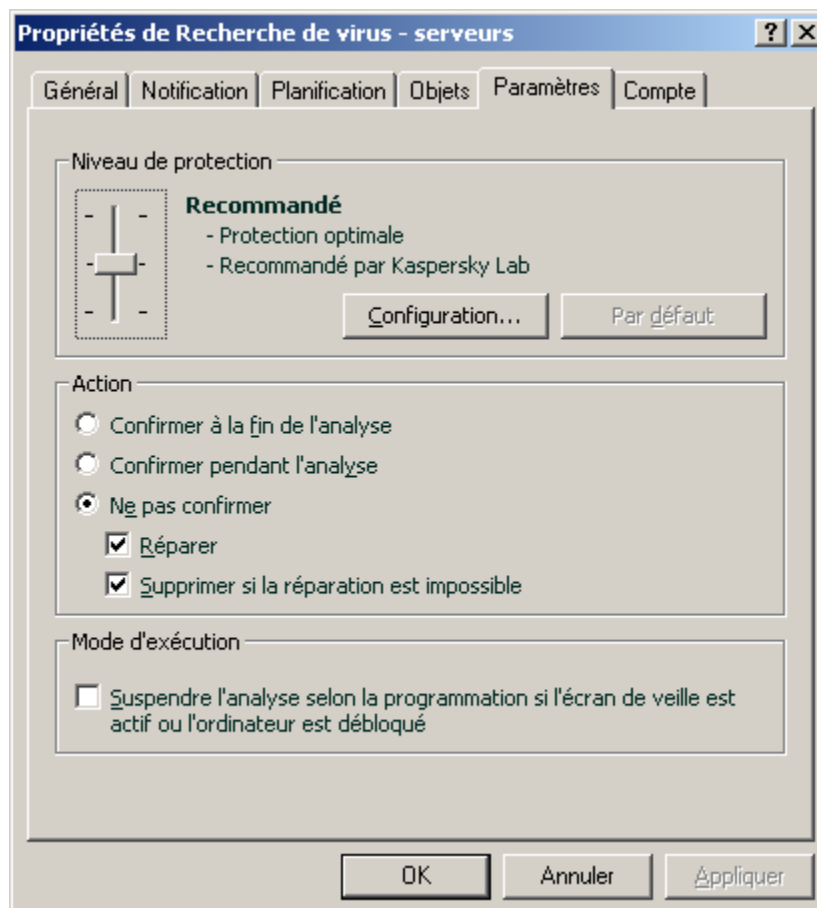


Illustration 17. Fenêtre des propriétés de la tâche. Onglet **Paramètres**

► Pour visualiser ou modifier une tâche locale, procédez comme suit :

1. Ouvrez la fenêtre des propriétés du poste client et sélectionnez l'onglet **Tâches**.
2. Sélectionnez la tâche dans la liste et appuyez sur le bouton **Propriétés**. Cette action permet d'ouvrir la fenêtre des paramètres de la tâche.

► Pour une tâche de groupe, procédez comme suit :

1. Ouvrez la console d'administration de Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe souhaité.
3. Dans le groupe sélectionné, ouvrez le sous-dossier **Tâches de groupe** dans lequel seront présentées l'ensemble des tâches créées pour ce groupe.
4. Sélectionnez la tâche souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

Le panneau des tâches présente quelques informations sur la tâche ainsi que des liens permettant de gérer son exécution et de modifier ses paramètres. Pour de plus amples informations sur les tâches de groupe, référez-vous au Manuel de référence de Kaspersky Administration Kit.

➤ Pour les tâches destinées à une sélection d'ordinateurs (tâches Kaspersky Administration Kit), procédez comme suit :



1. Ouvrez la console d'administration de Kaspersky Administration Kit.
2. Sélectionnez le dossier **Tâches pour une sélection d'ordinateurs (Tâches Kaspersky Administration Kit)**.
3. Sélectionnez la tâche souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

Le panneau des tâches présente quelques informations sur la tâche ainsi que des liens permettant de gérer son exécution et de modifier ses paramètres. Pour de plus amples informations sur les tâches Kaspersky Administration Kit et tâches destinées à une sélection d'ordinateurs, référez-vous au Manuel de référence de Kaspersky Administration Kit.

ADMINISTRATION DES STRATEGIES

La définition de stratégie est un moyen permettant d'appliquer une configuration des tâches et de l'application identique à tous les ordinateurs clients faisant partie d'un groupe d'administration.

Cette rubrique est consacrée à la création et à la configuration de stratégies pour Kaspersky Anti-Virus 6.0 for Windows Servers MP4. Vous trouverez de plus amples informations sur le concept de l'administration des stratégies via Kaspersky Administration Kit dans le manuel de l'administrateur de cette application.

Pendant la création et la configuration de la stratégie, vous pouvez empêcher complètement ou partiellement la modification des paramètres de groupes imbriqués, de tâche ou d'application. Pour ce faire, cliquez sur . Pour les paramètres qui ne peuvent pas être modifiés, l'icône doit ressembler à .

➤ Pour ouvrir la liste des stratégies concernant Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe dont fait partie le poste client.
3. Dans le groupe sélectionné, ouvrez le sous-dossier **Stratégies**. L'arborescence de la console affichera alors l'ensemble des stratégies créées pour ce groupe.

CREATION D'UNE STRATEGIE

Lorsque vous gérez Kaspersky Anti-Virus via Kaspersky Administration Kit, vous avez la possibilité de créer des stratégies le concernant.

Les stratégies peuvent être associées aux actions suivantes :

- configuration des paramètres d'une stratégie ;
- copie et transfert d'une tâche depuis un groupe vers un autre et suppression d'une tâche par le biais des options **Copier / Coller**, **Couper / Coller** et **Supprimer** du menu contextuel ou du menu **Action** ;
- importation ou exportation des paramètres d'une stratégie.

Pour de plus amples informations concernant le fonctionnement des stratégies, référez-vous au manuel de référence de Kaspersky Administration Kit.

➤ Pour créer une stratégie, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe souhaité.

3. Dans le groupe sélectionné, ouvrez le sous-dossier **Stratégies** dans lequel s'affichera l'ensemble des stratégies créées pour ce groupe.
4. Cliquez sur le lien **Créer une nouvelle stratégie** dans le panneau des tâches pour lancer l'assistant de création d'une nouvelle stratégie.
5. L'assistant pour la création d'une stratégie (cf. page [130](#)) est alors lancé dans la fenêtre ouverte. Suivez les instructions.

ASSISTANT POUR LA CREATION D'UNE STRATEGIE

L'assistant pour la création d'une stratégie se lance via le menu contextuel du dossier **Stratégies** correspondant au groupe d'administration souhaité ou par le biais du lien se trouvant dans le panneau des résultats (pour le dossier **Stratégies**).

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter le programme à n'importe quelle étape, cliquez sur **Annuler**.

ETAPE 1. SAISIE DES DONNEES GENERALES SUR LA STRATEGIE

Les premières fenêtres de l'Assistant sont des fenêtres d'introduction. Il faut à ce stade définir le nom de la stratégie (champ **Nom**) et sélectionnez l'application **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** dans la liste déroulante **Nom de l'application**.

Lorsque l'assistant pour la création d'une stratégie est démarré depuis le panneau des tâches du nœud **Stratégies** (via le lien **Créer une stratégie pour Kaspersky Anti-Virus for Windows Servers MP4**), le choix de l'application n'est pas présenté.

Si vous souhaitez créer une stratégie sur la base des paramètres d'une stratégie existante pour la version antérieure de l'application, cochez la case **Utiliser les paramètres des stratégies existantes** et sélectionnez la stratégie dont les paramètres seront utilisés dans la nouvelle stratégie. Pour définir la stratégie, cliquez sur **Sélectionner**, ce qui affichera la liste des stratégies existantes qui peuvent être utilisées lors de la création d'une stratégie.

ETAPE 2. SELECTION DE L'ETAT DE LA STRATEGIE

Une fois la stratégie créée, cette fenêtre vous propose de choisir l'état de la stratégie parmi la liste suivante: stratégie active, stratégie inactive. Pour de plus amples informations sur les états des stratégies, référez-vous au manuel de référence de Kaspersky Administration Kit.

Plusieurs stratégies peuvent être créées dans le groupe pour une application mais il ne peut y avoir qu'une seule stratégie active.

ETAPE 3. IMPORTATION DES PARAMETRES DE L'APPLICATION

Si vous possédez un fichier de paramètres précédemment sauvegardé, vous pouvez le désigner dans cette étape de l'Assistant grâce au bouton **Importer**. Les paramètres importés apparaîtront dans les fenêtres suivantes de l'Assistant.

ETAPE 4. CONFIGURATION DES PARAMETRES DE PROTECTION

Cette étape vous permet d'activer (désactiver), aussi que de configurer les composants de protection qui seront utilisés dans la stratégie.

Tous les composants de la protection sont activés par défaut. Pour désactiver un composant quelconque, désélectionnez la case qui se trouve en regard de son nom. Si vous souhaitez procéder à une configuration détaillée d'un composant de la protection, sélectionnez-le dans la liste et cliquez sur **Configuration**.

ETAPE 5. CONFIGURATION DE LA PROTECTION PAR UN MOT DE PASSE

Cette fenêtre de l'Assistant vous permet de configurer les paramètres de protection par mot de passe sur le fonctionnement avec l'application et sa suppression.

ETAPE 6. CONFIGURATION DE LA ZONE DE CONFIANCE

Cette fenêtre de l'assistant vous propose de configurer les paramètres de la zone de confiance: ajoutez dans la liste des applications de confiance les programmes utilisés pour administrer le réseau de manière à ce que Kaspersky Anti-Virus ne contrôle pas certains types de fichier.

ETAPE 7. CONFIGURATION DES PARAMETRES D'INTERACTION AVEC L'UTILISATEUR





Cette étape vous permet de spécifier les paramètres d'interaction entre l'utilisateur et l'interface de Kaspersky Anti-Virus :

- Affichage de l'interface de l'application sur un ordinateur distant.
- Notifications de l'utilisateur relatives aux événements.
- Affichage et animation de l'icône de l'application dans la zone de notification de la barre d'état.
- Affichage de "Protected by Kaspersky Lab" sur l'écran de bienvenue de Microsoft Windows.
- Affichage de l'application dans le menu "Démarrer".
- Affichage dans la liste des applications installées.

ETAPE 8. FIN DE LA CREATION D'UNE STRATEGIE

La dernière fenêtre de l'Assistant vous informe sur la réussite de la création de la stratégie.

Une fois l'assistant terminé, la stratégie est ajoutée au dossier **Stratégies** du groupe d'administration sélectionné et affichée dans l'arborescence de la console.

Vous pouvez ensuite modifier les paramètres de la stratégie créée et empêcher leur modification à l'aide des boutons  et  pour chaque groupe de paramètres. L'icône  indique que l'utilisateur du poste client n'a pas la possibilité de modifier la configuration. Alors que l'icône  signifie que l'utilisateur peut modifier les paramètres. La stratégie sera diffusée sur les ordinateurs clients lors de la première synchronisation des clients avec le serveur.

CONFIGURATION DE LA STRATEGIE

A cette étape, vous pouvez introduire des modifications dans la stratégie, interdire la modification de certains paramètres des stratégies des sous-groupes, de l'application et des tâches. Les paramètres de la stratégie sont modifiables depuis l'écran des propriétés de la stratégie (cf. ill. ci-dessous).

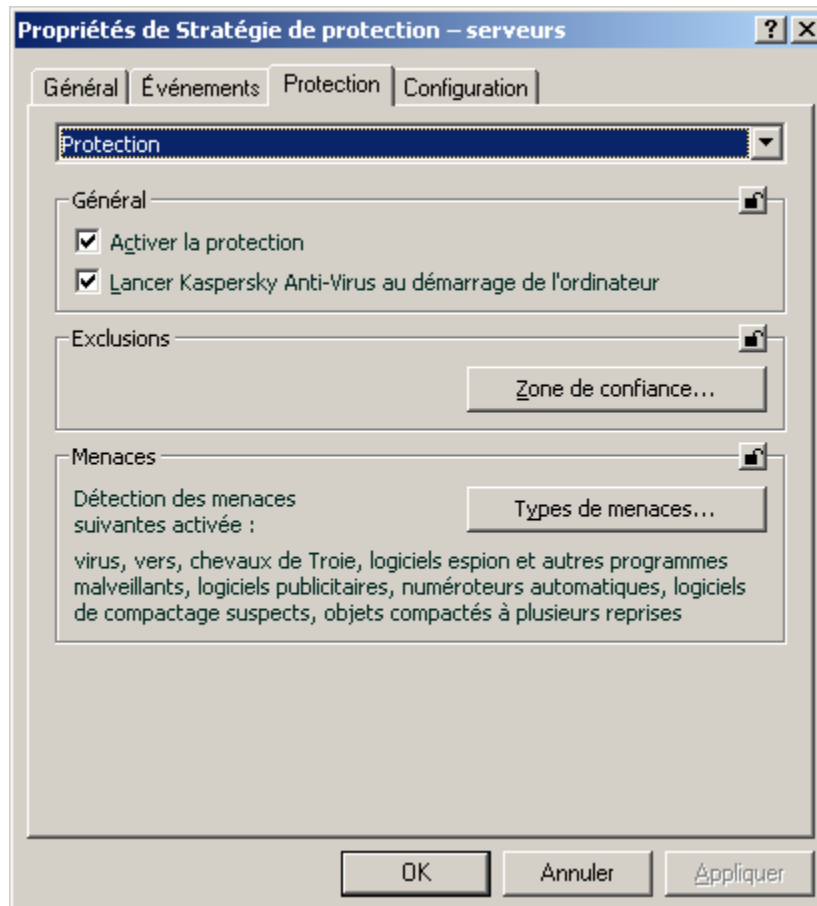


Illustration 18. Fenêtre des propriétés de la stratégie. L'onglet **Protection**

Tous les onglets (hormis **Protection** et **Configuration**) sont des onglets standards de Kaspersky Administration Kit. Vous trouverez leur description détaillée dans le manuel de référence correspondant.

Les paramètres de stratégie de Kaspersky Anti-Virus 6.0 comprennent les paramètres de l'application (cf. page [121](#)) et les paramètres des tâches. L'onglet **Configuration** contient les paramètres de l'application et l'onglet **Protection**, les paramètres des tâches.

Pour configurer les paramètres, il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure.

► Pour visualiser ou modifier les paramètres de la stratégie, procédez comme suit :

1. Ouvrez la console d'administration Kaspersky Administration Kit.
2. Dans **Ordinateurs gérés**, ouvrez le dossier portant le nom du groupe souhaité.
3. Dans le groupe sélectionné, ouvrez le sous-dossier **Stratégies** dans lequel s'affichera l'ensemble des stratégies créées pour ce groupe.
4. Sélectionnez la stratégie souhaitée dans l'arborescence de la console pour visualiser ou modifier ses propriétés.

5. Le panneau des tâches présente quelques informations sur la stratégie ainsi que des liens permettant de gérer son état et de modifier ses paramètres.

ou

Ouvrez le menu contextuel de la stratégie souhaitée et choisissez l'entrée **Propriétés** pour accéder à la fenêtre de configuration de la stratégie de Kaspersky Anti-Virus.

Pour de plus amples informations concernant le fonctionnement des stratégies, référez-vous au manuel de référence de Kaspersky Administration Kit.

UTILISATION D'UN CODE TIERS

Du code développé par des éditeurs tiers a été utilisé dans Kaspersky Anti-Virus.

DANS CETTE SECTION

Bibliothèque Boost-1.30.0	135
Bibliothèque LZMA SDK 4.40, 4.43	135
Bibliothèque Windows Template Library 7.5	135
Bibliothèque Windows Installer XML (WiX) toolset 2.0	136
Bibliothèque ZIP-2.31	139
Bibliothèque ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3	140
Bibliothèque UNZIP-5.51	140
Bibliothèque LIBPNG-1.0.1, LIBPNG-01/02/08, LIBPNG-01/02/12	141
Bibliothèque LIBJPEG-6B	143
Bibliothèque LIBUNGIF-04/01/04	145
Bibliothèque MD5 MESSAGE-DIGEST ALGORITHM-REV. 2	145
Bibliothèque MD5 MESSAGE-DIGEST ALGORITHM-V. 18/11/04	145
Bibliothèque INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04/11/99.....	145
Bibliothèque CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02/11/04	146
Bibliothèque COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum	146
Bibliothèque PLATFORM INDEPENDENT IMAGE CLASS	146
Bibliothèque FLEX PARSER (FLEXLEXER)-V. 1993.....	147
Bibliothèque ENSURECLEANUP, SWMRG, LAYOUT-V. 2000	147
Bibliothèque STDSTRING- V. 1999	148
Bibliothèque T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006	148
Bibliothèque NTSERVICE- V. 1997.....	149
Bibliothèque SHA-1-1.2.....	149
Bibliothèque COCOA SAMPLE CODE- V. 18/07/07	150
Bibliothèque PUTTY SOURCES-25/09/08	150
Autre information	151

BIBLIOTHEQUE BOOST-1.30.0

La bibliothèque Boost 1.30.0 a été utilisée dans le développement de l'application.

Copyright (C) 2003, Christof Meerwald

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.

BIBLIOTHEQUE LZMA SDK 4.40, 4.43

La bibliothèque LZMA SDK 4,40, 4,43 a été utilisée dans le développement de l'application.

BIBLIOTHEQUE WINDOWS TEMPLATE LIBRARY 7.5

La bibliothèque Windows Template Library 7.5 a été utilisée dans le développement de l'application.

Copyright (C) 2006, Microsoft Corporation

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce", "reproduction", "derivative works", and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

BIBLIOTHÈQUE WINDOWS INSTALLER XML (WIX) TOOLSET 2.0

La bibliothèque Windows Installer XML (WiX) toolset 2.0 toolset a été utilisée dans le développement de l'application.

Copyright (C) 2009, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of

software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED 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. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), 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 OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEQUE ZIP-2.31

La bibliothèque Zip-2.31 a été utilisée dans le développement de l'application.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

<ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved a été utilisée dans le développement de l'application.

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 following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) 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, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being 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 of the Info-ZIP URL(s).

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.

BIBLIOTHÈQUE ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3

La bibliothèque Zlib-1.0.4, ZLIB-1.0.8, Zlib-1.1.3, Zlib-1.2.3 a été utilisée dans le développement de l'application.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

 This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of 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 following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

BIBLIOTHEQUE UNZIP-5.51

La bibliothèque UnZip-5.51 a été utilisée dans le développement de l'application.

Copyright (c) 1990-2004, Info-ZIP

 This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved a été utilisée dans le développement de l'application.

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, 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, Christian Spieler, 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 following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) 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, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being 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 of the Info-ZIP URL(s).

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.

BIBLIOTHEQUE LIBPNG-1.0.1, LIBPNG-01/02/08, LIBPNG-01/02/12

La bibliothèque libpng-1.0.1, libpng-1.2.8, libpng-1.2.12 a été utilisée dans le développement de l'application.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 01/02/06, August 15, 2004, through 01/02/39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-01/02/05 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1,0.7, July 1, 2000, through 01/02/05 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1,0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0,97, January 1998, through 1,0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0,96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0,89, June 1996, through 0,96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0,88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0,5, May 1995, through 0,88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg" (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

BIBLIOTHEQUE LIBJPEG-6B

La bibliothèque libjpeg-6b a été utilisée dans le développement de l'application.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. 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) 1991-2009, Thomas G. Lane, Guido Vollbeding.

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, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

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."

BIBLIOTHEQUE LIBUNGIF-04/01/04

La bibliothèque libungif-4.1.4 a été utilisée dans le développement de l'application.

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.

BIBLIOTHEQUE MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

La bibliothèque MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 a été utilisée dans le développement de l'application.

BIBLIOTHEQUE MD5 MESSAGE-DIGEST ALGORITHM-V. 18/11/04

При создании программы использовалась библиотека MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

BIBLIOTHEQUE INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04/11/99

La bibliothèque Independent implementation of MD5 (RFC 1321)-v a été utilisée dans le développement de l'application. 04/11/99.

Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved a été utilisée dans le développement de l'application.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

BIBLIOTHÈQUE CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02/11/04

La bibliothèque Conversion routines between UTF32, UTF-16, and UTF-8-v a été utilisée dans le développement de l'application. 02/11/04.

Copyright 2001-2004 Unicode, Inc.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

BIBLIOTHÈQUE COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM

La bibliothèque Cool Owner Drawn Menus-v a été utilisée dans le développement de l'application. 2.4, 2.63 By Brent Corkum.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware, Shareware, Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

BIBLIOTHÈQUE PLATFORM INDEPENDENT IMAGE CLASS

La bibliothèque Platform Independent Image Class a été utilisée dans le développement de l'application.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

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.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEQUE FLEX PARSER (FLEXLEXER)-V. 1993

La bibliothèque Flex parser (FlexLexer)-v a été utilisée dans le développement de l'application. 1993.

Copyright (c) 1993 The Regents of the University of California

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

BIBLIOTHEQUE ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

La bibliothèque EnsureCleanup, SWMRG, Layout-v a été utilisée dans le développement de l'application. 2000.

Copyright (C) 2009, Microsoft Corporation

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252,227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52,227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

BIBLIOTHÈQUE STDSTRING- V. 1999

La bibliothèque StdString- v a été utilisée dans le développement de l'application. 1999.

Copyright (C) 1999, Joseph M. O'Leary

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your \$30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

BIBLIOTHEQUE T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

La bibliothèque T-Rex (tiny regular expression library)- v a été utilisée dans le développement de l'application. 2003-2006.

Copyright (C) 2003-2006, Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of 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 following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEQUE NTSERVICE- V. 1997

La bibliothèque NTService- v a été utilisée dans le développement de l'application. 1997.

Copyright (C) 1997, Joerg Koenig and the ADG mbH, Mannheim, Germany

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "///! TCW MOD"

BIBLIOTHEQUE SHA-1-1.2

La bibliothèque SHA-1-1.2 a été utilisée dans le développement de l'application.

Copyright (C) 2001, The Internet Society

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

BIBLIOTHEQUE COCOA SAMPLE CODE- V. 18/07/07

La bibliothèque Cocoa sample code- v a été utilisée dans le développement de l'application. 18/07/07.

Copyright (C) 2007, Apple Inc

Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. ("Apple")

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software (the "Apple Software"), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms; provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an "AS IS" basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEQUE PUTTY SOURCES-25/09/08

La bibliothèque PUTTY SOURCES-25.09.2008, 4,43 a été utilisée dans le développement de l'application. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified <http://www.opensource.org/licenses/> and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

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 SIMON TATHAM 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.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

AUTRE INFORMATION

L'analyse de la signature numérique électronique dans Kaspersky Anti-Virus repose sur la bibliothèque logicielle de protection de l'information "Crypto-Si" développée par CryptoEx OOO <http://www.cryptoex.ru>.

La composition et l'analyse de la signature numérique électronique dans Kaspersky Anti-Virus repose sur la bibliothèque logicielle de protection de l'information "Agava-C" développée par OOO "R-Alpha".

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.

GLOSSAIRE

A

ANALYSE A LA DEMANDE

Mode de fonctionnement initié par l'utilisateur et visant à analyser n'importe quel fichier.

ANALYSE DES DOSSIERS

Analyse des messages stockés sur le serveur de messagerie ainsi que du contenu des dossiers généraux, à l'aide de la dernière version des bases. L'analyse s'effectue en arrière-plan et peut être planifiée ou lancée manuellement. Tous les dossiers généraux et de messagerie (mailbox storage) sont analysés. L'analyse est capable de détecter les nouveaux virus dont la description manquait dans les bases lors de l'analyse précédente.

ANALYSEUR HEURISTIQUE

Technologie d'identification des menaces non reconnues par l'antivirus. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

APPLICATION INCOMPATIBLE

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Anti-Virus.

ARCHIVE

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

ATTAQUE VIRALE

Tentatives multiples d'infection virale d'un ordinateur.

B

BASES

Les bases de données sont créées par les experts de Kaspersky Lab et elles 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. Pour améliorer la qualité de la découverte de menaces, nous vous conseillons de télécharger fréquemment les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab.

BLOCAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

C

COPIE DE SAUVEGARDE

Création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et placement de cette copie dans la sauvegarde avec la possibilité de restaurer le fichier ultérieurement, par exemple pour l'analyse avec des bases actualisées.

D**DEGRE D'IMPORTANCE DE L'EVENEMENT**

Caractéristique de l'événement consignée dans le fonctionnement de l'application de Kaspersky Lab. Il existe 14 degrés d'importance :

Événement critique.

Refus de fonctionnement.

Avertissement.

Information.

Les événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

DOSSIER DE DONNEES

Dossier d'installation des services et bases de données nécessaires au bon fonctionnement de l'application. En cas de modification du dossier de données, toutes les informations qu'il contient doivent être conservées à une nouvelle adresse.

DOSSIER DE SAUVEGARDE

Dossier spécial où sont stockées les copies de données du serveur d'administration, préalablement créées par l'utilitaire de copie de sauvegarde.

DOSSIERS DE SAUVEGARDE

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression.

DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, 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 est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

E**EN-TETE**

L'information, qui est contenue dans le début du fichier ou du message, se compose des données de faibles niveaux selon l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements, tels que, les données de l'expéditeur, du destinataire et la date.

ETAT DE LA PROTECTION

État actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

F**FAUX-POSITIFS**

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

FICHER 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 le logiciel si celui-ci a été obtenu chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

FICHIERS COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

I**INTERCEPTEUR**

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

L**LES 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.

LICENCE ACTIVE

Licence en cours d'utilisation par l'application de Kaspersky Lab. La licence détermine la durée de validité du fonctionnement complet de l'application ainsi que la politique de licence de l'application. L'application ne peut avoir qu'une application active à la fois.

LICENCE COMPLEMENTAIRE

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 est arrivée à échéance.

LISTE "NOIRE" DES LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab préalablement bloquées, aux utilisateurs ayant transgressé les dispositions du contrat de licence et aux clés qui ont été émises mais qui, pour une quelconque raison, n'ont pas été vendues ou ont été échangées. Le fichier de la liste noire est indispensable au fonctionnement des applications de Kaspersky Lab. Le contenu du fichier est mis à jour en même temps que les bases.

M**MASQUE DE FICHIER**

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont * et ? (où * représente n'importe quel nombre de caractères et ? représente un caractère unique). A l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention! le nom et l'extension d'un fichier sont toujours séparés par un point.

MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés des serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR DISPONIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

MISE EN QUARANTAINE D'OBJETS

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante. Les objets mis en quarantaine peuvent être analysés à l'aide des bases antivirus mises à jour, être examinés par l'administrateur ou être envoyés à Kaspersky Lab.

N**NIVEAU RECOMMANDE**

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

O**OBJET CONTROLE**

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyé à l'application de Kaspersky Lab pour analyse.

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET IGNORE

Objet ignoré sans un quelconque changement. Des informations relatives à l'objet détecté seront inscrites dans le rapport pour autant que cela soit stipulé dans les paramètres du rapport.

OBJET INFECTE

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 OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET INFECTE POTENTIELLEMENT

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions com, exe, dll, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET POTENTIELLEMENT INFECTE

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 potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET SIMPLE

Corps de lettre ou pièce jointe, par exemple, sous d'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.

OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

P**PAQUET DE MISE A JOUR**

Ensemble de fichiers provenant d'Internet et s'installant sur votre ordinateur afin de mettre à jour une application.

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Tous les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION EN TEMPS REEL DES FICHIERS

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTECTION MAXIMALE

Niveau de protection le plus élevé que l'application peut garantir pour votre ordinateur. Ce niveau de protection antivirus permet d'analyser tous les fichiers présents sur l'ordinateur, les supports amovibles et les disques réseau éventuellement connectés.

Q**QUARANTAINE**

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

R

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

REPARATION 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. Si la réparation est la première action exécutée sur l'objet (toute première action exécutée sur l'objet directement après sa découverte), alors une copie de sauvegarde de l'objet sera créée au préalable. Une partie des données peut être perdue lors de la réparation. Vous pouvez utiliser cette copie par la suite pour restaurer l'objet à l'état qu'il avait avant la réparation.

REPARATION D'OBJETS LORS DU REDEMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

S

SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichier du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique considéré comme indésirable. Il se caractérise par la suppression physique du message. Cette méthode est recommandée lorsque le message est indubitablement indésirable. Une copie du message supprimé est conservée dans le dossier de sauvegarde (pour autant que cette fonctionnalité ne soit pas désactivée).

SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

T

TECHNOLOGIE I-CHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

la technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;

la technologie est compatible avec un nombre restreint de formats (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

V

VIRUS DE BOOT (AMORÇAGE)

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

VIRUS INCONNU

Nouveau virus pour lequel 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.

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

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'ACCEPTÉZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

LE LOGICIEL PEUT ÊTRE ACCOMPAGNE D'UN CONTRAT SUPPLÉMENTAIRE, OU D'UN DOCUMENT SUPPLÉMENTAIRE (LE " CONTRAT ADDITIONNEL "), QUI PEUT DETERMINER LE NOMBRE D'ORDINATEURS SUR LESQUELS PEUT ÊTRE UTILISÉ LE LOGICIEL, LA PÉRIODE D'UTILISATION DU LOGICIEL, LES TYPES D'OBJETS AUXQUELS IL EST DESTINÉ ET DIVERSES AUTRES CONDITIONS D'ACHAT, D'ACQUISITION ET D'UTILISATION SUPPLÉMENTAIRES. CE CONTRAT ADDITIONNEL EST PARTIE INTEGRANTE DU CONTRAT DE LICENCE.

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 patch, 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.
- 1.8. **Acquisition du logiciel** signifie son achat ou acquisition à des conditions définies dans un contrat additionnel, y compris une acquisition gratuite.

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 spécifiés dans les licences que vous avez obtenues auprès du Titulaire des droits, *sachant que*, sauf disposition contraire du contrat de licence, chaque licence achetée 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 acheté 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 ou comme spécifié dans le Contrat additionnel.
- 2.3. Si le Logiciel a été acheté sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'achat de la Licence du Logiciel ou comme spécifié dans le Contrat additionnel.
- 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 ou morales 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 acheté 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 acheté sur un support physique) ou stipulée pendant l'achat (si le Logiciel a été acheté 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 acheté 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 ou comme spécifié dans le Contrat additionnel.
- 3.3. Si le Logiciel a été acheté sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'achat ou comme spécifié dans le Contrat additionnel.
- 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.
- 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 acheté 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.

4. Assistance technique

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

- 5.1. 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.
- 5.2. Vous ne devez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.
- 5.3. 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.
- 5.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.
- 5.5. 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.
- 5.6. 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.

5.7. 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.

6. **Garantie limitée et avis de non-responsabilité**

- 6.1. 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 déchargé 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.
- 6.2. 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.
- 6.3. 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.
- 6.4. 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.
- 6.5. 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.
- 6.6. 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.

7. **Exclusion et Limitation de responsabilité**

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, OU AUTREMENT DE PAR OU 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.

8. Licence GNU et autres licences de tierces parties

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.

9. 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'acquiessez 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 que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.
- 10.3 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.

10. 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.

11. Délai de recours.

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.

12. Intégralité de l'accord ; divisibilité ; absence de renoncement.

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.

13. Service clientèle 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

© 1997-2010 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et toute documentation l'accompagnant font l'objet de droits d'auteur et sont protégés par les lois sur la protection des droits d'auteur et les traités internationaux sur les droits d'auteur, ainsi que d'autres lois et traités sur la propriété intellectuelle.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

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, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux États-Unis (Californie). 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, 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. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Kaspersky® Anti-virus, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. 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 noyau Kaspersky Antivirus® : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-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 œuvre 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 utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site officiel de
Kaspersky Lab : <http://www.kaspersky.com/fr>

Encyclopédie de
virus : <http://www.viruslist.com/fr/>

Laboratoire Anti-
Virus : newvirus@kaspersky.com

(uniquement pour l'envoi des objets suspects archivés)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>

(pour les demandes auprès des experts de virus)

INDEX

A

Actions sur les objets.....	41
Algorithme de fonctionnement	
Antivirus Fichiers	40
Analyse	
action sur l'objet sélectionné.....	53
analyse des fichiers composés.....	55
lancement automatique de la tâche ignorée	57, 58
mode de lancement	58
niveau de protection	52
optimisation de l'analyse.....	54
selon la programmation	58
suspension de la tâche.....	57, 58
technologies d'analyse.....	56
type d'objets analysés.....	54
Analyse heuristique	
Antivirus Fichiers	43
Antivirus Fichiers	
algorithme de fonctionnement.....	40
analyse des fichiers composés	44, 45
analyse heuristique.....	43
mode d'analyse.....	45
niveau de protection	41
optimisation de l'analyse.....	44
réaction face à la menace.....	41
statistiques de fonctionnement du composant.....	47
suspension du fonctionnement	46
technologie d'analyse	46
zone de protection	42
Autodéfense du logiciel	82

C

Catégories de menaces identifiées	74
---	----

D

Disque de dépannage	90, 91, 93
Dossier de sauvegarde.....	89

F

Fenêtre principale de l'application	36
---	----

I

Icône dans la zone de notification de la barre des tâches	34
INTERFACE DE L'APPLICATION.....	34

J

Journaux.....	87
---------------	----

K

Kaspersky Lab.....	11
--------------------	----

L

Lancement de la tâche	
-----------------------	--

analyse	50, 58, 59
mise à jour	62, 65, 66
Les fichiers iSwift.....	83

M

Menu contextuel.....	35
Mise à jour	
annulation de la dernière mise à jour.....	63
depuis un répertoire local.....	67
manuelle	62
mode de lancement	65, 66
objet de la mise à jour.....	66
paramètres régionaux.....	64
selon la programmation	66
source de mises à jour.....	63
utilisation du serveur proxy	64

N

Niveau de protection	
Antivirus Fichiers	41
Notifications.....	84

Q

Quarantaine.....	88, 89
Quarantaine et Dossier de sauvegarde	88, 89

R

Réaction face à la menace	
Antivirus Fichiers	41
recherche de virus	53
Restauration des paramètres par défaut	47
Restriction de l'accès à l'application	82

S

Statistiques de fonctionnement du composant	
Antivirus Fichiers	47

Z

Zone de confiance	
applications de confiance.....	75, 78
règles d'exclusion	75
Zone de protection	
Antivirus Fichiers	42