KASPERSKY LAB

Kaspersky® Anti-Virus 6.0 for Windows Servers

MANUEL DE L'UTILISATEUR

KASPERSKY® ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Manuel de l'utilisateur

http://www.kaspersky.fr/

Date d'édition: juillet 2007

Sommaire

CHAPITRE 1. MENACES SUR LA SECURITE INFORMATIQUE

Le développement continu des technologies informatiques et leur introduction dans tous les domaines d'activités humaines s'accompagnent d'une augmentation du nombre de crimes visant les données informatiques.

Les organismes publics et les grandes entreprises attirent les cybercriminels. Ils cherchent à voler des informations confidentielles, à miner les réputations commerciales, à gêner le fonctionnement quotidien et à accéder aux données de ces différentes organisations. Ces diverses actions peuvent entraîner des dommages matériels, financières et moraux conséquents.

Les grandes entreprises ne sont pas les seules exposées au risque. Les particuliers peuvent également devenir des victimes. Les criminels, grâces à divers moyens, peuvent avoir accès aux données personnelles telles que des numéros de compte bancaire, des cartes de crédit ou des mots de passe, ils peuvent rendre un ordinateur totalement inutilisable ou prendre les commandes de celui-ci. Ces ordinateurs pourront être ultérieurement utilisés en tant qu'élement d'un réseau de zombies, à savoir un réseau d'ordinateurs infectés utilisés par les individus mal intentionnés en vue de lancer des attaques contre des serveurs, de récolter des informations confidentielles, de diffuser de nouveaux virus et chevaux de Troie.

Tout le monde est désormais conscient de la valeur des informations et de la nécessité de les protéger. Mais ces données doivent rester accessibles à un groupe défini d'utilisateurs (par exemple, les collègues, les clients ou les partenaires de l'entreprise). Il faut dès lors trouver un moyen de mettre en œuvre un système de protection complexe des données. Ce système doit tenir compte de toutes les sources envisageables de menaces (facteurs humains ou techniques, catastrophes naturelles) et doit reposer sur un ensemble de mesures de protection au plan physique, administratif et technique.

1.1. Sources des menaces

Les menaces qui planent sur les données peuvent émaner d'un individu ou d'un groupe d'individus ou peuvent provenir de phénomènes indépendants de toute intervention humaine. Sur la base de ces informations, les sources de menaces peuvent être scindées en trois groupes :

- **Facteur humain**. Ce groupe de menaces provient d'un individu qui possède un accès autorisé ou non aux données. Les menaces de ce groupe sont :
    - *externes* lorsqu'elles proviennent de cybercriminels, d'escrocs, de partenaires peu scrupuleux ou de structures criminelles.
    - *internes* lorsqu'elles impliquent un membre du personnel de l'entreprise. Les actions des membres de ce groupe peuvent être préméditées ou accidentelles.
- **Facteur technique**. Ce type de menaces recouvre les problèmes techniques : matériel obsolète, mauvaise qualité des logiciels et du matériel utilisés pour traiter l'information. Tout cela entraîne la défaillance de l'équipement et, bien souvent, la perte de données.
- **Catastrophes naturelles**. Ce groupe contient tous les cas de forces majeures sur lesquels l'homme n'a aucun contrôle.

Il faut absolument tenir compte de ces trois catégories lors du développement d'un système de sécurité des données informatiques. Ce manuel traite uniquement de la source directement liée à l'activité de Kaspersky Lab, à savoir les menaces externes créées par un individu.

1.2. Propagation des menaces

Le développement des technologies informatiques et des moyens de communication permet aux individus mal intentionnés de propager les menaces par divers canaux. Nous allons les aborder en détail.

Internet

Le réseau des réseaux se caractérise par le fait qu'il n'appartient à personne et qu'il n'a pas de limites territoriales. Ces deux éléments contribuent pour beaucoup au développement de nombreuses ressources Internet et à l'échange d'informations. A l'heure actuelle, n'importe qui peut accéder à des données sur Internet ou créer son propre site.

Ce sont ces mêmes caractéristiques du réseau Internet qui permettent aux individus mal intentionnés de commettre leurs méfaits sans risquer d'être attrapés et punis.

Les individus mal intentionnés placent des virus et d'autres programmes malveillants sur des sites Web après les avoir « dissimulés » sous l'apparence d'un programme utile et gratuit. De plus, les scripts exécutés automatiquement à l'ouverture de certaines pages Web peuvent lancer des actions malveillantes sur votre ordinateur, y compris la modification de la base de registres système, le vol de données personnelles et l'installation de programmes malveillants.

Grâce aux technologies de réseau, les individus mal intentionnés lancent des attaques sur des serveurs d'entreprise. Le bilan de ces attaques peut être la mise hors service de la source, l'obtention de l'accès total à l'ordinateur et, par conséquent, aux informations qu'il contient ou l'utilisation de la ressource en tant que partie du réseau de zombies.

Intranet

Un intranet est un réseau interne développé afin de gérer les informations au sein de l'entreprise ou un réseau privé. L'intranet est le seul espace du réseau prévu pour la sauvegarde, l'échange et l'accès aux informations de tous les ordinateurs du réseau. Aussi, lorsqu'un ordinateur du réseau est infecté, les ordinateurs restant sont exposés à un risque considérable. Afin d'éviter toute situation similaire, il faut non seulement protéger le périmètre du réseau mais également chaque ordinateur qui en fait partie.

Courrier électronique

La présence d'un client de messagerie électronique sur presque tous les ordinateurs et l'exploitation du carnet d'adresses électroniques pour trouver de nouvelles adresses favorisent énormément la diffusion des programmes malveillants. L'utilisateur d'une machine infectée, sans se douter de quoi que ce soit, envoie des messages infectés à divers destinataires qui, à leur tour, envoient des messages infectés, etc. Il arrive même fréquemment qu'un document infecté se retrouve, suite à une erreur, dans les listes de diffusion commerciales d'une grande société. Dans ce cas, le nombre de victimes ne se chiffrent pas à quelques malheureux mais bien en centaines, voire en milliers de destinataires qui diffuseront, à leur tour, les fichiers infectés à des dizaines de milliers d'autres abonnés.

Média amovibles

Les disques amovibles (disquettes, cédéroms/DVD-ROM, cartes Flash) sont beaucoup utilisés pour conserver des données ou les transmettre.

Lorsque vous exécutez un fichier infecté par le code malicieux depuis un disque amovible, vous pouvez endommager les données sauvegardées sur votre ordinateur ou propager le virus sur d'autres disques de votre ordinateur ou des ordinateurs du réseau.

1.3. Types de menaces

A l'heure actuelle, votre ordinateur peut être endommagé par un nombre assez important de menaces. Cette rubrique se penche plus particulièrement sur les menaces bloquées par Kaspersky Anti-Virus :

Vers

Ce type de programmes malveillants se propage principalement en exploitant les vulnérabilités des systèmes d'exploitation. Les vers doivent leur nom à leur manière de passer d'un ordinateur à l'autre en exploitant le réseau et courrier électronique. Cette technique permet à de nombreux vers de se diffuser à une très grande vitesse.

Ils s'introduisent dans l'ordinateur, recherchent les adresses de réseau des autres machines et y envoient leur copie. De plus, les vers exploitent également les données contenues dans le carnet d'adresses des clients de messagerie. Certains représentants de cette catégorie de programmes malveillants peuvent créer des fichiers de travail sur les disques du système, mais ils peuvent très bien ignorer les ressources de l'ordinateur, à l'exception de la mémoire vive.

Virus

Il s'agit de programmes qui infectent d'autres programmes. Ils insèrent leur code dans celui de l'application ciblée afin de pouvoir prendre les commandes au moment de l'exécution des fichiers infectés. Cette définition simple permet d'identifier l'une des principales actions exécutées par les virus, à s'avoir *l'infection*.

Chevaux de Troie

Il s'agit d'applications qui réalisent diverses opérations sur l'ordinateur infecté à l'insu de l'utilisateur. Cela va de la destruction de données sauvegardées sur le disque dur au vol d'informations confidentielles en passant par le " crash " du système. Ces programmes malicieux ne sont pas des virus au sens traditionnel du terme (en effet, ils ne peuvent infecter les autres applications ou les données). Les chevaux de Troie sont incapables de s'introduire eux-mêmes dans un ordinateur. Au contraire, ils sont diffusés par des personnes mal intentionnées qui les présentent sous les traits d'applications « utiles ». Ceci étant dit, les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnelles.

Ces derniers temps, ce sont les vers qui constituent la majorité des programmes malicieux en circulation. Viennent ensuite, par ordre de diffusion, les virus et les chevaux de Troie. Certains programmes malicieux répondent aux définitions de deux, voire trois, des types mentionnés ci-dessous.

Adwares

Ce code est intégré, à l'insu de l'utilisateur, dans un logiciel afin d'afficher des messages publicitaires. En règle générale, les adwares sont intégrés à des logiciels distribués gratuitement. La publicité s'affiche dans l'espace de travail. Bien souvent, ces programmes recueillent également des données personnelles sur l'utilisateur qu'ils transmettent à leur auteur, ils

modifient divers paramètres du navigateur (page d'accueil et recherche, niveau de sécurité, etc.) et ils créent un trafic sur lequel l'utilisateur n'a aucun contrôle. Tout cela peut entraîner une violation de la politique de sécurité, voire des pertes financières.

Logiciels espion

Ces programmes sont capables de récolter des informations sur un individu particulier ou sur une organisation à son insu. Il n'est pas toujours facile de définir la présence de logiciels espion sur un ordinateur. En règle générale, ces programmes poursuivent un triple objectif :

- Suivre les actions de l'utilisateur sur l'ordinateur ;
- Recueillir des informations sur le contenu du disque dur ; il s'agit bien souvent du balayage de certains répertoires ou de la base de registres système afin de dresser la liste des applications installées sur l'ordinateur ;
- Recueillir des informations sur la qualité de la connexion, les modes de connexion, la vitesse du modem, etc.

Riskwares

Il s'agit d'un programme qui n'a aucune fonction malicieuse mais qui pourrait être exploité par un individu mal intentionné en guise de soutien à un programme malicieux en raison des failles ou des erreurs qu'il contient. Dans certains cas, la présence de tels programmes sur votre ordinateur expose vos données à un certain risque. Cette catégorie de programme contient par exemple certains utilitaires d'administration à distance, des programmes de permutation automatique de la disposition du clavier, des clients IRC, des serveurs FTP, des utilitaires d'arrêt de processus ou de dissimulation de leur fonctionnement.

Une autre catégorie de programmes présentant un risque potentiel, proche des adwares, spywares et riskwares, contient les programmes qui s'intègrent au navigateur et qui réorientent le trafic.

Jokewares

Ces programmes ne vont causer aucun dégât direct à votre ordinateur mais ils s'affichent des messages qui indiquent que des dégâts ont déjà été commis ou qu'ils seront commis sous certaines conditions. Ces programmes signalent souvent une menace inexistante telle que le formatage du disque dur (alors qu'aucun formatage n'est exécuté), découvrent des virus dans des fichiers sains, etc.

Rootkit

Utilitaires qui permettent de dissimuler une activité malveillante. Ils masquent la présence de programmes malveillants afin que ceux-ci ne

soient pas identifiés par les logiciels antivirus. Les rootkits modifient le système d'exploitation de l'ordinateur et remplacent ses fonctions fondamentales afin de dissimuler sa propre présence et les actions exécutées par l'individu mal intentionné sur l'ordinateur infecté.

Autres programmes dangereux

Programmes développés pour mener des attaques par déni de service sur des serveurs distants, pour s'introduire dans d'autres ordinateurs ou qui servent au développement de logiciels malicieux. Cette catégorie reprend les utilitaires d'attaque informatique, les constructeurs de virus, les balayeurs de vulnérabilités, les programmes d'identification de mots de passe, les programmes de pénétration des réseaux ou du système attaqué.

Attention !

Dans ce manuel, le terme « virus » désignera aussi bien les programmes malveillants que les riskwares. Le type de programme malveillant sera précisé au besoin.

CHAPITRE 2. KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVER

Kaspersky Anti-Virus 6.0 représente la nouvelle génération de solution de protection des données.

2.1. Nouveautés de Kaspersky Anti-Virus 6.0 for Windows Servers

Examinons maintenant les nouveautés de Kaspersky Anti-Virus 2006.

Nouveautés au niveau de la protection

- Modification de la technologie de protection des fichiers : il est désormais possible de réduire la charge sur le processeur central et les sous-systèmes disque et d'augmenter la vitesse de l'analyse des fichiers. Ce résultat est obtenu grâce au recours aux technologies iChecker et iSwift. Dans ce mode, l'application empêche l'analyse répétée des fichiers.
- La recherche de virus est désormais soumise à votre utilisation de l'ordinateur. L'analyse est gourmande en temps et en ressources système, mais l'administrateur peut poursuivre son travail. Si l'exécution d'une tâche quelconque requiert plus de ressources système, la recherche de virus sera suspendue jusqu'à la fin de cette tâche. L'analyse reprendra là où elle avait été interrompue.
- L'analyse des secteurs critiques de l'ordinateur, ceux dont l'infection entraînerait des conséquences irréversibles, est reprise dans une tâche séparée. Vous pouvez configurer cette tâche de telle sorte qu'elle soit lancée automatiquement à chaque démarrage du système.
- Elargissement de la fonction de notification de l'utilisateur (cf. point 11.8.1, p. 145) lorsque des événements définis se produisent pendant l'utilisation du logiciel. Vous pouvez choisir le mode de notification pour chaque type d'événement : courrier électronique, avertissement sonore, infobulle, consignation dans le journal.
- Ajout de la technologie d'autodéfense du logiciel, de protection contre l'administration non autorisée à distance, protection des fichiers de

l'application contre les modifications et les accès non autorisés et de protection de l'accès aux paramètres du logiciel grâce à l'instauration d'un mot de passe. Ceci permet d'éviter que des programmes malveillants, des personnes animées de mauvaises intentions ou des utilisateurs non qualifiés ne désactivent la protection.

Nouveautés au niveau de l'interface

- La nouvelle interface de Kaspersky Anti-Virus offre un accès simple et convivial à n'importe quelle fonction de l'application. Vous pouvez également modifier l'apparence du logiciel en utilisant vos propres éléments graphiques et la palette de couleurs.
- Vous recevez toutes les informations relatives au fonctionnement de l'application : Kaspersky Anti-Virus émet des messages sur l'état de la protection, joint des commentaires et des conseils à ses actions et offre une rubrique d'aide détaillée.

Nouveautés au niveau de la mise à jour du programme

- Cette version du logiciel intègre une procédure de mise à jour améliorée : Kaspersky Lab vérifie automatiquement la présence de fichiers de mise à jour sur la source. S'il identifie des actualisations récentes, Kaspersky Anti-Virus les télécharge et les installe.
- Seules les données qui vous manquent sont téléchargées. Cela permet de réduire par 10 le volume téléchargé lors de la mise à jour.
- La mise à jour est réalisée au départ de la source la plus efficace.
- Possibilité de revenir à l'état antérieur à la mise à jour en cas de corruption de fichiers ou d'erreurs lors de la copie des nouvelles signatures de menaces.
- Possibilité de copier les mises à jour dans un répertoire local qui sera accessibles aux autres ordinateurs du réseau afin de réduire le trafic Internet.

2.2. Configuration de la protection offerte par Kaspersky Anti-Virus

La protection offerte par Kaspersky Anti-Virus comprend :

- L'antivirus Fichiers qui contrôle les objets du système de fichiers de l'ordinateur en temps réel.

- Des tâches de recherche de virus (cf. point 2.2.2, p. 17) qui procède à la recherche d'éventuels virus dans l'ordinateur ou dans des fichiers, des répertoires, des disques ou des secteurs particuliers.
- Des services (cf. point 2.2.3, p. 18) qui garantissent le soutien information dans le cadre de l'utilisation du logiciel et qui permettent d'en élargir les fonctions.

2.2.1. Antivirus Fichiers

La protection en temps réel 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 après s'être infiltré via un disque amovible ou une page Internet 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 le serveur et tous les disques connectés. Chaque fichier sollicité sera intercepté par Kaspersky Anti-Virus et soumis à une analyse antivirus pour trouver des virus connus. Chaque requête adressée au fichier est interceptée par Kaspersky Anti-Virus et le logiciel recherche la présence éventuelle de virus connus dans le fichier. L'utilisation ultérieure du fichier sera possible uniquement si le fichier n'est pas infecté ou s'il a été bien réparé. 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) (cf. point 11.2, p. 127)ou mis en quarantaine (cf. point 11.1, p. 123).

2.2.2. Tâches de recherche de virus

En plus de la protection en temps réel à l'aide de l'antivirus Fichiers de tous les canaux par lesquels des programmes malveillants pourraient s'introduire sur votre ordinateur, il est important de procéder régulièrement à une analyse antivirus de l'ordinateur. 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 6.0 for Windows Servers ontient les tâches suivantes axées sur la recherche des virus :

Secteurs critiques

Recherche d'éventuels virus dans tous les secteurs critiques de l'ordinateur. Il s'agit de la mémoire système, des objets utilisés au démarrage du système, des secteurs d'amorçage des disques et des répertoires système *Microsoft Windows*. L'objectif poursuivi est d'identifier rapidement les virus actifs dans le système sans devoir lancer une analyse complète de l'ordinateur.

Mon poste de travail

Recherche d'éventuels virus sur votre ordinateur avec analyse minutieuse de tous les disques connectés, de la mémoire et des fichiers.

Objets de démarrage

Recherche d'éventuels virus dans les objets chargés lors du démarrage du système d'exploitation, ainsi que la mémoire vive et les secteurs d'amorçage des disques.

Il est possible également de créer d'autres tâches de recherche de virus et de programmer leur lancement.

2.2.3. Services du programme

Kaspersky Anti-Virus propose divers services. Ceux-ci visent à maintenir le logiciel à jour, à élargir les possibilités d'utilisation du programme et à fournir de l'aide pendant l'utilisation du programme.

Mise à 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 soit toujours à jour. Le composant *Mise à jour* a été conçu à cette fin. Il assure la mise à jour des signatures des menaces et des modules de Kaspersky Anti-Virus utilisés.

La copie des mises à jour permet de sauvegarder la mise à jour des signatures de menaces et des modules de l'application depuis les serveurs de Kaspersky Lab dans un répertoire local afin de les rendre accessibles aux autres ordinateurs du réseau dans le but de réduire le trafic Internet.

Rapport

Un rapport est généré pendant l'utilisation du programme pour Antivirus Fichiers, chaque tâche de recherche de virus exécutée ou mise à jour. Ce rapport contient les informations relatives aux opérations exécutées et à leurs résultats. Grâce à la fonction *Rapports*, 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 cryptés, 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 faudrait 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 la copie de sauvegarde depuis ce dossier vers son emplacement d'origine ou de la supprimer.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Anti-Virus ont accès au service d'assistance technique. Pour savoir où vous pouvez obtenir cette aide, utilisez la fonction *Assistance technique*.

A l'aide des liens prévus à cet effet, vous pouvez accéder au forum des utilisateurs des logiciels de Kaspersky Lab, consulter la liste des questions fréquemment posées où vous trouverez peut-être la solution à votre problème. De plus, vous pouvez contacter directement le service d'assistance technique en remplissant un formulaire en ligne afin de signaler une erreur ou de transmettre des commentaires sur le fonctionnement du logiciel.

Le service d'assistance technique est accessible en ligne et nos opérateurs sont toujours prêts à répondre à vos questions sur l'utilisation de Kaspersky Anti-Virus par téléphone.

2.3. Configurations matérielle et logicielle

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

Configuration générale :

- 50 Mo d'espace disque disponible.

- Lecteur de cédérom (pour installer Kaspersky Anti-Virus 6.0 à partir du cédérom).
- Microsoft Internet Explorer 5.5 ou suivant (pour la mise à jour des signatures des menaces et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.

Système d'exploitation:

- Microsoft Windows 2000 Server/Advanced Server (Service Pack 4 ou suivant, toutes les mises à jour actuelles).
- Microsoft Windows NT Server 4.0 (Service Pack 6a).
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003 (tous Service Packs, toutes les mises à jour actuelles).
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus® 6.0 chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr – rubrique **Boutique en ligne / Particuliers**).

Le pack logiciel en boite contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés
- La clé de licence reprise dans la distribution ou enregistrée sur une disquette spéciale ou le code d'activation de l'application collé sur l'enveloppe contenant le cédérom d'installation:
- Le manuel de l'utilisateur ;
- Le contrat de licence.

Avant d'ouvrir l'enveloppe contenant le cédérom (ou la disquette), lisez attentivement le contrat de licence.

Si vous achetez Kaspersky Anti-Virus en ligne, vous copiez le logiciel depuis le site de Kasperesky Lab (rubrique **Téléchargement → Télécharger nos**

produit). Les manuels sont disponibles dans la rubrique **Téléchargement → Documentation**.

La clé de licence ou le code d'activation vous sera envoyé par courrier électronique dès confirmation du paiement.

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab, Ltd qui précise les conditions dans lesquelles vous pouvez l'application que vous avez achetée.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les dispositions du contrat, vous pouvez rendre la boîte au distributeur où vous aviez acheté le logiciel contre le remboursement total. Dans ce cas, l'enveloppe contenant le cédérom d'installation ne peut avoir été ouverte.

En effet, l'ouverture de l'enveloppe contenant le cédérom (ou les disquettes) marque votre acceptation du contrat de licence!

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Kaspersky Anti-Virus 6.0 for Windows Servers peut être installé sur un ordinateur de différentes manières :

- Installation locale : installation de l'application sur un ordinateur distinct. Cette installation requiert un accès direct à l'ordinateur en question. L'installation locale peut être réalisée de deux manières :
    - interactive à l'aide de l'assistant d'installation de l'application (cf. point 3.1, p. 23) ; ce mode requiert l'intervention de l'utilisateur au cours de l'installation ;
    - non interactif ; le lancement de l'installation de l'application s'opère via la ligne de commande et applique les paramètres par défaut ; l'intervention de l'utilisateur dans le processus d'installation n'est pas requise (cf. point 3.3, p. 33).
- Installation à distance : installation de l'application sur des 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. « Manuel de déploiement de Kaspersky Administration Kit ») ;
    - Les stratégies de domaines de groupes de Microsoft Windows Server 2000/2003 (cf. point 3.4, p. 34).

Avant d'installer Kaspersky Anti-Virus (y compris en cas d'installation à distance), il est conseillé de quitter toutes les applications ouvertes.

Si la version 5.0 de Kaspersky Anti-Virus est déjà installée sur l'ordinateur, la procédure d'installation se transformera en procédure de mise à jour jusqu'à la version 6.0 avec suppression de la version antérieure (pour de plus amples informations, consultez le point 3.5 à la page 36). La mise à jour d'une version à l'autre dans le cadre de la version 6.0 s'opère sans caractéristiques particulières.

3.1. Procédure d'installation à l'aide de l'Assistant d'installation

Afin d'installer Kaspersky Anti-Virus sur votre ordinateur, vous devez exécuter le fichier d'installation repris sur le CD-ROM d'installation.

> Remarque.
>
> L'installation au départ d'un fichier téléchargé est en tout point identique à l'installation au départ du cédérom.

Le programme d'installation se présente sous la forme d'un Assistant. Chacune de ces boîtes présente différents boutons destinés à contrôler la procédure. En voici une brève description :

- **Suivant :** confirme l'action et passe au point suivant dans le processus d'installation.
- **Précédent** : revient au point précédent dans l'installation.
- **Annuler** interrompt l'installation.
- **Terminer** conclut l'installation du logiciel sur l'ordinateur.

Les pages suivantes expliquent étape par étape l'installation du logiciel.

Etape 1. Vérification de l'existence des conditions minimales requises pour l'installation de Kaspersky Anti-Virus

Avant de procéder à l'installation du logiciel sur votre ordinateur, le système vérifie si le système d'exploitation et les services packs installés suffisent pour Kaspersky Anti-Virus. Le système vérifie également si les programmes requis sont présents et si vous jouissez des privilèges suffisants pour installer l'application.

Un message vous préviendra si une des conditions n'est pas remplie. Il est conseillé d'installer les mises à jour requises à l'aide de **Windows Update** ainsi que les autres programmes nécessaires avant d'installer Kaspersky Anti-Virus.

Etape 2. Fenêtre d'accueil de la procédure d'installation

Si votre système répond aux conditions d'installation, la fenêtre de bienvenue s'affichera dès le lancement du fichier d'installation. Elle contient des renseignements sur le début de l'installation de Kaspersky Anti-Virus.

Cliquez sur **Suivant** pour poursuivre l'installation Cliquez sur **Annuler** pour interrompre l'installation.

Etape 3. Examen du contrat de licence

Cette fenêtre reprend le contrat de licence conclu entre l'utilisateur et Kaspersky Lab. Lisez-le attentivement est si vous acceptez les dispositions, sélectionnez l'option **J'accepte les termes du contrat de licence** puis, cliquez sur **Suivant**. L'installation passera à l'étape suivante.

Pour annuler l'installation, cliquez sur **Annuler**.

Etape 4. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le répertoire dans lequel vous souhaitez installer Kaspersky Anti-Virus. Il s'agit par défaut de :

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

Vous pouvez sélectionner un autre répertoire à l'aide du bouton **Parcourir…** qui ouvre la boîte de dialogue standard de sélection de répertoire ou en saisissant le chemin d'accès au répertoire dans le champ prévu à cet effet.

Si vous saisissez le chemin d'accès complet au répertoire d'installation manuellement, sachez qu'il ne peut pas contenir plus de 200 caractères, ni des caractères spéciaux

Cliquez sur **Suivant** pour poursuivre l'installation.

Etape 5. Utilisation des paramètres de l'application sauvegardés de l'installation antérieure

Cette étape vous permet de définir si vous souhaitez utiliser ou non les paramètres de la protection ou les signatures des menaces qui auraient été sauvegardés sur le serveur au moment de supprimer la version antérieure de Kaspersky Anti-Virus 6.0.

Voyons comment utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Anti-Virus était déjà installée sur le serveur et que, au moment de la supprimer, vous avez conservé les signatures des menaces, vous pourrez les utiliser avec la version que vous installez. Pour

ce faire, cochez la case ☑ **Signatures des menaces**. Les signatures des menaces livrées avec l'application ne seront dès lors pas copiées sur le serveur..

Pour utiliser les paramètres de protection définis dans la version antérieure que vous aviez sauvegardés, cochez la case ☑ **Paramètres de fonctionnement de l'application**.

Etape 6. Choix du type d'installation

Vous devez décider à ce stade du type d'installation. Deux options s'offrent à vous :

Complète. Tous les composants de Kaspersky Anti-Virus seront installés sur votre ordinateur. Pour en savoir plus sur la suite de l'installation, consultez l' Etape 8.

Personnalisée. Dans ce cas, vous pouvez sélectionner les composants que vous souhaitez installer. Pour de plus amples informations, consultez l'Etape 7

Cliquez sur le bouton qui correspond au type d'installation souhaité.

Etape 7. Sélection des composants à installer

Cette étape vous concerne uniquement si vous avez sélectionné l'option **Personnalisée** pour l'installation du logiciel.

Lorsque vous décidez de réaliser une installation personnalisée, vous devez composer la liste des composants de Kaspersky Anti-Virus que vous souhaitez installer. Les composants choisis par défaut sont l'Antivirus Fichiers, la recherche de virus et le connecteur à l'agent d'administration pour l'administration à distance via Kaspersky Administration Kit.

Pour sélectionner un composant à installer, il faut ouvrir le menu d'un clic gauche de la souris sur l'icône située à côté du nom du composant et sélectionner le point **Le composant sera installé sur le disque dur local**. La partie inférieure de cette fenêtre du programme d'installation vous fournira de plus amples informations sur le type de protection assurée par le composant sélectionné et l'espace disque requis.

Si vous ne souhaitez pas installer un composant, sélectionnez l'option **Le composant ne sera pas accessible** dans le menu contextuel.

Une fois que vous aurez opéré votre sélection, cliquez sur **Suivant**. Pour revenir à la liste des composants à installer, cliquez sur **Annuler**.

Etape 8. Recherche d'autres logiciels antivirus éventuellement installés

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

Si de tels programmes existent sur votre ordinateur, leur nom apparaîtra à l'écran. Vous pourrez les supprimer avant de poursuivre l'installation.

En dessus de la liste des logiciels antivirus découverts, vous pourrez décider de les supprimer automatiquement ou manuellement (seuls les logiciels de Kaspersky Lab seront supprimés automatiquement).

Cliquez sur **Suivant** pour poursuivre l'installation.

Etape 9. Préparation finale pour l'installation de l'application

Cette étape constitue la préparation finale pour l'installation du logiciel sur votre ordinateur.

En cas de première installation de Kaspersky Anti-Virus 6.0, il est déconseillé de désélectionner la case **Activer la protection des modules avant le début de l'installation**. Cette protection permet, en cas d'erreur lors de l'installation de l'application, de réaliser correctement la remise à l'état antérieur à l'installation. En cas d'installation répétée, il est conseillé de désélectionner cette case.

En cas d'installation de l'application via Windows Remote Desktop, il est conseillé de désélectionner la case **Activer la protection des modules avant le début de l'installation**. Dans le cas contraire, l'installation pourrait ne pas s'exécuter ou s'exécuter avec des erreurs.

Si vous souhaitez que la liste des exclusions reprenne automatiquement les exclusions recommandées par Microsoft pour les serveurs, cochez la case **Exclure de l'analyse antivirus les domaines recommandés par Microsoft**.

Si vous souhaitez que le chemin d'accès à avp.com soit ajouté après l'installation à la variable %Path%, cochez la case **Ajouter le chemin d'accès à avp.com la variable %Path%.**

Cliquez sur **Suivant** pour poursuivre l'installation.

Attention !

Lors de l'installation des composants de Kaspersky Anti-Virus chargés d'intercepter le trafic de réseau, les connexions de réseau établies sont interrompues. La majorité de ces connexions seront rétablies après un certain temps.

Etape 10. Fin de la procédure d'installation

La fenêtre **Fin de l'installation** contient les informations relatives à la fin de l'installation de Kaspersky Anti-Virus sur l'ordinateur.

Afin de lancer l'Assistant de configuration initiale, cliquez sur **Suivant** (cf. point 3.2, page 27).

Lorsque le redémarrage de l'ordinateur s'impose pour terminer l'installation, un message le signalera.

3.2. Assistant de configuration initiale

L'Assistant de configuration de Kaspersky Anti-Virus 2006 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 Microsoft Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Si vous interrompez la configuration initiale en fermant la fenêtre de l'Assistant, l'application ne fonctionnera pas. Chaque lancement de l'application s'appliquera du lancement de l'Assistant de configuration initiale tant que la configuration ne sera pas complètement réalisée.

3.2.1. Utilisation des objets sauvegardés de la version 5.0

Cette fenêtre de l'Assistant s'affiche lors de l'installation sur la version 5.0 de Kaspersky Anti-Virus. Vous devrez choisir les données utilisées par la version

5.0 qui devront être transmises dans la version 6.0. 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 6.0, cochez les cases adéquates

3.2.2. Activation du logiciel

Avant d'activer l'application, assurez-vous que la date système de l'ordinateur correspond bien à la date et à l'heure réelles.

La procédure d'activation du logiciel consiste à installer la clé que Kaspersky Anti-Virus utilisera pour confirmer la présence de droits d'utilisation de l'application et leur durée de validité.

La clé de licence contient les informations de service indispensables pour assurer le parfait fonctionnement du logiciel ainsi que des renseignements complémentaires :

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

3.2.2.1. Sélection du mode d'activation du programme

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

- **Activer à l'aide du code d'activation**. Sélectionnez cette option si vous avez acheté une version commerciale de l'application et que vous avez reçu le code d'activation. Vous recevrez, sur la base de ce code, la clé de licence qui vous donnera accès à l'ensemble des fonctions de l'application pendant toute la durée de validité de la licence.
- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation de l'application avant de décider d'acheter la version commerciale. Vous recevrez une clé de licence gratuite dont la durée de validité sera limitée par la licence associée à la version d'évaluation de l'application.
- **Utiliser la clé de licence obtenue antérieurement.** Activez l'application à l'aide du fichier de clé de licence pour Kaspersky Anti-Virus 6.0.
- **Activer le logiciel plus tard**. Sélectionnez cette option si vous êtes en attente de votre licence commerciale. L'activation du logiciel sera reportée à

plus tard. Ce logiciel Kaspersky sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser les signatures des menaces une fois que vous aurez activé le logiciel au moyen d'un des trois points précédents).

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 (cf. point 10.4.3, p. 117) 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 (cf. point 11.5, p. 139) au départ de l'interface de l'application ou en vous connectant à Internet depuis un autre ordinateur afin d'obtenir la clé de licence associée au code d'activation après vous être enregistré sur le site Web du service d'assistance technique de Kaspersky Lab.

3.2.2.2. Saisie du code d'activation

L'activation de l'application requiert la saisie du code d'activation. En cas d'achat de l'application via Internet, le code d'activation est envoyé par courrier électronique. Si vous avez acheté l'application dans un magasin traditionnel, le code d'activation est repris sur l'enveloppe contenant le disque d'installation.

Le code d'activation est une séquence de quatre groupes de 5 caractères séparés par des traits d'union sans espace. Par exemple 11AA1-11AAA-1AA11-1A111. Le code doit être saisi dans l'alphabet latin.

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 de la clé. Dans ce cas, vous pourrez obtenir une nouvelle clé de licence sur la base des coordonnées que vous aurez fournies.

3.2.2.3. Réception de la clé de licence

L'Assistant de configuration établit une connexion avec les serveurs de Kaspersky Lab sur Internet et envoie vos données d'enregistrement (code d'activation, coordonnées) qui seront vérifiées sur le serveur.

Si le code d'activation est correct, l'Assistant obtiendra la clé du fichier de licence. Si vous installez une version d'évaluation de l'application, l'Assistant de configuration recevra le fichier de clé d'évaluation sans code d'activation.

Le fichier obtenu sera installé automatiquement pour permettre le fonctionnement de l'application et vous verrez la boîte de dialogue de fin de l'activation avec les détails relatifs à la licence.

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

3.2.2.4. Sélection du fichier de clé de licence

Si vous possédez un fichier de clé de licence valide pour ce logiciel , cette boîte de dialogue vous invitera à l'installer. Pour ce faire, cliquez sur **Parcourir** et dans la boîte de dialogue standard de sélection des fichiers, sélectionnez le fichier de clé (format du nom de fichier : xxxxxxx.*key*).

Une fois la clé installée, les informations relatives à la licence seront reprises dans la partie inférieure de la fenêtre : nom du détenteur, numéro de licence, type (commerciale, test bêta, évaluation, etc.) et fin de validité de la clé.

3.2.2.5. Fin de l'activation du logiciel

L'Assistant de configuration vous informe de la réussite de l'activation du logiciel. Il fournit également des renseignements relatifs à la licence installée : nom du détenteur, numéro de licence, type (commerciale, évaluation, etc.) et date de fin de validité de la clé.

3.2.3. Configuration de la mise à jour

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

- **Automatique**. Kaspersky Anti-Virus vérifie selon la fréquence définie la présence de fichiers de mise à jour sur la source de la mise à jour. L'intervalle peut être réduit en cas d'épidémie de virus ou augmenté lorsque la situation est calme. Si Kaspersky Anti-Virus identifie de nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est activé 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**. 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 de la mise à jour (sélectionner les paramètres de réseau, sélectionner la ressource au départ de laquelle la mise à jour sera réalisée, configurer le lancement de la mise à jour au nom d'un compte particulier et activer le service de copie des mises à jour dans un répertoire local), cliquez sur **Configuration**.

3.2.4. 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 votre 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 des objets de démarrage

Par défaut, l'analyse des objets de démarrage s'opère automatiquement lors du lancement de Kaspersky Anti-Virus. Vous pouvez modifier les paramètres de la programmation dans la fenêtre qui s'ouvre à l'aide du bouton **Modifier**.

Analyse des secteurs critiques

Pour lancer automatiquement l'analyse des secteurs critique de l'ordinateur (mémoire système, objets de démarrage, secteurs d'amorçage, répertoires système Microsoft Windows Server), cochez la case dans le bloc correspondant. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.

Le lancement automatique de cette tâche est désactivé par défaut.

Analyse complète de l'ordinateur

Pour lancer automatiquement l'analyse complète de l'ordinateur, cochez la case dans le bloc correspondant. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.

Le lancement programmé de cette tâche est désactivé par défaut. Nous vous conseillons toutefois de lancer l'analyse complète du serveur directement après l'installation du logiciel.

3.2.5. Restriction de l'accès au logiciel

Dans la mesure où votre ordinateur peut être utilisé par différentes personnes vu que certains programmes malveillants peuvent désactiver la protection, vous avez la possibilité de définir un mot de passe pour limiter l'accès à Kaspersky Anti-Virus. Le mot de passe protège le logiciel contre les tentatives de désactivation non autorisée ou de modification des paramètres de la protection.

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

Indiquez ensuite les tâches qui seront concernées :

- ◉ **Toutes les opérations (sauf les notifications de danger).** Le mot de passe est nécessaire pour lancer n'importe quelle action du logiciel à l'exception de la manipulation des messages relatifs à la découverte d'objets dangereux.
- ◉ **Sélectionnez les actions protégées par un mot de passe:**
  - ☑ **Enregistrement des paramètres de fonctionnement de l'application** : le mot de passe est requis lorsque l'utilisateur tente d'enregistrer les modifications apportées aux paramètres du logiciel.
  - ☑ **Quitter le logiciel** : le mot de passe est requis pour quitter le logiciel.
  - ☑ **Arrêt/pause des composants de la protection et des tâches de recherche de virus** : le mot de passe est requis pour suspendre ou arrêter n'importe quel composant ou n'importe quelle tâche liée à la recherche de virus.

3.2.6. 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 l'application. Vous pouvez lancer directement l'application en cochant la case ☑ **Lancer l'application**.

En cas d'erreur lors de l'installation (exemple : découverte de versions incompatibles d'autres logiciels antivirus) vous devrez peut-être redémarrer l'ordinateur.

3.3. Procédure d'installation de l'application via la ligne de commande

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

```
msiexec /i <nom_du_paquetage>
```

Cette action entraîne le lancement de l'assistant d'installation (cf. point 3.1, p. 23). Il faut absolument redémarrer l'ordinateur après l'installation.

Pour installer l'application en mode non-interactif (sans l'aide de l'Assistant d'installation), saisissez :

```
msiexec /i <nom_du_paquetage> /qn
```

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

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

N'oubliez pas que le redémarrage automatique de l'ordinateur peut être réalisée uniquement en mode non interactif (avec l'argument /qn).

Pour installer l'application avec la définition d'un mot de passe qui confirme le privilège de suppression de l'application, saisissez :

`msiexec /i <nom_du_paquetage> KLUNINSTPASSWD=******` : lors de l'installation de l'application en mode interactif ;

`msiexec /i <nom_du_paquetage> KLUNINSTPASSWD=****** /qn` : lors de l'installation de l'application en mode non interactif sans redémarrage de l'ordinateur ;

`msiexec /i <nom_du_paquetage> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn` : lors de l'installation de l'application en mode `non interactif` avec redémarrage de l'ordinateur.

L'installation de Kaspersky Anti-Virus en mode non interactif prend en charge la lecture du fichier *setup.ini*, qui contient les paramètres généraux d'installation de l'application (cf. point A.4, p. 197), le fichier de configuration *install.cfg* (cf. point 13.7, p. 185), ainsi que la clé de licence. N'oubliez pas que ces fichiers doivent se trouver dans le même répertoire que le fichier d'installation de Kaspersky Anti-Virus.

3.4. Installation via l'éditeur d'objet de stratégie de groupe

Cette option est disponible uniquement sur les ordinateurs tournant sous Microsoft Windows 2000 Server et suivant.

Grâce à **l'éditeur d'objet de stratégie de groupe**, vous pouvez installer, actualiser et supprimer Kaspersky Anti-Virus sur les postes de travail de l'entreprise qui font partie du domaine sans devoir utiliser Kaspersky Administration Kit.

3.4.1. Installation de l'application

Pour installer Kaspersky Anti-Virus:

1. Créez un répertoire de réseau partagé sur l'ordinateur faisant office de contrôleur du domaine et placez-y le fichier d'installation de Kaspersky Anti-Virus au format *.msi*.

   Vous pouvez également ajouter le fichier *setup.ini* qui contient la liste des paramètres d'installation de Kaspersky Anti-Virus (la liste détaillée des paramètres de ce fichier est reprise au point A.4 à la page 197), le fichier de configuration *install.cfg* (cf . point 13.7, p. 185) ainsi que la clé.

2. Ouvrez **l'éditeur d'objet de stratégie de groupe** via la console MMC standard (l'utilisation de l'éditeur est expliquée dans les rubriques d'aide de Microsoft Windows Server).

3. Créez un nouveau paquet. Pour ce faire, sélectionnez dans l'arborescence **Objet de stratégie de groupe**/ **Configuration de l'ordinateur** (Computer Configuration)/ **Paramètres du logiciel** (Software Settings)/ **Installation du programme** (Software installation) puis, utilisez la commande **Nouveau**/ **Paquet** dans le menu contextuel.

   Indiquez, dans la fenêtre qui s'ouvre, le chemin d'accès au répertoire de réseau partagé contenant le fichier d'installation de Kaspersky Anti-Virus (cf. point 1). Dans la boîte de dialogue **Déploiement du programme** (Select Deployment Method), sélectionnez le paramètre **Appliquer** (Assign) et cliquez sur **OK**.

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

3.4.2. Mise à jour de l'application

Pour actualiser Kaspersky Anti-Virus :

1. Placez le fichier contenant la mise à jour de Kaspersky Anti-Virus, au format *.msi*, dans le répertoire de réseau partagé.
2. Ouvrez **l'éditeur d'objet de stratégie de groupe** et créez un nouveau paquet comme décrit ci-dessus.
3. Sélectionnez le nouveau paquet dans la liste et choisissez la commande **Propriétés** (Properties) dans le menu contextuel. Dans la fenêtre des propriétés du paquet, sélectionnez l'onglet **Mises à jour** (Upgrades) et indiquez le paquet contenant le fichier d'installation de la version antérieure de Kaspersky Anti-Virus. Pour installer la version actualisée de Kaspersky Anti-Virus tout en préservant les paramètres de la protection, sélectionnez l'option d'installation sur un paquetage existant.

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

N'oubliez pas que les ordinateurs tournant sous Microsoft Windows 2000 Server ne sont pas compatibles avec la mise à jour de Kaspersky Anti-Virus via l'éditeur d'objet de stratégie de groupe.

3.4.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

1. Ouvrez l'**éditeur d'objet de stratégie de groupe**.
2. Sélectionnez, dans l'arborescence de la console, **Objet_de_stratégie_de_groupe/ Configuration de l'ordinateur** (Computer Configuration)/ **Paramètres du logiciel** (Software Settings)/ **Installation du logiciel** (Software installation).

   Sélectionnez le paquet Kaspersky Anti-Virus dans la liste, ouvrez le menu contextuel et exécutez la commande **Toutes les tâches** (All Tasks)/ **Supprimer** (Remove).

   Dans la boîte de dialogue **Suppression de l'application** (Remove Software), sélectionnez **Suppression immédiate de cette application de l'ordinateur de tous les utilisateurs** (Immediately uninstall the software from users and computers) afin que Kaspersky Anti-Virus soit supprimer lors du prochain redémarrage.

3.5. Mise à niveau de la version 5.0 à la version 6.0

Si vous avez installé Kaspersky Anti-Virus 5.0 for Windows File Servers, vous pouvez réaliser la mise à niveau à la version 6.0.

Une fois que vous aurez lancé le programme d'installation de Kaspersky Anti-Virus 6.0 vous serez invité en premier lieu à supprimer l'installation de la version 5.0. Une fois cette version supprimée, vous devrez redémarrer l'ordinateur puis vous pourrez commencer l'installation de la version 6.0.

Attention !

Si vous installez Kaspersky Anti-Virus 6.0 for Windows Servers depuis un répertoire de réseau protégé par un mot de passe dans la version antérieure, il faudra faire attention à la particularité suivante. Une fois la suppression de la version 5.0 et le redémarrage de l'ordinateur réalisés, le programme d'installation ne permet pas d'accéder au répertoire de réseau qui contient la distribution de l'application. Pour cette raison, l'installation du logiciel est interrompue. Afin de pouvoir installer correctement l'application, lancez l'installation uniquement depuis une ressource locale.

CHAPITRE 4. INTERFACE DU LOGICIEL

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

- L'icône de la barre des tâches (cf. point 4.1, p. 37);
- Le menu contextuel (cf. point 4.2, p. 38);
- La fenêtre principale (cf. point 4.3, p. 39);
- Fenêtre de configuration des paramètres du logiciel (cf. point 4.4, p. 42).

4.1. Icône de la barre des tâches

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 reflète l'état de la protection et illustre également diverses tâches fondamentales exécutées par l'application.

Si l'icône est activée  (en couleur), cela signifie que la protection de l'ordinateur est activée. Si l'icône n'est pas activée  (noir et blanc) cela signifie que la protection en temps réel n'est pas activée.

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 signatures des menaces et des modules logiciels de Kaspersky Anti-Virus est en cours.
	Une erreur s'est produite dans un des composants de Kaspersky Anti-Virus.

L'icône donne également accès aux éléments principaux de l'interface du logiciel : le menu contextuel (cf. point 4.2, p. 38) et la fenêtre principale (cf. point 4.3, p. 39);

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

Pour ouvrir la fenêtre principale de Kaspersky Anti-Virus à l'onglet **Protection** (c'est l'onglet de départ proposé par défaut), double-cliquez avec le bouton gauche de la souris sur l'icône du programme. Si vous cliquez une seule fois, vous ouvrirez la fenêtre principale à la rubrique active lorsque vous avez quitté le programme la dernière fois.

4.2. Menu contextuel

Le menu contextuel (cf. Illustration 1) permet d'exécuter toutes les tâches principales liées à la protection.

Illustration 1. Menu contextuel

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

Analyser du Poste de travail : lance l'analyse complète de l'ordinateur à la recherche d'éventuels objets malveillants. Les objets de tous les disques, y compris sur les disques amovibles, seront analysés.

Recherche de virus : passe à la sélection des objets et à la recherche d'éventuels virus parmi eux. Par défaut, la liste comprend toute une série d'objets comme la mémoire système, les objets de démarrage, les bases de messagerie, tous les disques de l'ordinateur, etc. Vous pouvez également compléter la liste, sélectionner des objets à analyser et lancer la recherche d'éventuels virus.

Mise à jour : lance la mise à jour des modules de l'application et des signatures de menaces de Kaspersky Anti-Virus et les installe sur l'ordinateur.

Activation : passe à l'activation du logiciel. Pour obtenir le statut d'utilisateur enregistré, qui donne droit à toutes les fonctions de l'application et au service d'assistance technique, il faut obligatoirement activer votre version de Kaspersky Anti-Virus. Ce point apparaît uniquement si le programme n'est pas activé.

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 (cf. point 4.3, p. 39).

Suspension de la protection/Activation de la protection : désactive temporairement/active le fonctionnement de l'Antivirus Fichiers (cf. point 2.2.1, p. 17). Ce point du menu n'a aucune influence sur la mise à jour de l'application ou sur l'exécution de la recherche de virus.

Quitter : quitte Kaspersky Anti-Virus (si ce point du menu est sélectionné, l'application sera déchargée de la mémoire vive de l'ordinateur).

Si une tâche quelconque de recherche de virus 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.

4.3. Fenêtre principale du logiciel

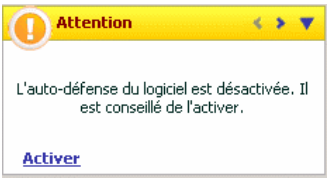
La fenêtre principale (cf. Illustration 2) de Kaspersky Anti-Virus est constituée de deux panneaux :

Illustration 2. Fenêtre principale de Kaspersky Anti-Virus

- Le panneau de gauche est réservé à la *navigation*. Il permet de passer rapidement et simplement à n'importe quel composant, de lancer les recherches de virus et les mises à jour et d'accéder aux services du logiciel;
- Le panneau de droite est à caractère *informatif* : il contient les informations relatives au composant sélectionné dans le panneau de gauche, permet d'accéder à la configuration de chacun d'entre eux, propose les instruments pour l'exécution de la recherche des virus, la manipulation des fichiers en quarantaine et des copies de réserve, la gestion des clés de licence, etc.

Dès que vous avez sélectionné une section dans le panneau de gauche, le panneau de droite reprendra toutes les informations relatives au composant .

Examinons en détails les éléments du panneau de navigation de la fenêtre principale.

Section du panneau de navigation de la fenêtre principale	**Fonction**
La tâche principale de cette fenêtre est de vous informer sur l'état de la protection de votre ordinateur. La section **Protection** est prévue précisément à cette fin. 	Pour consulter les informations générales sur le fonctionnement de Kaspersky Anti-Virus, les statistiques de fonctionnement du logiciel, vérifier le bon fonctionnement du système, sélectionnez la section **Protection** dans le panneau de navigation.
La section **Analyser** est prévue pour la recherche d'objets malveillants. 	Cette section contient la liste des objets que vous pouvez soumettre individuellement à l'analyse antivirus. Les tâches qui, selon les experts de Kaspersky Lab, vous seront les plus utiles sont reprises dans cette section. Il s'agit de la recherche de virus dans les secteurs critiques, parmi les objets de démarrage ainsi que l'analyse complète de l'ordinateur.
La section **Services** contient les fonctions complémentaires de Kaspersky Anti-Virus. 	Vous pouvez passer à la mise à jour du logiciel, à la consultation des rapports relatifs aux tâches ou composants en cours ou arrêtés, à la manipulation des objets en quarantaine ou des copies de sauvegarde ou à la fenêtre d'administration des clés de licence.
La section **Commentaires et conseils** vous accompagne tout au long de l'utilisation de l'application. 	Cette section vous offrira toujours des conseils pour renforcer la protection de l'ordinateur. C'est ici que vous trouverez également les commentaires sur le fonctionnement actuel de l'application et sur ces paramètres. Grâce aux liens repris dans cette section, vous pouvez accéder directement à l'exécution de l'action recommandée dans un cas concret ou en savoir plus sur les informations.

Chaque élément du panneau de navigation est doté d'un menu contextuel spécial. Ainsi, pour l'Antivirus Fichiers et les services, ce menu contient des points qui permettent d'accéder rapidement aux paramètres, à l'administration et à la consultation des rapports. Le menu contextuel de la recherche de virus et de la mise à jour prévoit un point supplémentaire qui vous permet de personnaliser la tâche sélectionnée.

Il est possible également de modifier l'apparence de la fenêtre principale de l'application

4.4. Fenêtre de configuration des paramètres du logiciel

La fenêtre de configuration de Kaspersky Anti-Virus peut être ouverte depuis la fenêtre principale (cf. point 4.3, p. 39). Pour ce faire, cliquez sur le lien Configuration dans la partie supérieure.

La fenêtre de configuration (cf. Illustration 3) ressemble à la fenêtre principale :

- La partie gauche offre un accès simple et rapide à la configuration de l'Antivirus Fichiers, des tâches liées à la recherche de virus, aux mises à jour ainsi qu'à la configuration des services du logiciel;
- La partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionné dans la partie gauche.

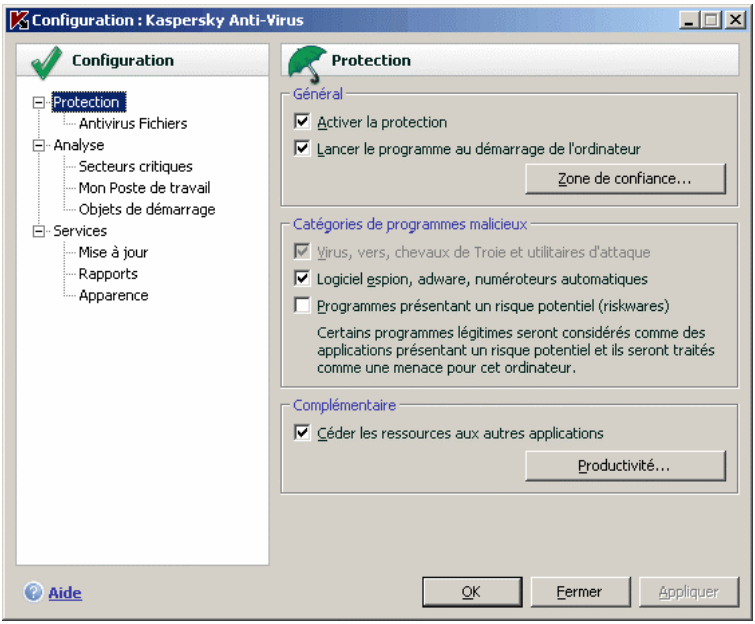


Illustration 3. Fenêtre de configuration de Kaspersky Anti-Virus

Lorsque vous sélectionnez dans la partie gauche de la fenêtre de configuration une section, un composant ou une tâche quelconque, la partie droite affiche les paramètres fondamentaux de l'élément sélectionné. Afin passer à la configuration détaillée de certains paramètres, vous pourrez ouvrir une boîte de dialogue pour la configuration de deuxième ou de troisième niveau. Une description détaillée des paramètres est offerte dans les sections correspondantes de l'aide électronique.

CHAPITRE 5. 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 (cf. point 3.2, p. 27). Cet Assistant démarre à la fin de l'installation du logiciel. En suivant les indications de l'Assistant, vous pourrez activer le programme, configurer la mise à jour et le lancement de la recherche de virus, 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 (cf. point 5.1, p. 44) pour s'assurer que Kaspersky Anti-Virus offre le niveau de sécurité souhaité.
- Mettre à jour le logiciel (au cas où cela n'aurait pas été réalisé à l'aide de l'Assistant de configuration ou automatiquement après l'installation du logiciel) (cf. point 5.5, p. 52).
- Analyser l'ordinateur (cf. point 5.2, p. 50).

5.1. Etat de la protection de l'ordinateur

Toutes les informations relatives à la protection de votre ordinateur sont reprises dans la section **Protection** de la fenêtre principale de Kaspersky Anti-Virus. Vous y trouverez *l'état actuel de la protection* de l'ordinateur ainsi que des *statistiques générales* sur le fonctionnement du logiciel.

L'**Etat de la protection de l'ordinateur** illustre l'état actuel de la protection de votre ordinateur à l'aide d'indices spéciaux (cf. point 5.1.1, p. 45). Les statistiques (cf. point 5.1.2, p. 48) affichent les résultats du travail actuel du logiciel.

5.1.1. Indices de protection

L'état de la protection est défini par trois indices qui illustrent le niveau de protection de votre ordinateur à ce moment et qui indiquent tout problème au niveau de la configuration et du fonctionnement du logiciel.

L'importance de l'événement signalé par l'indice peut prendre l'une des trois valeurs suivantes :

– *indice informatif* : il signale que la protection de l'ordinateur est au niveau requis et qu'il n'y a aucun problème au niveau de la configuration du logiciel ou du fonctionnement des composants.

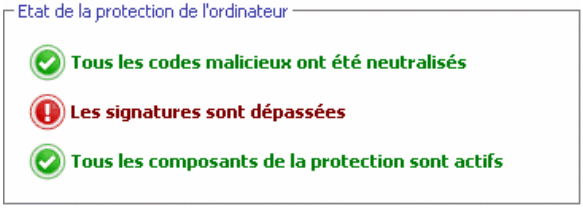


Illustration 4. Indices indiquant l'état de protection de l'ordinateur

– *l'indice attire votre attention sur quelques écarts* dans le fonctionnement de Kaspersky Anti-Virus par rapport au mode recommandé, ce qui peut avoir une incidence sur la protection de l'information. Veuillez prêter attention aux recommandations des experts de Kaspersky Lab reprises dans la section Commentaires et conseils de la fenêtre principale du logiciel.

– *l'indice signale une situation critique* au niveau de la protection de votre ordinateur. Suivez scrupuleusement les recommandations fournies dans la section Commentaires et conseils de la fenêtre principale du logiciel. Elles visent toutes à renforcer la protection de votre ordinateur. Les actions recommandées apparaissent sous la forme d'un lien.

Voici une présentation détaillée des indices de protection et des situations dans laquelle ils apparaissent.

Le premier indice illustre une situation impliquant la présence d'objets malveillants sur l'ordinateur. L'indice prend une des valeurs suivantes :

	*Aucun code malicieux découvert*
	Tous les objets malveillants ont été neutralisés Kaspersky Anti-Virus a réparé tous les objets infectés et supprimés ceux qu'il n'a pas pu réparer.
	*Des objets malveillants ont été découverts* Votre ordinateur est actuellement exposé à un risque d'infection. Kaspersky Anti-Virus a découvert des objets malveillants qu'il faut absolument neutraliser. Pour ce faire, cliquez sur Réparer tous. Le lien Détails vous permet d'obtenir de plus amples informations sur les objets malveillants.

Le deuxième indice illustre le degré d'actualité de la protection de l'ordinateur à ce moment. L'indice prend une des valeurs suivantes :

	*Les signatures ont été diffusées (date, heure)* Le logiciel n'a pas besoin d'être mis à jour. Toutes les bases utilisées par Kaspersky Anti-Virus contiennent les informations les plus récentes pour la protection de l'ordinateur.
	*Les signatures ne sont plus d'actualité* Les modules de l'application et les bases de données de Kaspersky Anti-Virus n'ont pas été actualisées depuis quelques jours. Vous risquez d'infecter votre ordinateur avec de nouveaux programmes malveillants ou d'être soumis aux nouvelles attaques apparues depuis la dernière mise à jour de l'application. Il est vivement recommandé de mettre à jour Kaspersky Anti-Virus. Pour ce faire, cliquez sur Mettre à jour.
	Les signatures sont partiellement corrompues Les fichiers des signatures de menaces sont partiellement corrompus. Il est conseillé dans ce cas de lancer à nouveau la mise à jour de l'application. Si l'erreur se reproduti après la nouvelle mise à jour, contactez le service d'assistance technique de Kaspersky Lab.

	Le redémarrage de l'ordinateur est indispensable La mise à jour correcte du logiciel requiert le redémarrage du système. Enregistrez et fermez tous les fichiers avec lesquels vous travailliez et cliquez sur Redémarrer l'ordinateur.
	La mise à jour automatique est inactive Le service de mise à jour des signatures de menaces et des modules de l'application est désactivé. Il est conseillé d'activer la mise à jour pour maintenir l'actualité de la protection.
	*Les signatures sont dépassées* Il y a longtemps que Kaspersky Anti-Virus n'a plus été mis à jour. Vous exposez les données de votre ordinateur à un grand risque. Il faut mettre le logiciel à jour le plus vite possible. Pour ce faire, cliquez sur Mettre à jour.
	Les signatures sont corrompues Les fichiers des signatures des menaces sont corrompus. Il est conseillé de lancer à nouveau la mise à jour. Si l'erreur se reproduit, contactez le service d'assistance technique de Kaspersky Lab.

Le troisième indice indique le degré d'utilisation des possibilités du logiciel. L'indice prend une des valeurs suivantes :

	*Tous les composants de la protection sont actifs* Tous les vecteurs de propagation des programmes malveillants sont protégés par Kaspersky Anti-Virus Suite.
	La protection n'est pas définie Lors de l'installation de Kaspersky Anti-Virus, aucun des composants de la protection en temps réel n'a été installé. Le présent mode autorise unique la recherche d'éventuels virus dans les objets. Pour garantir la protection maximale de l'ordinateur, il est conseillé d'installer les composants de la protection.
	*Tous les composants de la protection sont inactifs* La protection de l'ordinateur est complètement désactivée. Aucun des composants de la protection ne fonctionne. Pour rétablir le fonctionnement du composant, sélectionnez l'élément **Activation**

	de la protection dans le menu contextuel qui s'ouvre lorsque vous cliquez sur l'icône de l'application dans la barre des tâches.
	Tous les composants de la protection sont inactifs La protection de l'ordinateur est complètement désactivée. Aucun des composants de la protection ne fonctionne. Pour rétablir le fonctionnement des composants, sélectionnez l'élément **Activation de la protection** dans le menu contextuel qui s'ouvre lorsque vous cliquez sur l'icône de l'application dans la barre des tâches.
	*Certains composants de la protection ne sont pas corrects* Le fonctionnement du composant de la protection de Kaspersky Anti-Virus s'est soldé par un échec. Il est conseillé dans ce cas d'activer le composant ou de redémarrer l'ordinateur (l'enregistrement des pilotes du composant après l'application d'une mise à jour s'impose peut-être).

5.1.2. Etat d'un composant particulier de Kaspersky Anti-Virus

Pour savoir comment Kaspersky Anti-Virus protège le système de fichiers, pour suivre l'exécution de la recherche de virus ou de la mise à jour des signatures des menaces, il suffit d'ouvrir la section adéquate dans la fenêtre principale du logiciel.

Ainsi, pour consulter l'état actuel de la protection des fichiers, sélectionnez **Antivirus Fichiers** dans la partie gauche de la fenêtre du programme. La partie droite de la fenêtre reprendra des informations de synthèse sur le fonctionnement du composant.

Chaque composant est accompagné d'une **barre d'état**, d'une section **Etat** (**Configuration** pour la recherche de virus et les mises à jour) et d'une section **Statistiques**.

Examinons la *barre d'état* d' Antivirus Fichiers :

- *Antivirus Fichiers : en exécution*: la protection des fichiers est assurée selon les paramètres du niveau sélectionné. (cf. point 7.1, p. 75).

- *Antivirus Fichiers : pause* : l'antivirus de fichiers a été désactivé pour un temps déterminé. Le composant sera activé automatiquement une fois ce laps de temps écoulé ou après le redémarrage du logiciel. Vous pouvez activer vous-même la protection des fichiers. Pour ce faire, cliquez sur dans la barre d'état.

- *Antivirus Fichiers* : *inactif*. L'utilisateur a arrêté le composant. Vous pouvez activer la protection des fichiers. Pour ce faire, cliquez sur dans la barre d'état.

- *Antivirus Fichiers : ne fonctionne pas*. La protection des fichiers est inaccessible pour une raison quelconque.

- *Antivirus Fichiers : échec*. Le composant s'est arrêté suite à un échec.

  Si un erreur se produit durant le fonctionnement du composant, essayez de le lancer à nouveau. Si cette tentative se solde également sur un échec, consultez le rapport sur le fonctionnement du composant. Vous y trouverez peut-être la cause de l'erreur. Si vous ne parvenez pas à résoudre vous-même ce problème, enregistrez le rapport sur fonctionnement du composant dans un fichier à l'aide du bouton **Actions → Enregistrer sous** et contactez le Service d'assistance technique de Kaspersky Lab

Les paramètres de fonctionnement du composant sont repris dans le groupe **Etat**:

- *Antivirus Fichiers* : état actuel du composant (fonction, arrêt, suspension, etc.).

- *Niveau de protection* : sélection de paramètres de fonctionnement du composant qui définissent la façon dont l'application assure la lutte contre les virus. Par défaut, c'est le niveau **Recommandé** qui est utilisé. A ce niveau, seuls les objets du système de fichiers qui peuvent être infectés sont analysés. Par exemple, les fichiers exécutables (exe).

- *L'action* qui sera exécutée en cas de découverte d'un objet malveillant.

La section **Etat** n'est pas proposée pour les tâches liées à la recherche de virus et à la mise à jour. Le niveau de protection appliqué contre les programmes dangereux lors de l'analyse et le mode de lancement de la mise à jour figure dans le bloc **Configuration**.

Le bloc **Statistiques** contient les résultats du fonctionnement du composant de la protection, de la mise à jour ou de la recherche de virus.

5.1.3. Statistiques

Les statistiques du fonctionnement de l'application sont reprises dans le groupe **Statistique** de la section **Protection** de la fenêtre principale de l'application (cf. Illustration 5). Elles fournissent des informations générales sur la protection de l'ordinateur, depuis l'installation de Kaspersky Anti-Virus.

Illustration 5. Bloc des statistiques générales sur le fonctionnement du programme

Un clic du bouton gauche de la souris dans n'importe quel endroit du bloc ouvre un rapport détaillé. Les différents onglets comprennent :

- des informations sur les objets découverts (cf. point 11.3.2, p. 134) et le statut qui leur a été attribué;
- le journal des événements (cf. point 11.3.3, p. 135);
- des statistiques générales sur l'analyse de l'ordinateur (cf. point 11.3.4, p. 136);
- les paramètres de fonctionnement du logiciel (cf. point 11.3.5, p. 137).

5.2. Recherche d'éventuels virus

Une fois installée, l'application vous signalera à l'aide de messages affichés dans la partie inférieure gauche de la fenêtre que l'analyse du serveur n'a pas encore été réalisée et qu'il est grand temps de le faire.

Kaspersky Anti-Virus possède une tâche de recherche de virus sur l'ordinateur. Elle se trouve dans la section **Analyser** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Mon poste de travail**, vous pouvez consulter les statistiques de la dernière analyse et les paramètres de la tâche : le niveau de sécurité sélectionné et l'action exécutée sur les objets dangereux.

Pour rechercher la présence d'éventuels objets malveillants sur l'ordinateur :

1. Ouvrez la fenêtre principale de l'application et sélectionnez la tâche **Poste de travail** dans la rubrique **Analyser**.
2. Cliquez sur le bouton **Analyser**.

Cette action lancera l'analyse de l'ordinateur et les détails de celle-ci sont repris dans une fenêtre spéciale. Le bouton **Fermer** fermera la fenêtre d'information sur la progression de l'analyse mais l'analyse ne sera pas interrompue.

5.3. Recherche d'éventuels virus dans les secteurs critiques de l'ordinateur

Il est primordial de protéger les secteurs critiques de l'ordinateur afin de préserver leur fonctionnement. Une tâche spéciale a été configurée pour rechercher d'éventuels virus dans ces secteurs. Elle se trouve dans la section **Analyser** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Secteurs critiques**, vous pouvez consulter les statistiques de la dernière analyse et les paramètres de la tâche : le niveau de sécurité sélectionné et l'action exécutée sur les objets malveillants. Il est possible de sélectionner également les secteurs critiques précis que vous souhaitez analyser et lancer directement l'analyse antivirus de ceux-ci.

Pour rechercher la présence d'éventuels objets malveillants dans les secteurs critiques de l'ordinateur :

1. Ouvrez la fenêtre principale de l'application et sélectionnez la tâche **Secteurs critiques** dans la rubrique **Analyser**.
2. Cliquez sur le bouton **Analyser**.

Cette action lancera l'analyse des secteurs choisis et les détails de celle-ci sont repris dans une fenêtre spéciale. Le bouton **Fermer** fermera la fenêtre d'information sur la progression de l'analyse mais l'analyse ne sera pas interrompue.

5.4. Recherche d'éventuels virus dans les fichiers, les répertoires ou les disques

Il arrive parfois que vous deviez absolument rechercher la présence d'éventuels virus non pas dans tout l'ordinateur mais uniquement dans un objet particulier comme l'un des disques durs. Vous pouvez sélectionner l'objet à analyser à

l'aide des méthodes traditionnelles du système d'exploitation Microsoft Windows Server (via l'**Assistant** ou sur le **Bureau**, etc.)

Pour lancer l'analyse d'un objet :

Placez la souris sur l'objet, ouvrez le menu contextuel de Microsoft Windows Server d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. Illustration 6).

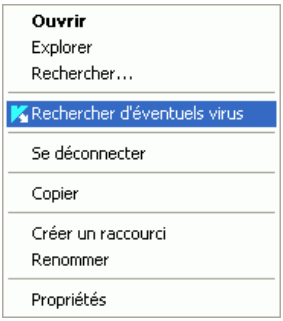


Illustration 6. Recherche d'éventuels virus dans un objet sélectionné à l'aide des outils Microsoft Windows Server

Cette action lancera l'analyse de l'objet choisi et les détails de celle-ci sont repris dans une fenêtre spéciale. Le bouton **Fermer** fermera la fenêtre d'information sur la progression de l'analyse mais l'analyse ne sera pas interrompue.

5.5. Mise à jour du logiciel

Kaspersky Lab met à jour les signatures des menaces et les modules de Kaspersky Anti-Virus via des serveurs spéciaux de mise à jour.

Les serveurs de mises à jour de Kaspersky Lab sont les sites Internet que Kaspersky Lab utilise pour diffuser les mises à jour du logiciel.

Attention !

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

Kaspersky Anti-Virus vérifie automatiquement par défaut la présence des mises à jour sur les serveurs de Kaspersky Lab. Si le serveur héberge les dernières mises à jour, Kaspersky Anti-Virus les télécharge et les installe en arrière plan.

Pour procéder à la mise à jour manuelle de Kaspersky Anti-Virus :

Sélectionnez le composant **Mise à jour** dans la section **Services** de la fenêtre principale du logiciel et cliquez sur **Mettre à jour** dans la partie droite.

Cette action entraînera la mise à jour de Kaspersky Anti-Virus. Tous les détails du processus sont illustrés dans une fenêtre spéciale.

5.6. Que faire si la protection ne fonctionne pas

En cas de problème ou d'erreur de fonctionnement de l'Antivirus Fichiers, veuillez vérifier son état. Si l'état donné est *ne fonctionne pas* ou *échec*, essayez de redémarrer Kaspersky Anti-Virus.

Si le problème n'est pas résolu après le redémarrage du logiciel, nous vous conseillons de corriger les erreurs à l'aide du programme de réparation de l'application (**Démarrer→Programmes→Kaspersky Anti-Virus 6.0 for Windows Servers→Modification, réparation ou suppression**).

Si la procédure de réparation n'a pas résolu le problème, contactez le service d'assistance technique de Kaspersky Lab. Vous devrez peut-être enregistrer le rapport sur l'activité du composant ou de l'ensemble de l'application et l'envoyer aux opérateurs du service d'assistance technique afin de leur fournir un maximum d'informations.

Afin d'enregistrer le rapport dans un fichier :

1. Sélectionnez Antivirus Fichiers dans la section **Protection** de la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc **Statistiques**.
2. Cliquez sur **Enregistrer sous** et saisissez, dans la fenêtre qui s'ouvre, le nom du fichier dans lequel vous souhaitez enregistrer les résultats du fonctionnement du composant.

Afin d'enregistrer directement le rapport sur le lancement ou l'état de tous les composants de Kaspersky Anti-Virus (Fichiers Antivirus, tâches de recherche de virus, fonctions de services),

1. Sélectionnez la section **Protection** dans la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc **Statistiques**.

   ou

Dans la fenêtre du rapport de n'importe quel composant, cliquez sur le lien Tous les rapports. Les rapports pour tous les composants de l'application seront repris dans l'onglet **Rapport**.

2. Cliquez sur **Enregistrer sous** et indiquez, dans la fenêtre qui s'ouvre, le nom du fichier dans lequel les résultats du fonctionnement du programme seront conservés.

CHAPITRE 6. ADMINISTRATION COMPLEXE DE LA PROTECTION

Kaspersky Anti-Virus peut être soumis à une administration complexe :

- Désactivation/activation du logiciel (cf. point 6.1, p. 55).
- Sélection des logiciels contrôlés contre lesquels Kaspersky Anti-Virus vous protégera (cf. point 6.2, p. 59).
- Constitution de la liste des exclusions pour la protection (cf. point 6.3, p. 61).
- Création de tâches personnalisées de recherche de virus et de mise à jour (cf. point 6.4, p. 68).
- Configuration du lancement des tâches à l'heure qui vous convient (cf. point 6.5, p. 70).
- Configuration des paramètres de performance (cf. point 6.6, p. 72) de la protection de l'ordinateur.

6.1. Désactivation/activation de la protection de votre ordinateur

Par défaut, Kaspersky Anti-Virus est lancé au démarrage du système comme en témoigne le message *Kaspersky Anti-Virus 6.0* qui apparaît dans le coin supérieur droit de l'écran. La protection est garantie pendant toute la séance de travail. Antivirus Fichiers est activé (cf. point 2.2.1, p. 17).

Vous pouvez désactiver la protection offerte par Kaspersky Anti-Virus.

Attention !

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

Notez que dans ce cas, la protection est envisagée dans le contexte d'Antivirus Fichiers. La désactivation ou la suspension du fonctionnement de l'Antivirus Fichiers n'a pas d'influence sur la recherche de virus et la mise à jour du logiciel.

6.1.1. Suspension de la protection

La suspension signifie l'Antivirus Fichiers est désactivé pour un certain temps.

Pour suspendre le fonctionnement de Kaspersky Anti-Virus :

1. Sélectionnez **Suspension de la protection** dans le menu contextuel (cf. point 4.2, p. 38)
2. Dans la fenêtre de désactivation (cf. Illustration 7), sélectionnez la durée au terme de laquelle la protection sera réactivée :
   - **Dans <intervalle de temps>** : la protection sera activée au terme de l'intervalle indiqué. Pour sélectionner la valeur, utilisez la liste déroulante.
   - **Après le redémarrage du logiciel:** la protection sera activée si vous lancez le programme depuis le menu **Démarrer** ou après le redémarrage du système (pour autant que le lancement du programme à l'allumage de l'ordinateur soit activé (cf. point 6.1.5, p. 59).
   - **Uniquement à la demande de l'utilisateur** : la protection sera activée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Activation de la protection** dans le menu contextuel du programme.

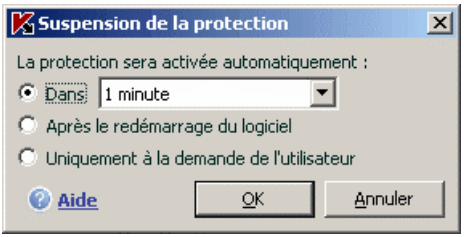


Illustration 7. Fenêtre de suspension de la protection de votre ordinateur

Astuce.

Vous pouvez également désactiver la protection du serveur de l'une des deux méthodes suivantes :

- Cliquez sur dans la section **Protection**.
- Sélectionnez **Quitter** dans le menu contextuel. Le programme sera déchargé de la mémoire vive.

Cette action suspend le fonctionnement de tous les composants de la protection. Les éléments suivants permettent de confirmer la désactivation :

Le nom des composants désactivés apparaît en grisé dans la section **Protection** de la fenêtre principale.
L'icône de l'application dans la barre des tâches est en noir et blanc.
Le troisième indice de protection (cf. point 5.1.1, p. 45) de votre ordinateur indique **Tous les composants de la protection sont suspendus.**

6.1.2. Désactivation complète de la protection du serveur

La désactivation complète signifie l'arrêt de l'Antivirus Fichiers. La recherche des virus et la mise à jour se poursuivent dans ce mode.

Si la protection est totalement désactivée, elle ne pourra être réactivée qu'à la demande de l'administrateur. L'activation automatique de l'Antivirus Fichiers après le redémarrage du système ou du logiciel n'aura pas lieu dans ce cas. Si pour une raison quelconque Kaspersky Anti-Virus entre en conflit avec d'autres logiciels installés sur l'ordinateur, vous pouvez arrêter le fonctionnement de l'Antivirus Fichiers ou composer une liste d'exclusions (cf. point 6.3, p. 61).

Pour désactiver complètement la protection de l'ordinateur :

1. Ouvrez la fenêtre de configuration de Kaspersky Anti-Virus et sélectionnez la section **Protection**.
2. Désélectionnez la case **Activer la protection**.

Cette action entraînera l'arrêt du fonctionnement de l'Antivirus Fichiers. Les éléments suivants permettent de confirmer la désactivation :

- Le nom de l'Antivirus Fichiers désactivé apparaît en grisé dans la section **Protection** de la fenêtre principale.
- L'icône de l'application dans la barre des tâches est en noir et blanc.

- L'indice de la protection (cf. point 5.1.1, p. 45) de votre ordinateur indique **Tous les composants de la protection sont désactivés**.

6.1.3. Suspension / désactivation du composant de la protection ou des tâches

Il existe plusieurs moyens de désactiver l'Antivirus Fichiers ou une tâche liée à la mise à jour ou à la recherche de virus. Toutefois, avant de faire quoi que ce soit, nous vous conseillons de définir la raison pour laquelle vous souhaitez les suspendre. Le problème pourrait également être résolu en modifiant, par exemple, le niveau de protection. Ainsi, si vous utilisez une base de données qui selon vous ne peut contenir de virus, il suffit de reprendre ce répertoire et les fichiers qu'il contient dans les exclusions (cf. point 6.3, p. 61).

Pour suspendre l'Antivirus Fichiers, la recherche de virus ou la mise à jour

Sélectionnez le composant ou la tâche dans la section correspondante de la partie gauche de la fenêtre principale du logiciel et cliquez sur dans la barre d'état.

L'état du composant (de la tâche) passe à *pause*. La protection assurée par le composant ou la tâche qui était exécutée sera suspendue jusqu'à ce que vous la réactiviez en cliquant sur le bouton .

Lorsque vous arrêtez le composant ou la tâche, les statistiques relatives à la session actuelle de Kaspersky Anti-Virus seront conservées et reprendront après la restauration du composant ou de la tâche.

Pour arrêter un composant, la recherche de virus ou la mise à jour :

Cliquez sur dans la barre d'état. Vous pouvez également arrêter un composant dans la boîte de dialogue de configuration du programme en désélectionnant la case **Activer <nom du composant>** dans le bloc **Général**.

Dans ce cas, l'état du composant (tâche) devient *désactivé (interrompu)*. La protection assurée par le composant ou la tâche qui était exécutée sera arrêtée jusqu'à ce que vous la réactiviez en cliquant sur le bouton . Pour la recherche de virus et la mise à jour, vous aurez le choix entre les options suivantes : poursuivre l'exécution de la tâche interrompue ou la reprendre à zéro.

En cas d'arrêt du composant ou de la tâche, toutes les statistiques antérieures sont perdues et les données seront à nouveau consignées au lancement du composant

6.1.4. Rétablissement de la protection de l'ordinateur

Si vous avez à un moment quelconque arrêté ou suspendu la protection de l'ordinateur, vous pourrez la rétablir à l'aide de l'une des méthodes suivantes :

Au départ du menu contextuel.

Sélectionnez le point **Activation la protection**.

Au départ de la fenêtre principale du logiciel.

Cliquez sur ▶ dans la barre d'état de la section **Protection** dans la fenêtre principale

L'état de la protection redevient immédiatement *fonctionne*. L'icône du logiciel dans la barre des tâches redevient active (en couleur). Le troisième indice de protection (cf. point 5.1.1, p. 45) de l'ordinateur indique ✔ **Tous les composants de la protection sont actifs**.

6.1.5. Fin de l'utilisation du logiciel

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Anti-Virus, sélectionnez le point **Quitter** dans le menu contextuel (cf. point 4.2, p. 38) du programme. Celui-ci sera déchargé de la mémoire vive, ce qui signifie que votre ordinateur ne sera plus protégé à partir de ce moment.

Si vous avez quitté le logiciel, sachez que vous pouvez à nouveau activer la protection de l'ordinateur en lançant Kaspersky Anti-Virus au départ du menu **Démarrer → Programmes → Kaspersky Anti-Virus 6.0 for Windows Servers → Kaspersky Anti-Virus 6.0 for Windows Servers**.

Il est possible également de lancer la protection automatiquement après le redémarrage du système d'exploitation. Afin d'activer ce mode, passez à la section **Protection** et cochez la case ☑ **Lancer l'application au démarrage de l'ordinateur**.

6.2. Types de programmes malveillants contrôlés

Kaspersky Anti-Virus vous protège contre divers types de programmes malveillants. Quels que soient les paramètres définis, l'application protègera toujours l'ordinateur contre les types de programmes malveillants les plus

dangereux tels que les virus, les chevaux de Troie et les utilitaires d'attaque. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une plus protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

Afin de sélectionner les types de programmes malveillants contre lesquels Kaspersky Anti-Virus vous protégera, passez à la section **Protection**, de la fenêtre de configuration du logiciel (cf. point 4.4, p. 42).

Les types de menaces (cf. point 1.1, p. 9) figurent dans le bloc **Catégories de programmes malicieux** :

- **Virus, vers, chevaux de Troie et utilitaires d'attaque**. Ce groupe reprend les programmes malveillants les plus répandus et les plus dangereux. Cette protection est le niveau minimum admissible. Conformément aux recommandations des experts de Kaspersky Lab, Kaspersky Anti-Virus contrôle toujours les programmes malveillants de cette catégorie.
- **Logiciel espion, adware, numéroteurs automatiques**. Ce groupe recouvre tous les riskwares qui peuvent entraîner une gêne ou certains dommages.
- **Programmes présentant un risque potentiel (riskwares)**. Ce groupe reprend les logiciels qui ne sont pas malveillants ou dangereux mais qui dans certaines circonstances peuvent servir à endommager votre ordinateur.

Ces groupes règlent l'ensemble de l'utilisation des signatures de menaces lors de l'analyse d'objets en temps réel ou lors de la recherche d'éventuels virus sur votre ordinateur.

Lorsque tous les groupes sont sélectionnés, Kaspersky Anti-Virus garantit la protection antivirus maximale de votre ordinateur. Si le deuxième et le troisième groupe sont désélectionnés, le logiciel vous protège uniquement contre les objets malveillants les plus répandus sans prêter attention aux programmes dangereux ou autres qui pourraient être installés sur votre ordinateur et causer des dommages matériels ou moraux.

Les experts de Kaspersky Lab ne conseillent pas de désactiver le contrôle du deuxième groupe. Lorsque Kaspersky Anti-Virus considère un programme comme étant dangereux alors que, d'après vous ce n'est pas le cas, il est conseillé de l'exclure (cf. point 6.3, p. 61).

6.3. Constitution de la zone de confiance

La Zone de confiance est en réalité une liste d'objets composée par l'administrateur. 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'administrateur 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 ou 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 de la classification de l'Encyclopédie des virus (état attribué à l'objet par le programme suite à l'analyse).

Attention !

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.

Afin de composer une liste des exclusions de la protection :,

1. Ouvrez la fenêtre de configuration l'application et passez à la section **Protection**.
2. Cliquez sur **Zone de confiance** dans le bloc du **Général**.
3. Dans la boîte de dialogue (cf. Illustration 8) qui apparaît, configurez les règles d'exclusion pour les objets et composez également une liste d'applications de confiance.

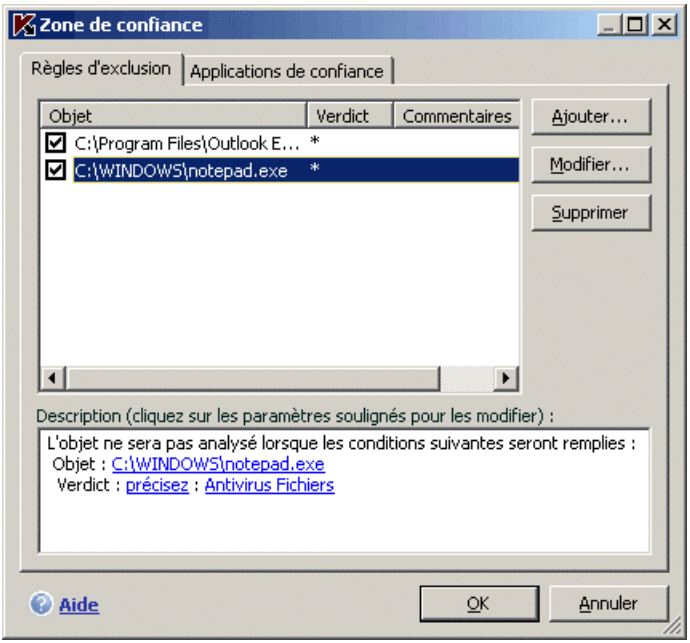


Illustration 8. Constitution de la zone de confiance

6.3.1. Règles d'exclusion

La règle d'exclusion est un ensemble de paramètres qui détermine si un objet quelconque sera analysé ou non par Kaspersky Anti-Virus

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 la classification de l'Encyclopédie des virus.

La classification est l'état que Kaspersky Anti-Virus a attribué à un objet après l'analyse. Il est attribué sur la base du classement des programmes malveillants et des riskwares présentés dans l'encyclopédie des virus de Kaspersky Lab.

Les riskwares n'ont pas de fonction malveillante mais ils peuvent être utilisés en tant que "complice" d'autres programmes malveillants car il présentent des failles et des erreurs. Les programmes d'administration à distance, les clients IRC, les serveurs FTP, tous les utilitaires d'arrêt ou de dissimulation de processus, les détecteurs de frappe de clavier, les décrypteurs de mot de passe, les dialers, etc. appartiennent à cette catégorie. Un tel programme n'est pas considéré comme un virus (not-a-virus) mais il peut appartenir à un sous-groupe tel que

Adware, Joke, Riskware, 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). De tels programmes peuvent être bloqués après l'analyse. Dans la mesure où certains d'entre eux sont très populaires auprès des utilisateurs, il est possible de les exclure de l'analyse. Pour ce faire, il faut ajouter le nom ou le masque de la menace en fonction du classement de l'Encyclopédie des virus à la zone de confiance.

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 classe cette activité parmi les activités qui présentent un risque potentiel et peut la bloquer. Afin d'éviter le blocage de l'application, il faut composer une règle d'exclusion pour laquelle la classification sera not-a-virus:RemoteAdmin.Win32.RAdmin.22.

L'ajout d'une exclusion s'accompagne de la création d'une règle qui pourra être exploitée Antivirus Fichiers et lors de l'exécution de tâches liées à la recherche de virus. Vous pouvez composer la règle dans une boîte de dialogue spéciale accessible au départ de la fenêtre de configuration de l'application, au départ de la notification de la découverte d'un objet ou au départ de la fenêtre du rapport.

*Ajout d'exclusion sur l'onglet **Règles d'exclusion** :*

1. Cliquez sur **Ajouter…** dans la fenêtre **Règles d'exclusion**.
2. Dans la fenêtre qui apparaît (cf. Illustration 9), sélectionnez le type d'exclusion dans la section **Paramètres** :

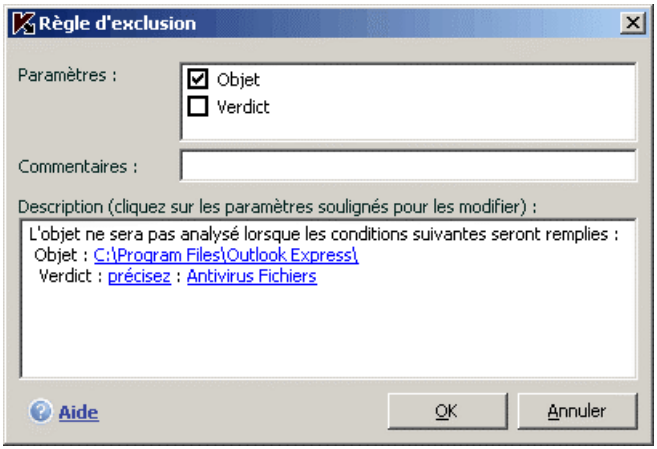


Illustration 9. Création d'une règle d'exclusion

☑ **Objet** : exclusion de l'analyse d'un objet, d'un répertoire particulier ou de fichiers correspondant à un masque défini.

☑ **Verdict :** exclusion de l'analyse d'un objet en fonction d'un état attribué selon le classement de l'encyclopédie des virus.

Si vous cochez simultanément les deux cases, vous créerez une règle pour l'objet défini répondant à la classification sélectionnée. Dans ce cas, les règles suivantes entreront en application :

- Si un fichier quelconque a été défini en tant qu' **Objet** et qu'un état particulier a été sélectionné pour la **Classification**, cela signifie que le fichier sélectionné sera exclu uniquement si l'état défini lui sera attribué pendant l'analyse.
- Si un secteur ou un répertoire quelconque a été défini en tant qu'**Objet** et qu'un état (ou masque de verdict) a été défini en tant que **Classification**, cela signifie que les objets correspondant à cet état, mais découverts uniquement dans ce secteur/répertoire, seront exclus.

3. Définissez la valeur du type d'exclusion sélectionné. Pour ce faire, cliquez avec le bouton gauche de la souris dans la section **Description** sur le lien précisez, situé à côté du type d'exclusion :
   - Pour le type **Objet**, saisissez dans la fenêtre qui s'ouvre son nom (il peut s'agir d'un fichier, d'un répertoire quelconque ou d'un masque de fichier (cf. point A.2, p. 195). Afin que l'objet indiqué (fichier, masque de fichiers, répertoire) soit ignoré partout pendant l'analyse, cochez la case ☑ **Sous-répertoires compris**.
   - Pour la **Verdict** indiquez le nom complet de l'exclusion telle qu'elle est reprise dans l'encyclopédie des virus ou selon un masque (cf. point A.3, p. 197).

     Pour certaines classifications, il est possible de définir dans le champ **Paramètres complémentaires** des conditions supplémentaires pour l'application de la règle.
4. Définissez les composants de Kaspersky Anti-Virus qui exploiteront la règle ainsi créée. Si vous choisissez la valeur quelconque, cette règle sera exploitée par tous les composants. Si vous souhaitez limiter l'application de cette règle à quelques composants uniquement, cliquez à nouveau sur quelconque et le lien prendra la valeur indiqué. Dans la fenêtre qui s'ouvre, cochez la case en regard des composants qui exploiteront la règle d'exclusion.

Création d'une règle d'exclusion au départ de la notification de la découverte d'un objet dangereux :

1. Cliquez sur Ajouter à la liste de confiance dans la fenêtre de notification

2. Dans la boîte de dialogue qui s'affiche, 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**.

Création d'une règle d'exclusion au départ de la fenêtre du rapport :

1. Sélectionnez dans le rapport l'objet que vous souhaitez ajouter aux exclusions.
2. Ouvrez le menu contextuel et sélectionnez le point **Ajouter à la zone de confiance** (cf. Illustration 10).

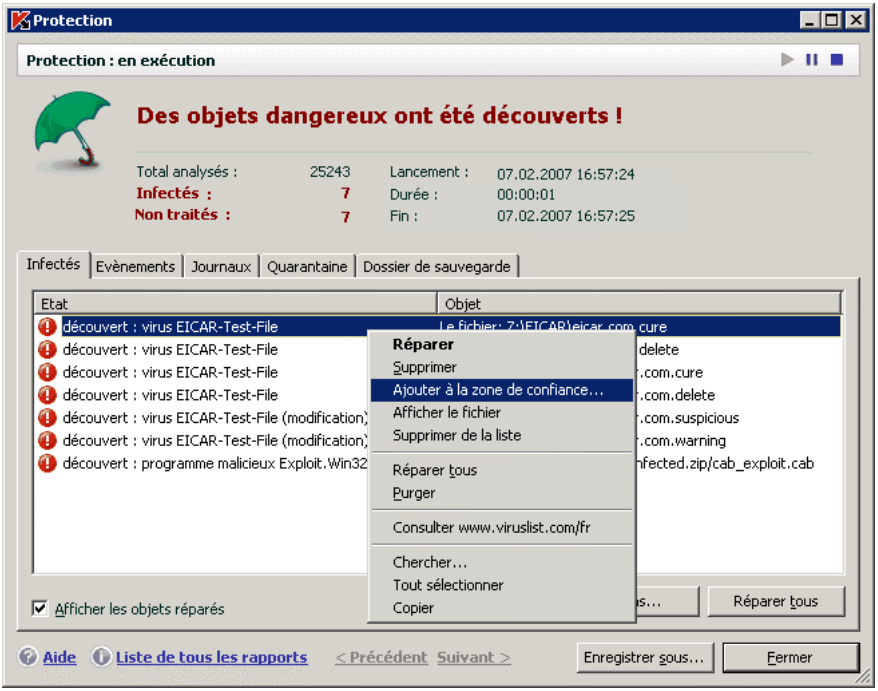


Illustration 10. Création d'une règle d'exclusion au départ du rapport

6.3.2. Applications de confiance

Kaspersky Anti-Virus vous permet de créer une liste d'applications de confiance dont l'activité, y compris les activités suspectes, les activités de fichiers 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 Servers sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance à 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 (cf. point 6.3.1, p. 62).

De plus, certaines actions considérées comme dangereuses sont en réalité normales dans le cadre du fonctionnement de divers programmes. Ainsi, l'interception du texte tapé avec le clavier est une action tout à fait normale pour les programmes de permutation automatique de la disposition du clavier (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.

De même, l'utilisation d'exclusion d'applications de confiance permet de résoudre divers problèmes de compatibilité entre certaines applications et Kaspersky Anti-Virus (par exemple, le trafic de réseau en provenance d'un autre ordinateur déjà analysé par un logiciel) et d'accroître les performances de l'ordinateur.

Par défaut Kaspersky Anti-Virus analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel.

La constitution de la liste des applications de confiance s'opère sur l'onglet spécial **Applications de confiance** (cf. Illustration 11). La liste des applications de confiance contient par défaut les applications dont l'activité n'est pas analysée sur la base des recommandations des experts de Kaspersky Lab. Si vous estimez que les applications de cette liste ne sont pas de confiance, désélectionnez les cases correspondantes. Vous pouvez modifier la liste à l'aide des boutons **Ajouter…**, **Modifier…** et **Supprimer** situés à droite.

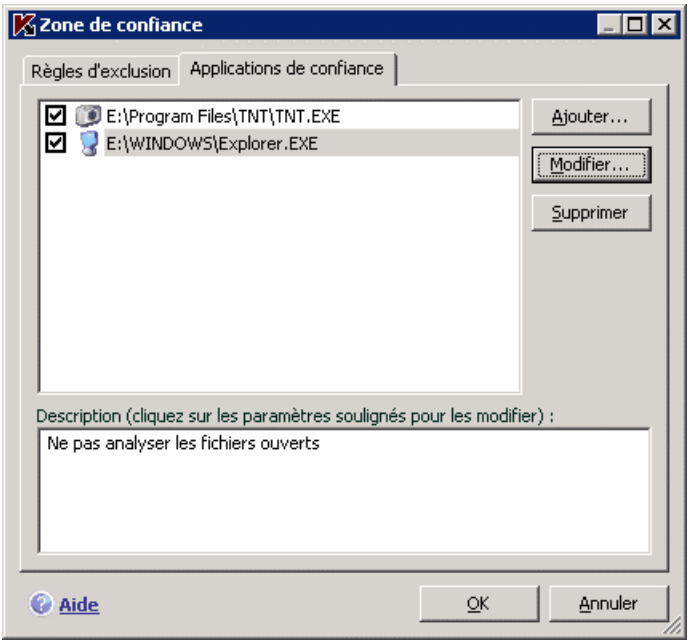


Illustration 11. Liste des applications de confiance

Afin d'ajouter un programme à la liste des applications de confiance :

1. Cliquez sur le bouton **Ajouter…** situé dans la partie droite de l'onglet **Applications de confiance**.
2. Dans la fenêtre **Application de confiance** (cf. Illustration 12) 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.

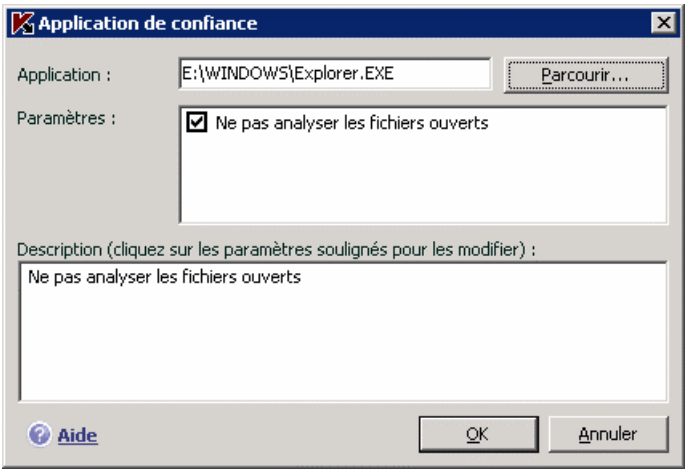


Illustration 12. Ajout d'une application à la liste des applications de confiance

Lors de la sélection du programme Kaspersky Anti-Virus enregistre les attributs internes du fichier exécutable. Ils serviront à l'identification de l'application pendant l'analyse comme application de confiance.

Le chemin d'accès au fichier est repris automatiquement lors de la sélection du nom.

3. Ensuite, le cas échéant, indiquez l'action de ce processus qui ne sera pas contrôlée par Kaspersky Anti-Virus:

   Ne pas analyser les fichiers ouverts : exclut de l'analyse tous les fichiers ouverts par le processus de l'application de confiance.

6.4. Lancement d'une tâche avec les privilèges d'un autre compte

Kaspersky Anti-Virus 6.0 offre la possibilité de lancer une tâche au nom d'un autre utilisateur (représentation). Cette option est désactivée par défaut et les tâches sont exécutées sous le compte de votre enregistrement dans le système.

Par exemple, il se peut que des privilèges d'accès à l'objet à analyser soient requis pour exécuter la tâche. Grâce à ce service, vous pouvez configurer le lancement de la tâche au nom d'un autre compte qui jouit de tels privilèges.

S'agissant de la mise à jour du logiciel, elle peut être réalisée au départ d'une source à laquelle vous n'avez pas accès (par exemple, le répertoire de mise à jour du réseau) ou pour laquelle vous ne connaissez pas les paramètres

d'autorisation du serveur proxy. Vous pouvez utiliser ce service afin de lancer la mise à jour au nom d'un utilisateur qui jouit de ces privilèges.

Pour configurer le lancement d'une tâche au nom d'un autre utilisateur :,

1. Sélectionnez le nom de la tâche dans la section **Analyser** (pour la recherche de virus) ou **Services** (pour la mise à jour)de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.
2. Cliquez sur le bouton **Configuration…** dans la boîte de dialogue de configuration de la tâche et passez à l'onglet **Complémentaire** dans la fenêtre qui s'affiche (cf. Illustration 13).
3. Pour activer ce service, cochez la case ☑ **Lancement de la tâche au nom de l'utilisateur**. Saisissez en dessous les données du compte sous lequel la tâche sera exécutée: nom d'utilisateur et mot de passe.

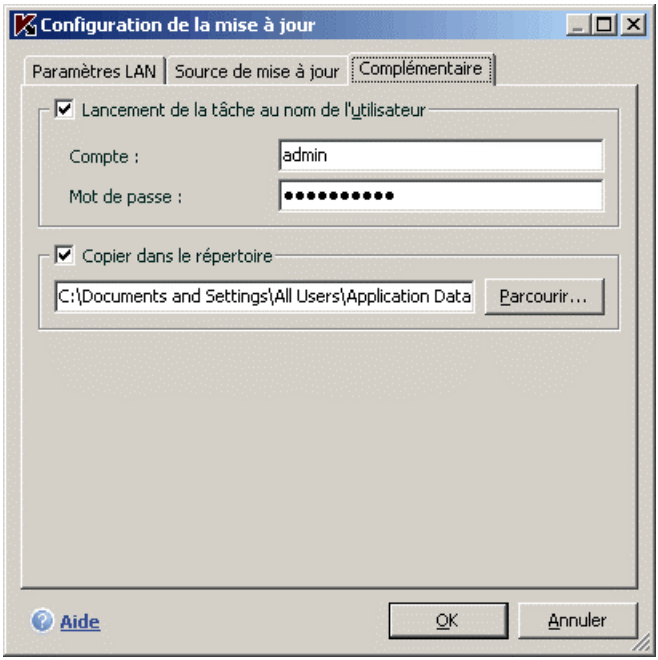


Illustration 13. Configuration du lancement de la mise à jour au nom d'un autre utilisateur

6.5. Programmation du lancement de tâches et de l'envoi des notifications

La configuration de la programmation est standard pour les tâches de recherche de virus, pour les mises à jour de l'application et pour l'envoi des notifications sur le fonctionnement de Kaspersky Anti-Virus.

Le lancement des tâches de recherche de virus créées lors de l'installation de l'application est désactivé par défaut. La seule exception est la tâche d'analyse des objets de démarrage qui est exécutée chaque fois que Kaspersky Anti-Virus est lancé. S'agissant des mises à jour, elles sont exécutées automatiquement par défaut au fur et à mesure que les mises à jour sont publiées sur les serveurs de Kaspersky Lab. Pour la mise à jour, la tâche est lancée par défaut toutes les 2 heures.

Si ce mode d'exécution de la tâche ne vous convient pas, il vous suffit de modifier les paramètres de la planification. Pour ce faire, sélectionnez le nom de la tâche dans la section **Analyser** (pour la recherche de virus) ou **Service** (pour la mise à jour et la copie des mises à jour) et cliquez sur le lien Configuration afin d'ouvrir la boîte de dialogue de configuration.

Afin d'activer le lancement programmer d'une tâche, cochez la case en regard de la condition de lancement de la tâche dans le bloc **Mode d'exécution**. Vous pouvez modifier les conditions de lancement de l'analyse dans la fenêtre **Programmation** (cf. Illustration 14) en cliquant sur **Modifier…**.

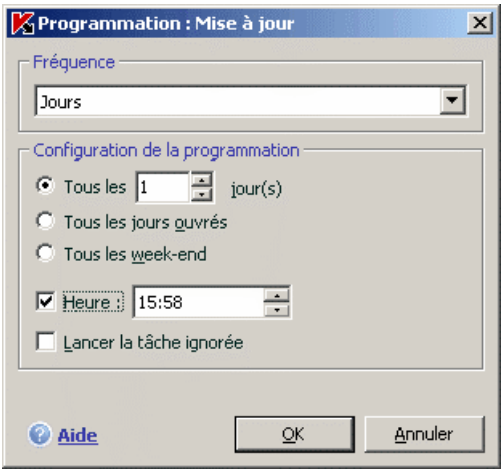


Illustration 14. Programmation de l'exécution de la tâche

L'élément le plus important à définir, c'est l'intervalle selon lequel l'événement aura lieu (exécution de la tâche ou envoi des notifications). Pour ce faire, sélectionnez l'option souhaitée dans le groupe **Fréquence** (cf. Illustration 14). Il faudra ensuite définir les paramètres de planification pour l'option choisie dans le bloc **Configuration de la programmation**. Vous avez le choix entre les options suivantes :

- **Au moment défini**. L'exécution de la tâche ou l'envoi de notifications a lieu au jour et à l'heure indiqué.
- **Au lancement de l'application**. L'exécution de la tâche ou l'envoi de notification a lieu à chaque démarrage de Kaspersky Anti-Virus. Vous pouvez également définir l'intervalle de temps après le lancement de l'application qui doit s'écouler avant l'exécution de la tâche.
- **Après chaque mise à jour**. La tâche est lancée après chaque mise à jour des signatures des menaces (ce point concerne uniquement les tâches liées à la recherche de virus).
- **Minutes.** L'intervalle entre les lancements de la tâche ou l'envoi de notifications se mesure en quelques minutes uniquement. Précisez le nombre de minutes entre chaque lancement dans les paramètres de programmation. L'intervalle maximum est de 59 minutes.
- **Heures**. L'intervalle entre les lancements de la tâche ou l'envoi de notifications est mesuré en heures. Si vous avez choisi cette fréquence, indiquez l'intervalle dans les paramètres de programmation : **Toutes les X heure(s)** et définissez l'intervalle X. Pour une mise à jour toute les heures, sélectionnez *Toutes les 1 heure(s).*

- **Jours**. L'exécution de la tâche ou l'envoi de notifications a lieu tous les quelques jours. Définissez la valeur de l'intervalle dans les paramètres de programmation :
  - Sélectionnez **Tous les X jours** et précisez l'intervalle *X* si vous souhaitez un intervalle de quelques jours.
  - Sélectionnez **Tous les jours ouvrés** si vous souhaitez exécuter l'action tous les jours du lundi au vendredi.
  - Sélectionnez **Tous les week-ends** si vous voulez que la tâche soit lancée uniquement les samedi et dimanche.

  En plus de la fréquence, définissez l'heure à laquelle la tâche sera lancée dans le champ **Heure**.
- **Semaines**. L'exécution de la tâche ou l'envoi de notifications a lieu certains jours de la semaine. Si vous avez choisi cette fréquence, il vous faudra cocher les jours d'exécution de la tâche dans les paramètres de la programmation. Précisez l'heure dans le champ **Heure**.
- **Mois**. L'exécution de la tâche ou l'envoi de notifications a lieu une fois par mois à l'heure indiquée.

Si pour une raison quelconque l'exécution est impossible (par exemple, aucun client de messagerie n'est installé ou l'ordinateur était éteint), vous pouvez configurer l'exécution automatique dès que cela sera possible. Pour ce faire, cochez la case **Lancer la tâche ignorée** dans la fenêtre de programmation.

6.6. Configuration de la productivité

La recherche de virus augmente la charge du processeur central et sur les sous-systèmes du disque, ce qui ralentit les autres applications. Par défaut, lorsqu'une telle situation se présente, l'application interrompt la recherche de virus et libère ainsi des ressources pour les autres applications de l'utilisateur.

Cependant, il existe de nombreux programmes qui sont lancés dès que des ressources sont libérées et qui fonctionnent en arrière plan. Afin que la recherche de virus ne dépendent pas de ces programmes, cochez la case **Céder les ressources aux autres applications** (cf. Illustration 15).

Notez 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 a une priorité supérieure.

Dans la fenêtre **Productivité** vous permet de configurer les performances des serveurs dotés de plusieurs processeurs.

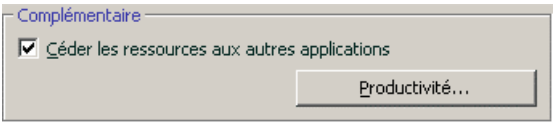


Illustration 15. Configuration de la productivité

Pour configurer les performances :

Sélectionnez la rubrique **Protection** dans la fenêtre principale de l'application et cliquez sur le lien Configuration. La configuration des performances s'opère dans le groupe **Complémentaire**.

6.7. Configuration multi-processeurs

Cette fenêtre vous permet de configurer les performances des serveurs dotés de plusieurs processeurs :

Nombre de copies du moteur antivirus : nombre de copies du moteur antivirus chargées au lancement de Kaspersky Anti-Virus sur le serveur. Cette valeur définit le nombre de processus antivirus exécutés en parallèle.

Plus le nombre de copies du moteur antivirus lancées est élevé, plus rapide sera le traitement antivirus des objets. Cela a toutefois des répercussions sur les performances du serveur.

De plus, l'exécution simultanée de plusieurs processus antivirus permet de garantir une protection continue au cas où un des moteurs arrêterait de fonctionner.

Afin de répartir automatiquement les processus antivirus entre les processeurs du serveur , cochez la case **Utiliser le pilote spécial pour l'organisation du traitement en parallèle**.

Lorsque la case est désélectionnée, vous pouvez régler manuellement la charge du serveur, par exemple réserver une partie des processeurs au traitement antivirus et l'autre, aux tâches directes du serveur. Pour ce faire, désélectionnez la case en regard du processeur à réserver exclusivement au travail du serveur dans le groupe **Processeurs utilisés**.

Les spécialistes de Kaspersky Lab recommande de réserver au moins un processeur aux tâches du serveur.

CHAPITRE 7. PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS DU SERVEUR

Kaspersky Anti-Virus possède un composant baptisé *Antivirus Fichiers* qui protège le système de fichiers du serveur contre les infections. Il 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.

L'icône de Kaspersky Anti-Virus dans la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un fichier est analysé.

Par défaut, l'antivirus de fichiers analyse *uniquement les nouveaux* fichiers ou les fichiers *modifiés*, c'est-à-dire les fichiers dans lesquels des données ont été ajoutées ou modifiées depuis la dernière requête. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Toute requête provenant d'un utilisateur ou d'un programme quelconque adressée à chaque fichier est interceptée par le composant.
2. L'antivirus de fichiers vérifie si la base iChecker™ ou iSwift™ contient des informations relatives au fichier intercepté. La nécessité d'analyser ou non le fichier est prise sur la base des informations obtenues.

Le processus d'analyse contient les étapes suivantes :

1. Le fichier est soumis à la recherche d'éventuels virus. L'identification des objets malveillants s'opère sur la base des *signatures des menaces* utilisées par le composant. Les signatures contiennent la définition de tous les programmes malveillants, menaces connus à ce jour et leur mode d'infection.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
    a. Si le fichier contient un code malveillant, l'antivirus de fichiers le bloque, place une copie dans le *dossier de sauvegarde* et tente de le réparer. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier 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 placé en *quarantaine*.

c. Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

7.1. Sélection du niveau de protection des fichiers

L'antivirus de fichiers protège les fichiers que vous utilisez selon un des niveaux suivants (cf. Illustration 16):

- **Elevé** : le contrôle des fichiers ouverts, enregistrés et modifiés est total.
- **Recommandé** : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. Ils prévoient l'analyse des objets suivants :
  - Programmes et objets en fonction du contenu;
  - Uniquement les nouveaux objets et les objets modifiés depuis la dernière analyse;
  - Les objets OLE intégrés.
- **Faible** : ce niveau vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de fichiers analysés est réduit.

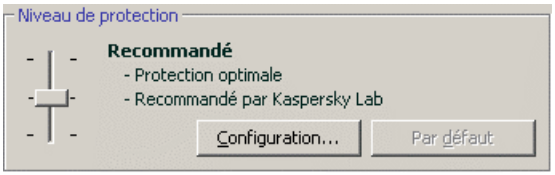


Illustration 16. Niveau de protection d'Antivirus Fichiers

Par défaut, la protection des fichiers s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau de protection des fichiers en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration complémentaire des paramètres de la protection. Dans ce cas, il est conseillé de choisir le niveau le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**. Voici un exemple d'une situation où le niveau Utilisateur serait le plus indiqué pour la protection des fichiers.

Exemple:

Dans le cadre de votre activité, vous travaillez avec de nombreux fichiers de divers formats et notamment des fichiers assez volumineux. Vous ne voulez pas prendre de risque en excluant de l'analyse certains fichiers sur la base de leur extension ou de leur taille, même si une telle décision va avoir des répercussions sur les performances de votre ordinateur.

Conseil pour la sélection du niveau :

Sur la base de ces informations, nous pouvons dire que le risque d'infection par un programme malveillant est relativement élevé. La taille et le type de fichiers utilisés sont trop hétérogènes et les exclure de l'analyse exposerait les informations sauvegardées sur l'ordinateur à des risques. Ce qui compte ici, c'est l'analyse des fichiers utilisés au niveau du contenu et non pas de leur extension.

Dans ce cas, il est conseillé d'utiliser le niveau **Recommandé** qui sera modifié de la manière suivante : lever les restrictions sur la taille des fichiers analysés et optimiser le fonctionnement de l'antivirus de fichiers en analysant uniquement les nouveaux fichiers et les fichiers modifiés. Cela permettra de réduire la charge de l'ordinateur pendant l'analyse des fichiers et de continuer à travailler sans problème avec d'autres applications.

Pour modifier les paramètres du niveau de protection actuel :

cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus de fichiers, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

Un quatrième niveau de protection est ainsi configuré : **Utilisateur** selon les paramètres que vous aurez définis.

7.2. Configuration de la protection des fichiers

La protection des fichiers sur l'ordinateur est définie par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 7.2.1, p. 77);
- Les paramètres qui définissent la zone protégée (cf. point 7.2.2, p. 80);
- Les paramètres qui définissent les actions à réaliser sur l'objet dangereux (cf. point 7.2.5, p. 85)).
- Les paramètres complémentaires de fonctionnement de l'Antivirus Fichiers (cf. point 7.2.3, page 82).

Tous ces paramètres sont abordés en détails ci-après.

7.2.1. Définition du type de fichiers analysés

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 texte). 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.

Le type de fichiers à analyser est défini dans la section **Types de fichiers** (cf. Illustration 17). Choisissez l'une des trois options :

- **Analyser tous les fichiers.** Dans ce cas, tous les objets ouverts, exécutés et enregistrés dans le système de fichiers seront analysés sans exception.
- **Analyser les programmes et les documents (selon le contenu).** L'antivirus de fichiers analysera uniquement les fichiers qui présentent un risque d'infection, c.-à-d. les fichiers dans lesquels un virus pourrait s'insérer.

Informations.

Il existe plusieurs formats de fichiers qui présentent un faible risque d'infection par un code malveillant suivie d'une activation de ce dernier. Les fichiers au format txt appartiennent à cette catégorie.

Il existe d'autre part des fichiers qui contiennent ou qui peuvent contenir un code exécutable. Il s'agit par exemple de fichiers exe, dll ou doc. Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.

Avant de passer à la recherche de virus dans le fichier, le système définit le format du fichier (txt, doc, exe, etc.) en analysant l'en-tête interne du fichier. Si l'analyse détermine qu'aucun des fichiers de ce format ne peut être infecté, le fichier n'est pas soumis à l'analyse et devient tout de suite accessible. Si le format du fichier laisse supposer un risque d'infection, le fichier est soumis à l'analyse.

- **Analyser les programmes et les documents (selon l'extension)**. Dans ce cas, l'antivirus de fichiers analyse uniquement les fichiers potentiellement infectés et le format du fichier est pris en compte sur la base de son extension. En cliquant sur le lien extension, vous pourrez découvrir la liste des extensions des fichiers (cf. point A.1, p. 193) qui seront soumis à l'analyse dans ce cas.

Conseil.

Il ne faut pas oublier qu'une personne mal intentionnée peut envoyer un virus sur votre ordinateur dans un fichier dont l'extension est txt alors qu'il s'agit en fait d'un fichier exécutable renommer en fichier txt. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon l'extension)**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon le contenu)**, l'antivirus de 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 minutieuse.

Vous pouvez, dans la section **Optimisation**, préciser que seuls les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse seront soumis à l'analyse antivirus. Ce mode réduit considérablement la durée de l'analyse et augmente la vitesse de traitement du logiciel. Pour ce faire, il est indispensable de cocher la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

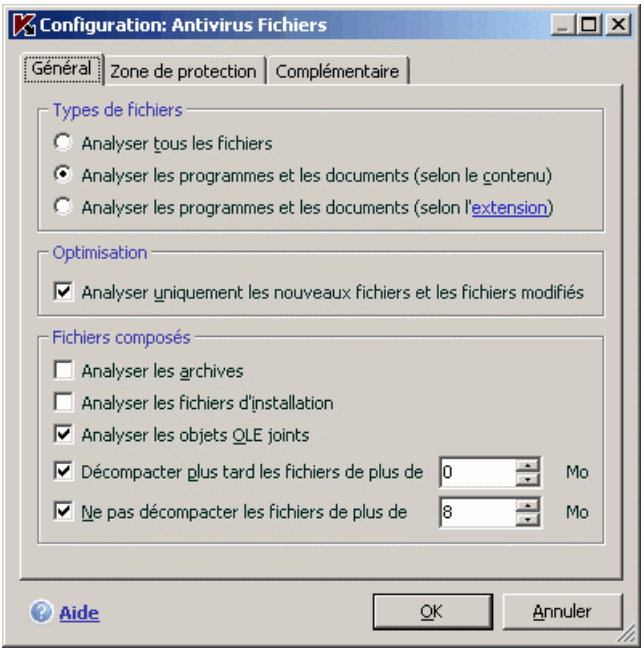


Illustration 17. Sélection du type de fichier soumis à l'analyse antivirus

Indiquez, dans la section **Fichiers composés**, les types de fichiers composés qui devront être soumis à l'analyse antivirus :

- **Analyser les archives/uniquement les nouvelles archives** : analyse les archives au format ZIP, CAB, RAR, ARJ.
- **Analyser les/uniquement les nouveaux fichiers d'installation** : recherche la présence d'éventuels virus dans les archives autoextractibles.
- **Analyser les/uniquement les nouveaux objets OLE joints** : analyse les objets intégrés au fichier (exemple : tableau Excel, macro dans un document Microsoft Office Word, pièce jointe d'un message électronique, etc.)

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 avez défini dans la section **Optimisation** l'analyse uniquement des nouveaux fichiers et des fichiers modifiés, il sera impossible de sélectionner un type de fichier composé.

Afin de préciser le type de fichiers composés qu'il ne faut pas analyser, utilisez l'un des paramètres suivants :

☑ **Décompacter plus tard les fichiers de plus de ... Mo**. Lorsque la taille de l'objet composé dépasse cette limite, il sera analysé en tant qu'objet unique (l'en-tête est analysée) et il pourra être manipulé. L'analyse des objets qu'il contient sera réalisée plus tard. Si la case n'est pas cochée, l'accès aux fichiers dont la taille est supérieure à la valeur définie sera bloqué jusque la fin de l'analyse des objets.

☑ **Ne pas décompacter les fichiers de plus de … Mo**. Dans ce cas, le fichier dont la taille est supérieure à la valeur indiquée sera ignoré par l'analyse.

7.2.2. Constitution de la zone protégée

Par défaut, l'antivirus de fichiers analyse tous les fichiers dès qu'une requête leur est adressée, quel que soit le support sur lequel ils se trouvent (disque dur, cédérom/DVD ou carte Flash).

Vous pouvez définir la zone protégée. Pour ce faire :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration
2. Cliquez sur le bouton **Configuration** et sélectionnez l'onglet **Zone de protection** dans la fenêtre qui s'ouvre (cf. Illustration 18).

L'onglet reprend la liste des objets qui seront soumis à l'analyse de l'antivirus de fichiers. La protection de tous les objets situés sur les disques durs, les disques amovibles et les disques de réseaux connectés à votre ordinateur est activée par défaut. Vous pouvez enrichir et modifier cette liste à l'aide des boutons **Ajouter…**, **Modifier…** et **Supprimer**.

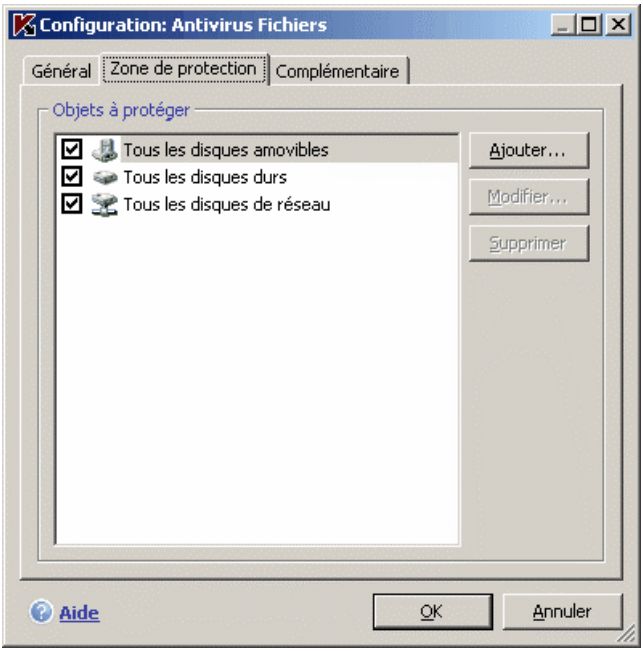


Illustration 18. Constitution de la zone protégée

Si vous souhaitez restreindre le nombre d'objets protégés, vous pouvez suivre l'une des méthodes suivantes :

- Indiquer uniquement les répertoires, disques ou fichiers qui doivent être protégés.
- Constituer une liste des objets qui ne doivent pas être protégés (cf. point 6.3, page 61).
- Utiliser simultanément la première et la deuxième méthode, c.-à-d. définir une zone de protection de laquelle une série d'objets seront exclus.

Vous pouvez utiliser des masques lors de l'ajout d'objets à analyser. N'oubliez pas que la saisie de masques est uniquement admise avec le chemin d'accès absolu aux objets :

- **C:\dir*.*** ou **C:\dir*** ou **C:\dir** : tous les fichiers du répertoire *C:\dir*
- **C:\dir*.exe** : tous les fichiers *.exe du répertoire *C:\dir*
- **C:\dir*.ex?**tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère

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

Afin que l'analyse de l'objet sélectionné soit complète, cochez la case ☑ **Y compris les sous-répertoires**.

Attention.

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 votre ordinateur !

7.2.3. Configuration des paramètres complémentaires

En guise de paramètres complémentaires de l'antivirus Fichiers, vous pouvez définir le mode d'analyse des objets du système de fichiers et les conditions d'arrêt temporaire du composant.

Pour configurer les paramètres complémentaires de l'antivirus fichiers :

1. Sélectionnez **Antivirus fichiers** dans la fenêtre principale et à l'aide du lien Configuration, ouvrez la fenêtre de configuration du composant.
2. Cliquez sur le bouton **Configuration** et dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Complémentaire** (cf. Illustration 19).

Le mode d'analyse des objets est défini par les conditions de déclenchement de l'antivirus Fichiers. Vous avez le choix entre les options suivantes :

- **Mode intelligent**. Ce mode vise à accélérer le traitement des objets afin de les rendre plus vite accessibles à l'utilisateur. Lorsque ce mode est sélectionné, la décision d'analyser un objet est prise sur la base de l'analyse des opérations réalisées avec cet objet.

  Par exemple, en cas d'utilisation d'un document Microsoft Word, Kaspersky Antivirus analyse le fichier à la première ouverture et après la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

  Le mode intelligent est utilisé par défaut.

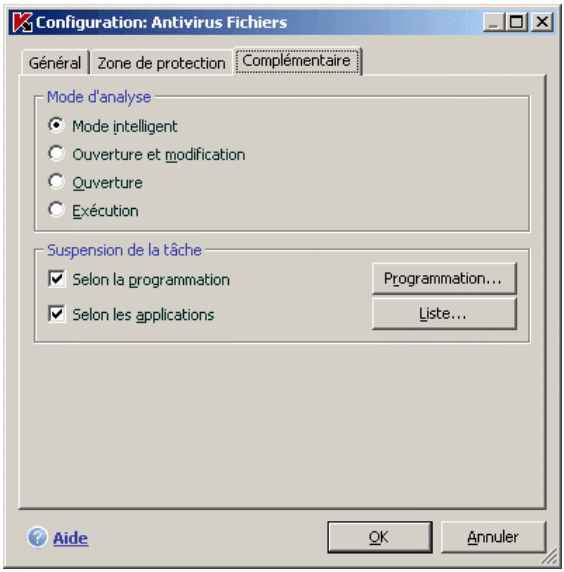


Illustration 19. Configuration des paramètres complémentaires de l'Antivirus Fichiers.

- **Ouverture et modification** : l'antivirus de fichiers analyse les objets à l'ouverture et à chaque modification.
- **Ouverture** : les objets sont analysés uniquement lors des tentatives d'ouverture.
- **Exécution** : les objets sont analysés uniquement lors des tentatives d'exécution.

La suspension temporaire de l'antivirus de fichiers peut s'imposer lors de l'exécution de tâches qui nécessitent beaucoup de ressources du système d'exploitation. Pour réduire la charge et permettre à l'utilisateur d'accéder rapidement aux objets, il est conseillé de désactiver le composant à certains moment ou lors de l'utilisation de certains programmes.

Afin de suspendre l'activité du composant pour un certain temps, cochez la ☑ **Selon la programmation** et dans la fenêtre (cf. Illustration 20) qui s'ouvre après avoir cliqué sur le lien **Programmation…**, définissez la plage d'arrêt du composant. Pour ce faire, saisissez la valeur au format hh:mm dans les champs correspondants.

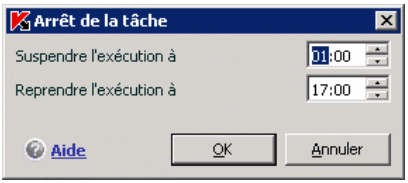


Illustration 20. Suspension du composant

Pour désactiver le composant en cas d'utilisation d'applications gourmande s en ressources, cochez la case **Selon les applications** (cf. Illustration 21) et dans la fenêtre qui s'ouvre après avoir cliqué sur le bouton **Liste…**, composez la liste des programmes.

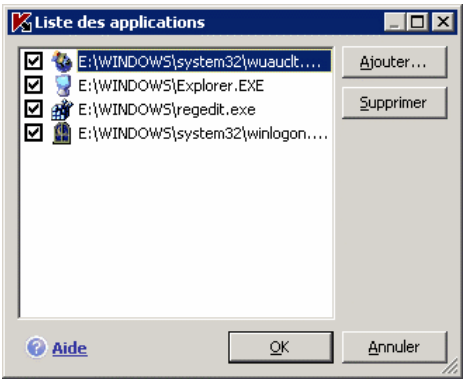


Illustration 21. Constitution de la liste des applications

Pour ajouter des applications à la liste, cliquez sur le bouton **Ajouter…**. Cette action entraînera l'ouverture d'un menu contextuel contenant le point **Parcourir.** Vous aurez accès à une fenêtre standard de sélection des fichiers où vous pourrez indiquer le fichier exécutable de l'application à ajouter. L'élément **Applications**, quant à lui, vous permettra d'opérer un choix parmi les applications en cours d'exécution.

Afin de supprimer une application, sélectionnez-la puis cliquez sur **Supprimer**.

Vous pouvez suspendre temporairement l'arrêt de l'antivirus de fichiers lors de l'utilisation d'une application concrète. Pour ce faire, il suffit de désélectionner la case située en regard de l'application. Il n'est pas nécessaire de la supprimer complètement de la liste.

7.2.4. Restauration des paramètres de protection des fichiers par défaut

Lorsque vous configurez l'Antivirus de 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**.

Pour restaurer les paramètres de protection des fichiers par défaut :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection.**

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 conserver la liste des objets, cochez la case **Zone d'analyse** dans la fenêtre **Restauration des paramètres**.

7.2.5. Sélection de l'action exécutée sur les objets

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

L'antivirus de fichier peut attribuer l'un des statuts suivants à l'objet :

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*) (cf. point 1.1, p. 9).
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le code du fichier contient une séquence de code semblable à celle d'un virus inconnu ou le code modifié d'un virus connu.

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

Pour modifier l'action à exécuter sur l'objet :

Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien

Configuration Toutes les actions possibles sont reprises dans la section correspondante (cf. Illustration 22).

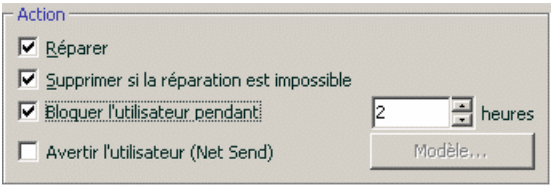


Illustration 22. Actions que peut exécuter Antivirus Fichiers sur un objet dangereux

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
☑ **Réparer** ☐ **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 réparation a réussi, l'utilisateur pourra y accéder. En cas d'échec de la réparation, l'objet est placé en quarantaine. Les informations sont consignées dans le rapport. Il est possible de tenter de réparer l'objet ultérieurement.
☑ **Réparer** ☑ **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 réparation a réussi, l'utilisateur pourra y accéder. En cas d'échec de la réparation, l'objet est supprimé.
☐ **Réparer** ☑ **Supprimer**	L'Antivirus Fichiers bloque l'accès à l'objet et le supprime.
☑ **Bloquer l'utilisateur pendant… heures**	Bloquer la connexion actuelle du compte utilisateur au serveur en cas de tentative de copie d'un objet infecté ou potentiellement infecté. Cette action peut être prise en plus de l'action associée au traitement de

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
	l'objet (réparation ou suppression). N'oubliez pas que si l'utilisateur arrête la séance et entre à nouveau dans le système, Kaspersky Anti-Virus considèrera cela comme une nouvelle connexion et le blocage sera levé.
☑ **Avertir l'utilisateur (NetSend)**	Avertir, via NetSend, l'utilisateur de l'ordinateur au départ duquel la tentative de copie d'un objet infecté ou potentiellement infecté sur le serveur a eu lieu. Afin de configurer le modèle de notification, cliquez sur Modèles (cf. point 7.2.6, p. 87).

Avant toute réparation ou suppression d'un objet, Kaspersky Anti-Virus crée une copie de sauvegarde et la place dans le dossier de sauvegarde au cas où il faudrait restaurer l'objet ou s'il devenait possible de le réparer.

Attention ! Les actions **Bloquer l'utilisateur** et **Avertir l'utilisateur (NetSend)** ne sont pas disponibles dans les applications installées sous Microsoft Windows NT Server 4.0.

7.2.6. Composition des modèles de notification

Cette fenêtre vous permet de composer le texte du modèle de notification de l'utilisateur de l'ordinateur au départ duquel la tentative de copie d'un objet infecté ou potentiellement infecté sur le serveur a eu lieu.

Le texte du message peut contenir des macros afin d'apporter plus d'informations : chemin d'accès à l'objet dangereux et nom de la menace. Pour ajouter des macros au texte, cliquez sur **Macros**.

Pour rétablir le texte d'origine utilisé en guise de modèle pour la notification, cliquez sur **Par défaut**.

7.3. Réparation différée des objets

Dans Kaspersky Anti-Virus for Windows Servers, 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 les réparer. Pour ce faire :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc Statistiques.
2. Sélectionnez les objets qui vous intéressent sur l'onglet **Infectés** et cliquez sur **Actions** ⟶ **Réparer tous**.

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 de votre ordinateur ! Il est vivement conseillé de ne pas ignorer les objets malveillants.

CHAPITRE 8. RECHERCHE DE VIRUS SUR VOTRE ORDINATEUR

Kaspersky Anti-Virus 6.0 for Windows Servers recherche la présence éventuelle de virus aussi bien dans des objets particuliers (fichiers, répertoires, disques, disques amovibles) que dans tout l'ordinateur. 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 propose par défaut les tâches de recherche de virus suivantes :

Secteurs critiques

Recherche de la présence éventuelle de virus dans tous les secteurs critiques de l'ordinateur. Il s'agit de : la mémoire système, des objets exécutés au démarrage du système, des secteurs d'amorçage des disques et des répertoires système *Windows* et *system32*. Cette tâche consiste à identifier rapidement dans le système tous les virus actifs sans lancer une analyse complète de l'ordinateur.

Mon poste de travail

Recherche de la présence éventuelle de virus sur votre ordinateur avec analyse minutieuse de tous les disques connectés, de la mémoire et des fichiers.

Objets de démarrage

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 (cf. point 8.4, p. 93) et même programmer le lancement de la tâche (cf. point 6.5, p. 70).

Il est possible également de créer des tâches personnalisées (cf. point 8.3, p. 92) de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des bases de messagerie une fois par semaine ou une tâche pour la recherche de la présence éventuelle de virus dans un répertoire quelconque.

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 traditionnelles (ex. : dans la fenêtre de l'**Assistant** ou au départ du **Bureau**, etc.).

La section **Recherche de virus** dans la partie gauche de la fenêtre principale de l'application reprend la liste complète des tâches liées à la recherche de virus créées sur votre ordinateur.

8.1. Administration des tâches de recherche de virus

Les tâches liées à la recherche de virus peuvent être lancées manuellement ou automatiquement selon un horaire défini (cf. point 6.5, p. 70).

Afin de lancer la tâche de recherche de virus manuellement :

Sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale du logiciel et cliquez sur ▶ dans la barre d'état.

Les tâches en cours d'exécution (y compris les tâches créées via Kaspersky Administration Kit) sont reprises dans le menu contextuel qui s'ouvre d'un clic droit sur l'icône de l'application dans la barre des tâches.

Pour suspendre l'exécution de la tâche de recherche de virus :

Cliquez sur ❚❚ dans la barre d'état. L'état de l'exécution de la tâche devient *pause*. L'analyse sera suspendue jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon l'horaire.

Pour suspendre l'exécution de la tâche de recherche de virus :

Cliquez sur ■ dans la barre d'état. L'état de l'exécution de la tâche devient *interrompue*. L'analyse sera arrêtée jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon l'horaire. Au moment du prochain lancement de la tâche vous pourrez soit reprendre la recherche là où elle a été interrompue ou en lancer une nouvelle.

8.2. Composition de la liste des objets à analyser

Afin de consulter la liste des objets qui seront analysés lors de l'exécution de la tâche, sélectionnez le nom de la tâche (ex. : **Mon poste de travail**) dans la section **Analyser** dans la fenêtre principale du programme. La liste des objets

sera reprise dans la partie droite de la fenêtre sous la barre d'état (cf. Illustration 23).

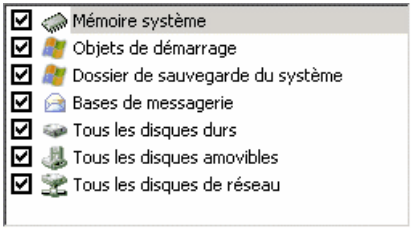


Illustration 23. Liste des objets à analyser

La liste des objets à analyser pour la liste des tâches créées par défaut lors de l'installation du logiciel est déjà composée. Lors de la création d'une tâche personnalisée ou lors de la sélection d'un objet dans le cadre de la recherche de virus, vous constituez vous-même la liste des objets.

Les boutons situés à droite de la liste vous permettront d'ajouter de nouveaux éléments ou de modifier la liste des objets à analyser. Afin d'ajouter un nouvel objet à analyser, cliquez sur **Ajouter…** et indiquez l'objet dans la fenêtre qui s'affiche.

Pour le confort de l'utilisateur, il est possible d'ajouter aux zones d'analyse des catégories telles que les boîtes aux lettres de l'utilisateur, la mémoire système, les objets de démarrage, le dossier de sauvegarde du système d'exploitation et les objets situés dans le dossier de quarantaine de Kaspersky Anti-Virus.

De plus, lors de l'ajout d'un répertoire contenant des objets intégrés, vous pouvez modifier la récursion. Pour ce faire, sélectionnez l'objet dans la liste des objets à analyser, ouvrez le menu contextuel et choisissez la commande **Sous-répertoires compris.**

Afin de supprimer un objet, sélectionnez-le dans la liste (son nom apparaîtra sur un fond gris) puis cliquez sur **Supprimer**. Vous pouvez suspendre temporairement l'analyse de certains objets sans avoir à les supprimer de la liste. Pour ce faire, il suffit de désélectionner la case qui se trouve en regard de l'objet qui ne doit pas être analysé.

Afin de lancer l'analyse, cliquez sur **Analyser** ou sélectionnez **Lancement** dans le menu qui apparaît après avoir cliqué sur **Actions…**.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows Server (exemple : via l'**Assistant** ou sur le **Bureau**, etc. (cf. Illustration 24). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

Illustration 24. Analyse d'un objet au départ du menu contextuel de Microsoft Windows

8.3. Création de tâches liées à la recherche de virus

Afin de rechercher la présence éventuelle de virus parmi les objets de votre ordinateur, vous pouvez soit utiliser les tâches d'analyse intégrées livrées avec le logiciel, soit utiliser des tâches personnalisées. La création d'une nouvelle tâche s'opère sur la base des tâches d'analyse existantes.

Afin de créer une nouvelle tâche d'analyse :

1. Dans la section **Analyser** de la fenêtre principale du logiciel, sélectionnez la tâche dont les paramètres vous conviennent le mieux.
2. Ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situés à droite de la liste des objets à analyser puis sélectionnez **Enregistrer sous**.
3. Saisissez, dans la fenêtre qui s'ouvre, le nom de la nouvelle tâche puis cliquez sur **OK**. La nouvelle tâche apparaît désormais sous le nom choisi dans la liste de tâches de la section **Analyser** de la fenêtre principale du logiciel.

Attention !

Le nombre de tâches qui peuvent être créées est limité. Le nombre maximal est de quatre tâches.

La nouvelle tâche possède des paramètres identiques à ceux de la tâche qui lui a servi de fondation. Pour cette raison, vous devrez procéder à une configuration complémentaire : composer la liste des objets à analyser (cf. point 8.2, p. 90),

indiquer les paramètres d'exécution de la tâche (cf. point 8.4, p. 93) et, le cas échéant, programmer (cf. point 6.5, p. 70)le lancement automatique.

Afin de renommer une tâche créée :

> sélectionnez la tâche dans la section **Analyser** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situé à droite de la liste des objets à analyser puis sélectionnez le point **Renommer**.

Saisissez, dans la fenêtre qui s'ouvre, le nouveau nom de la nouvelle tâche puis cliquez sur **OK**. Le nom de la tâche dans la section **Analyser** sera modifié.

Pour supprimer une tâche créée :

> sélectionnez la tâche dans la section **Analyser** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situé à droite de la liste des objets à analyser puis sélectionnez le point **Supprimer**.

Confirmez la suppression de la tâche dans la boîte de dialogue de confirmation. La tâche sera ainsi supprimée de la liste des tâches dans la section **Analyser**.

Attention !

Vous pouvez uniquement renommer les tâches que vous avez créées.

8.4. Configuration des tâches liées à la recherche de virus

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

Afin de passer à la configuration des paramètres des tâches :

> Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Analyser**.

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

- sélectionner le niveau de protection pour l'exécution de la tâche (cf. point 8.4.1, p. 94);
- passer à la configuration détaillée du niveau :

- indiquer les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 8.4.2, p. 95);
- configurer le lancement des tâches au nom d'un autre compte utilisateur (cf. point 6.4, p. 68);
- définir les paramètres complémentaires de l'analyse (cf. point 8.4.5, p. 101);

- restaurer les paramètres d'analyse utilisés par défaut (cf. point 8.4.3, p. 98);
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou potentiellement infecté (cf. point 8.4.4, p. 99);
- programmer le lancement automatique de la tâche (cf. point 6.5, p. 70).

De plus, vous pouvez définir des paramètres uniques de lancement pour toutes les tâches (cf. point 8.4.6, p. 103).

Tous ces paramètres de configuration de la tâche sont abordés en détails ci-après.

8.4.1. Sélection du niveau de protection

Chaque tâche liée à la recherche de virus analyse les objets selon un des trois niveaux suivants (cf. Illustration 25):

Elevé pour l'analyse complète en profondeur de votre ordinateur ou d'un disque, d'un répertoire ou d'un dossier particulier. Ce niveau est recommandé lorsque vous pensez que votre ordinateur a été infecté par un virus.

Recommandé. les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets qu'au niveau **Elevé**, à l'exception des fichiers au format de courrier électronique.

Faible : ce niveau vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de fichiers analysés est réduit.

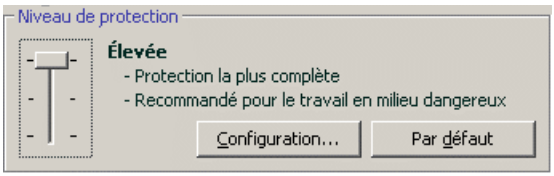


Illustration 25. Sélection du niveau de protection pour la recherche de virus

Par défaut, l'analyse des objets s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau d'analyse des objets en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration complémentaire des paramètres de l'analyse. Dans ce cas, il est conseillé de choisir le niveau le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**.

Pour modifier les paramètres du niveau de protection actuel :

cliquez sur **Configuration** dans la fenêtre de configuration de la tâche, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

Un quatrième niveau de protection est ainsi configuré : **Utilisateur** selon les paramètres que vous aurez défini.

8.4.2. Définition du type d'objet analysé

La définition du type d'objet à analyser précise le format, la taille et l'emplacement des fichiers sur lesquels porte la tâche.

Le type de fichiers à analyser est défini dans la section **Types de fichiers** (cf. Illustration 26). Choisissez l'une des trois options :

- **Analyser tous les fichiers**. Tous les fichiers sans exception seront analysés.
- **Analyser les programmes et les documents (selon le contenu).** Le programme analysera uniquement les fichiers qui présentent un risque d'infection, c.-à-d. les fichiers dans lesquels un virus pourrait s'insérer.

  Avant de passer à la recherche de virus dans l'objet, le système définit le format du fichier (txt, doc, exe, etc.) en analysant l'en-tête interne du fichier.

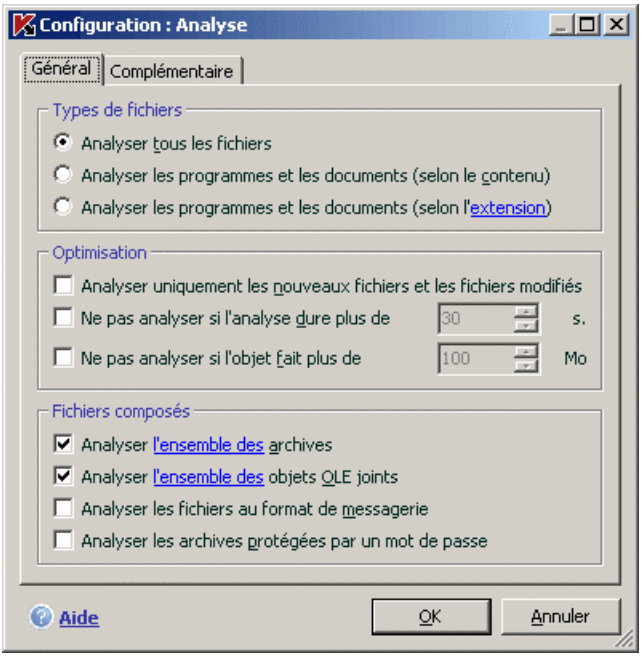


Illustration 26. Configuration des paramètres de l'analyse

Informations.

Il existe plusieurs formats de fichiers qui présentent un faible risque d'infection par un code malveillant suivie d'une activation de ce dernier. Les fichiers au format txt appartiennent à cette catégorie.

Il existe d'autre part des fichiers qui contiennent ou qui peuvent contenir un code exécutable. Il s'agit par exemple de fichiers exe, dll ou doc. Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.

- **Analyser les programmes et les documents (selon l'extension).** Dans ce cas, le programme analyse uniquement les fichiers potentiellement infectés et le format du fichier est pris en compte sur la base de son extension. En cliquant sur l'extension, vous pourrez découvrir a liste des extensions des fichiers qui seront soumis à l'analyse dans ce cas (cf. point A.1, p. 193).

Conseil.

Il ne faut pas oublier que le virus dans un fichier texte est peut-être un fichier exécutable renommé en fichier texte. Si vous sélectionnez l'option **Analyser**

les programmes et les documents (selon l'extension), ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon le contenu)**, le programme 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.

Vous pouvez, dans la section **Optimisation**, préciser que seuls les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse, seront soumis à l'analyse antivirus. Ce mode réduit considérablement la durée de l'analyse et augmente la vitesse de traitement du logiciel. Pour ce faire, il est indispensable de cocher la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

Vous pouvez aussi, dans la section **Optimisation**, instaurer une limite sur la durée de l'analyse et la taille maximale d'un objet:

- **Ne pas analyser si l'analyse dure plus de…s**. Cochez cette case afin de limiter dans le temps l'analyse d'un objet et saisissez dans le champ de droite la durée maximale autorisée pour l'analyse. Si cette valeur est dépassée, l'objet sera exclu de l'analyse.
- **Ne pas analyser si l'objet fait plus de … Mo**. Cochez cette case pour limiter au niveau de la taille l'analyse des objets et saisissez dans le champ de droite la taille maximale autorisée. Si cette valeur est dépassée, l'objet est exclu de l'analyse.

Indiquez, dans la section **Fichiers composés**, les types de fichiers composés qui devront être soumis à l'analyse antivirus :

- **Analyser l'ensemble des/uniquement les nouveaux(-elles) archives** : analyse les archives au format ZIP, CAB, RAR, ARJ, LHA, JAR, ICE.

Attention !

La suppression des archives qui ne sont pas réparées par Kaspersky Anti-Virus (par exemple : HA, UUE, TAR) n'est pas automatique, même si la réparation ou la suppression automatique a été sélectionnée, si la réparation est impossible.

Pour supprimer de telles archives, cliquez sur le lien Supprimer archive dans la fenêtre de notification de découverte d'un objet dangereux. Ce message apparaît en cas de sélection de l'action **Confirmer pendant l'analyse/ Confirmer à la fin de l'analyse** (cf. point 8.4.4, p. 99). Une telle archive infectée peut être supprimée manuellement.

- **Analyser l'ensemble des/uniquement les nouveaux(-elles) objets OLE joints** : analyse les objets intégrés au fichier (ex. : tableau Excel ou macro dans Word, pièce jointe d'un message, etc.)

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 avez défini dans la section **Optimisation** l'analyse uniquement des nouveaux fichiers et des fichiers modifiés, il sera impossible de sélectionner un type de fichier composé.

☑ **Analyser les fichiers au format de messagerie** : analyse les fichiers au format de courrier électronique ainsi que les bases de données de messagerie. Si la case est désélectionnée, les fichiers au format de messagerie seront analysés comme des fichiers binaires (sans interprétation du format) et si le fichier n'est pas infecté et que le paramètre Analyser tous les fichiers a été sélectionné, le rapport indiquer le statut *ok*. Si les paramètres d'analyse des fichiers ont été définis (selon le type ou l'extension), l'objet sera ignoré avec le verdict *exclu en fonction du type*.

Nous attirons votre attention sur les particularités suivantes de l'analyse de bases de messagerie protégées par un mot de passe :

- Kaspersky Anti-Virus identifie le code malveillant dans les bases de messagerie de Microsoft Office Outlook 2000 mais ne les répare pas;
- Le programme ne prend pas en charge la recherche de code malveillant dans les bases de messagerie de Microsoft Office Outlook 2003 protégées par un mot de passe.

☑ **Analyser les archives protégées par un mot de passe** : active l'analyse des archives protégées par un mot de passe. La boîte de dialogue de saisie du mot de passe s'affichera avant de procéder à l'analyse des objets de l'archive. Si la case n'est pas cochée, les archives protégées par un mot de passe seront ignorées.

8.4.3. Restauration des paramètres d'analyse par défaut

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 d'analyse des objets par défaut :

1. Sélectionnez le nom de la tâche dans la section **Recherche de virus** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection.**

8.4.4. Sélection de l'action exécutée sur les objets

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*)
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient probablement 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 suspects sont placés en quarantaine.

Pour modifier l'action à exécuter sur l'objet :

sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration de la tâche. Toutes les actions possibles sont reprises dans la section correspondante (cf. Illustration 27).

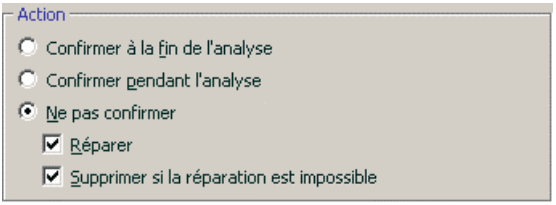


Illustration 27. Sélection de l'action à réaliser sur l'objet dangereux

Action choisie	**Conséquence en cas de découverte d'un objet malveillant/potentiellement infecté**
Confirmer à la fin de l'analyse	Le programme reporte le traitement des objets jusque la fin de l'analyse. Les fenêtres de confirmation pour chaque objet apparaîtront les unes après les autres à la fin de l'analyse.

Action choisie	Conséquence en cas de découverte d'un objet malveillant/potentiellement infecté
◉ **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.
◉ **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 potentiellement infectés, ce qui conduira inévitablement à l'infection de celui-ci.
◉ **Ne pas confirmer** ☑ **Réparer**	Le programme, sans notification préalable, tente de réparer l'objet découvert. Si la réparation est possible, l'objet est placé dans le dossier de sauvegarde en vue d'un traitement ultérieur. Si la tentative a échoué, l'accès à l'objet est bloqué.
◉ **Ne pas confirmer** ☑ **Réparer** ☑ **Supprimer si la réparation est impossible**	Le programme, sans notification préalable, tente de réparer l'objet découvert. Si la réparation de l'objet échoue, il sera supprimé. Une copie de l'objet est placée dans le dossier de sauvegarde.
◉ **Ne pas confirmer** ☑ **Réparer** ☑ **Supprimer**	Le programme supprimera automatiquement l'objet.

Avant de réparer ou de supprimer un objet , Kaspersky Anti-Virus crée une copie de sauvegarde et la place dans le dossier de sauvegarde (cf. point 11.2, p. 127)

au cas où il serait nécessaire de restaurer l'objet ou un moyen de le réparer serait à nouveau disponible.

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

8.4.5. Paramètres complémentaires pour la recherche de virus

En plus de la configuration des paramètres principaux de la recherche de virus, vous pouvez également définir des paramètres complémentaires (cf. Illustration 28):

☑ **Activer la technologie iChecker™** : utilise la technologie qui permet d'accélérer l'analyse grâce à l'exclusion de certains objets. L'exclusion d'un objet s'opère selon un algorithme particulier qui tient compte de la date d'édition des signatures de menaces, de la date de l'analyse précédente et des modifications des paramètres d'analyse.

Admettons que vous ayez une archive qui a été analysée par le programme et qui est saine. 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 changé le contenu de l'archive (ex. : ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases des signatures des menaces, l'archive sera analysée à nouveau.

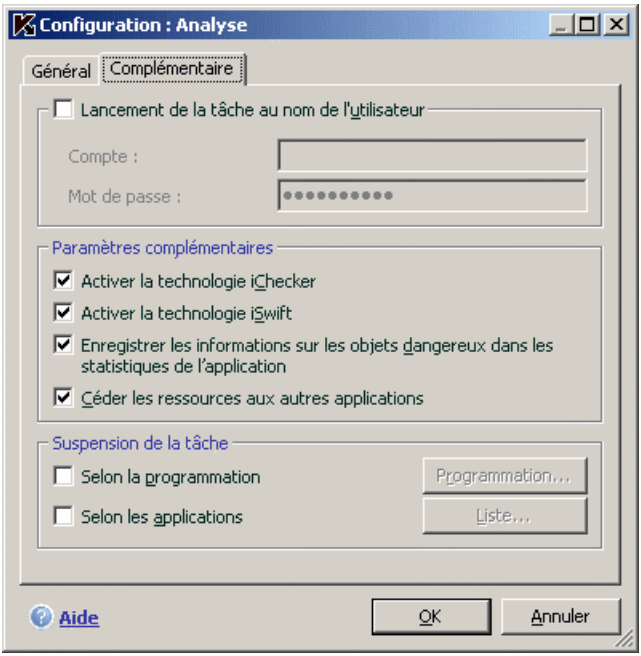


Illustration 28. Configuration complémentaire de l'analyse

La technologie iChecker™ a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et ne s'applique qu'aux objets dont la structure est connue de Kaspersky Anti-Virus (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

Activer la technologie iSwift : Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. La technologie iSwift a ses limites : elle est liée à un emplacement particulier du fichier dans le système de fichiers et applicable uniquement aux objets figurant dans le système de fichiers NTFS.

Enregistrer les informations sur les objets dangereux dans les statistiques de l'application: enregistre les informations sur la découvertes d'objets dangereux dans les statistiques globales de l'application et affiche la liste des menaces dangereuses sur l'onglet Infectés de la fenêtre du rapport (cf. point 11.3.2, p. 134). Si la case n'est pas cochée, les informations relatives aux objets dangereux ne seront pas reprises dans le rapport et par conséquent, il sera impossible de traiter ces objets.

Céder les ressources aux autres applications : interrompt la recherche de virus si les ressources du processeur sont occupées par d'autres applications.

8.4.6. Définition de paramètres d'analyse uniques pour toutes les tâches

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.

Afin de définir des paramètres d'analyse uniques pour toutes les tâches :

1. Sélectionnez la section **Analyser** dans la partie gauche de l'onglet et cliquez sur le lien Configuration.
2. Dans la boîte de dialogue de configuration qui s'affiche, définissez les paramètres de l'analyse : sélectionnez le niveau de protection (cf. point 8.4.1, p. 94), réalisez la configuration complémentaire du niveau et indiquez l'action qui sera réalisée sur les objets (cf. point 8.4.4, p. 99).
3. Afin d'appliquer les paramètres définis à toutes les tâches, cliquez sur **Appliquer** dans la section **Paramètres des autres tâches**. Confirmez les paramètres uniques dans la boîte de dialogue de confirmation.

CHAPITRE 9. ESSAI DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Une fois que vous aurez installé et configuré Kaspersky Anti-Virus, nous vous conseillons de vérifier l'exactitude des paramètres et le bon fonctionnement de l'application à l'aide d'un « virus » d'essai et d'une de ses modifications.

9.1. Virus d'essai EICAR et ses modifications

Ce virus d'essai a été développé spécialement par l'organisation eicar (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Il NE S'AGIT PAS D'UN VIRUS et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent 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 : http://www.eicar.org/anti_virus_test_file.htm.

Le fichier téléchargé du site de l'organisation **EICAR** contient le corps d'un virus d'essai standard. Lorsque Kaspersky Anti-Virus le découvre, il lui attribue le statut **virus** et exécute l'action définie par l'administrateur pour les objets de ce type.

Afin de vérifier le comportement de Kaspersky Anti-Virus lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du « virus » d'essai standard en ajoutant un des préfixes repris dans le tableau ci-après.

Préfixe	**Etat du virus d'essai**	**Actions lors du traitement de l'objet par l'application**
Pas de préfixe, « virus » d'essai standard	Le fichier contient le virus d'essai. Réparation impossible.	L'application identifie l'objet comme un objet malveillant qui ne peut être réparé et le supprime.
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).
SUSP- WARN-	Le fichier contient le virus d'essai (modification). Réparation impossible.	Cet objet est une modification d'un virus connu ou il s'agit d'un virus inconnu. Au moment de la découverte, les bases des signatures des menaces ne contenait pas la description de la réparation de cet objet. L'application place l'objet en quarantaine en vue d'un traitement ultérieur à l'aide des signatures des menaces actualisées.
ERRO-	Erreur de traitement.	Une erreur s'est produite lors du traitement de l'objet : l'application ne peut accéder à l'objet à analyser 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).
CURE-	Le fichier contient le virus d'essai. Réparation possible. L'objet sera réparé et le texte du corps du « virus » sera remplacé par CURE.	L'objet contient un virus qui peut être réparé. L'application réalise le traitement antivirus de l'objet qui sera totalement réparé.

Préfixe	Etat du virus d'essai	Actions lors du traitement de l'objet par l'application
DELE-	Le fichier contient le virus d'essai. Réparation impossible.	L'objet contient un virus qui ne peut être réparé ou un cheval de Troie. L'application supprime de tels objets.

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 contient une description de l'état et la réaction de Kaspersky Anti-Virus face à divers types de virus d'essai. La troisième colonne contient les informations relatives au traitement que réserver l'application aux objets dont l'état est identique.

Les actions exécutées sur chacun des objets sont définies par les paramètres de l'analyse antivirus.

9.2. Vérification de l'Antivirus Fichiers

Afin de vérifier le fonctionnement de l'Antivirus Fichiers :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai téléchargé depuis le site officiel de l'organisation (cf. point 9.1, p. 104) ainsi que les versions modifiées du virus d'essai.
2. 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. Pour ce faire, cochez la case ☑ **Enregistrer les événements non critiques** dans la fenêtre de configuration des rapports (cf. point 11.3.1, p. 133).
3. Exécutez le virus d'essai ou sa modification.

Antivirus Fichiers intercepte la requête adressée au fichier, il l'analyse et la supprime.

En choisissant diverses actions à exécuter sur l'objet découvert, vous pouvez vérifier les réactions d'Antivirus Fichiers en cas de découverte de divers types d'objets.

Tous les résultats du fonctionnement d'Antivirus Fichiers sont consultables dans le rapport de fonctionnement du composant.

9.3. Vérification des tâches de recherche de virus

Pour vérifier les tâches de recherche de virus

1. Créez un répertoire sur le disque, copiez-y le virus d'essai téléchargé depuis le site officiel de l'organisation (cf. point 9.1, p. 104) ainsi que les versions modifiées du virus d'essai.
2. Créez une nouvelle tâche de recherche de virus (cf. point 8.3, p. 92) et en guise d'objet à analyser, sélectionnez le dossier contenant la sélection de virus d'essais (cf. point 9.1, p. 104).
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. Pour ce faire, cochez la case ☑ **Enregistrer les événements non critiques** dans la fenêtre de configuration des rapports.
4. Exécutez la tâche (cf. point 8.1, p. 90) de recherche des virus.

Au fur et à mesure que des objets infectés ou suspects seront identifiés, des messages apparaîtront à l'écran et fourniront les informations sur l'objet et sur l'action à exécuter :

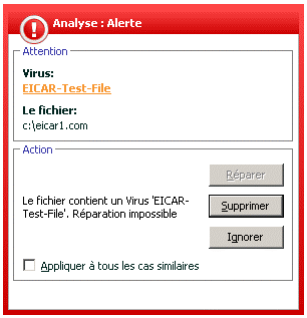


Illustration 29. Découverte d'un objet dangereux

Ainsi, en choisissant diverses actions, vous pouvez vérifier les réactions de Kaspersky Anti-Virus en cas de découverte de différents types d'objets.

Tous les résultats de l'exécution de la tâche sont consultables dans le rapport de fonctionnement du composant.

CHAPITRE 10. MISE A JOUR DU LOGICIEL

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

La mise à jour du logiciel suppose le téléchargement et l'installation sur votre ordinateur des :

- **Signature des menaces**

  La protection de vos données est réalisée à l'aide des signatures des menaces. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces signatures 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 versions antérieures des logiciels antivirus de Kaspersky Lab prenaient en charge l'utilisation de différentes bases de signatures des menaces : *standard* ou *étendues*. Elles se différenciaient par le type d'objets dangereux contre lesquels elles assuraient une protection. Avec Kaspersky Anti-Virus, il n'est plus nécessaire de se soucier du choix des bases de signatures des menaces adéquates. Nos logiciels utilisent désormais les signatures des menaces qui offrent une protection non seulement contre divers types de programmes malveillants et d'objets présentant un risque potentiel, mais également contre les attaques de pirates informatiques.

- **Modules de l'application**

  En plus des signatures des menaces connues, vous pouvez actualiser les modules logiciels de Kaspersky Anti-Virus. Ces mises à jour sont diffusées régulièrement par Kaspersky Lab.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour de Kaspersky Anti-Virus. Afin de pouvoir télécharger ces bases, votre ordinateur doit absolument être connecté à Internet.

Si vous n'avez pas accès au serveur de mise à jour de Kaspersky Lab (par exemple, pas de connexion Internet), vous pouvez contacter notre bureau principal aux numéros de téléphone +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 afin d'obtenir les coordonnées d'un partenaire de Kaspersky

Lab qui pourra vous proposer ces mises à jour sur une disquette ou un cédérom dans une archive zip

Le téléchargement des mises à jour s'opère selon l'un des modes suivants :

- *Automatique*. Kaspersky Anti-Virus vérifie la source des mises à jour selon une fréquence déterminée afin de voir si elle contient une mise à jour. La fréquence peut être augmentée lors des épidémies de virus et réduites en dehors de celles-ci. S'il identifie des actualisations récentes, Kaspersky Anti-Virus les télécharge et les installe. Ce mode est activé par défaut.
- *Programmé*. La mise à jour du logiciel est réalisée selon un horaire défini.
- *Manuel*. Vous lancez vous-même la procédure de mise à jour du logiciel.

Au cours du processus, les modules logiciels et les signatures des menaces installés sur votre ordinateur sont comparés à ceux de la source. Si le serveur abrite la dernière version des signatures et des modules, un message le signale dans la fenêtre de l'application. Si les signatures et les composants installés sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les signatures et les modules diffèrent, la partie manquante de la mise à jour sera installée. La copie des signatures 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 signatures des menaces, 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 (cf. point 10.2, p. 110) une mise à jour est indispensable, par exemple si les signatures des menaces 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 (cf. point 10.4.4, p. 119). Ce service permet d'actualiser les bases antivirus et les modules utilisés par les applications de la version 6.0 sur les ordinateurs du réseau en réduisant le trafic Internet.

10.1. Lancement de la mise à 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 (cf. point 10.4.1, p. 112).

Vous pouvez lancer la mise à jour du logiciel depuis :

- le menu contextuel (cf. point 4.2, p. 38);

- la fenêtre principale du logiciel (cf. point 4.3, p. 39).

Pour lancer la mise à jour du logiciel depuis le menu contextuel :

1. Ouvrez le menu à l'aide d'un clic droit sur l'icône du logiciel dans la barre des tâches.
2. Sélectionnez le point **Mise à jour**.

Pour lancer la mise à jour du logiciel depuis la fenêtre principale du logiciel :

1. Sélectionnez le composant **Mise à jour** dans la section **Services**.
2. Cliquez sur le bouton **Mettre à jour** (appel du programme depuis l'aide) dans la partie droite de la fenêtre principale ou sur dans la barre d'état.

Le processus de mise à jour du logiciel sera illustré dans une fenêtre spéciale. Vous pouvez dissimuler la fenêtre avec les résultats actuels de la mise à jour. Pour ce faire, cliquez sur **Fermer**. La mise à jour ne sera pas interrompue.

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 (cf. point 10.4.4, p. 119).

10.2. Annulation de la dernière mise à jour

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Anti-Virus commence par créer une copie de sauvegarde de la version actuelle des signatures des menaces avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau la version antérieure des signatures après une mise à jour ratée.

Pour revenir à l'utilisation de la version précédente des signatures des menaces:

1. Sélectionnez le composant **Mise à jour** dans la section **Service** dans la fenêtre principale du logiciel.
2. Cliquez sur le bouton **Retour à l'état précédent** (appel du programme depuis l'aide) dans la partie droite de la fenêtre principale).

10.3. Création de tâches liées à la mise à jour

Une tâche de mise à jour a été intégrée à Kaspersky Anti-Virus pour la mise à jour des signatures des menaces et des modules de l'application. Vous pouvez toutefois créer vos propres tâches de mise à jour avec différents paramètres et heures de lancement.

Admettons que vous avez installé Kaspersky Anti-Virus sur un ordinateur portable que vous utilisez à la maison et au bureau. A la maison, la mise à jour s'opère depuis les serveurs de mise à jour de Kaspersky Lab et au bureau, depuis un répertoire local contenant les fichiers nécessaires. Afin de ne pas devoir modifier chaque fois les paramètres en fonction de l'endroit où vous vous trouvez, vous pouvez créer deux tâches différentes.

Pour créer une nouvelle tâche de mise à jour :

1. Sélectionnez le point **Mise à jour** de la section **Services** dans la fenêtre principale, ouvrez le menu contextuel d'un clic droit et sélectionnez le point **Enregistrer sous**.
2. Saisissez le nom de la tâche dans la fenêtre qui s'affiche puis cliquez sur **OK**. La nouvelle tâche figure désormais dans la section **Services** de la fenêtre principale du logiciel.

Attention !

Le Kaspersky Anti-Virus n'accepte qu'un maximum de deux tâches de mise à jour créées par l'utilisateur.

La nouvelle tâche applique tous les paramètre de la tâche qui lui a servi de modèle, à l'exception de la programmation. Le lancement automatique de la nouvelle tâche est désactivé par défaut. Vous devrez dès lors procéder à une configuration complémentaire: indiquer la source de la mise à jour (cf. point 10.4.1, page. 112), définir les paramètres de connexion (cf. point 10.4.3, p. 117) et, le cas échéant activer le lancement avec les privilèges (cf. point 6.4, p. 68) et configurer la programmation (cf. point 6.5, p. 70).

Pour renommer une tâche :

Sélectionnez la tâche dans la section **Services** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris et sélectionnez le point **Renommer**.

Saisissez le nouveau nom de la tâche dans la fenêtre qui s'affiche puis, cliquez sur **OK**. Le nom de la tâche dans la section **Service** sera modifié.

Pour supprimer une tâche :

Sélectionnez la tâche dans la section **Service** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris et sélectionnez le point **Supprimer**.

Confirmez la suppression de la tâche dans la boîte de dialogue qui s'affiche. La tâche sera supprimée de la liste des tâches de la section **Service**.

Attention !

Il est possible de renommer ou de supprimer uniquement les tâches utilisateur que vous avez créées.

10.4. Configuration de la mise à jour

La mise à jour du logiciel s'exécute selon les paramètres qui définissent :

- la ressource d'où les fichiers seront copiés avant d'être installés (cf. point 10.4.1, p. 112);
- le mode de lancement de la mise à jour du logiciel et les éléments mis à jour (cf. point 10.4.2, p. 115);
- la fréquence d'exécution de la mise à jour si le lancement automatique a été configuré (cf. point 6.5 p. 70);
- le nom du compte utilisateur sous lequel la mise à jour va être réalisée (cf. point 6.4, p. 68) ;
- la nécessité ou non de copier les mises à jour récupérées dans un répertoire local (cf. point 10.4.4; p. 119);
- les actions à réaliser après la mise à jour du logiciel (cf. point 10.4.4, p. 119).

Tous ces paramètres sont abordés en détails ci-après.

10.4.1. Sélection de la source des mises à jour

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

Vous pouvez choisir une des sources suivantes :

- *Serveur d'administration* : entrepôt centralisé des mises à jour sur le serveur d'administration de Kaspersky Administration Kit (pour de plus

amples informations, consultez le guide de l'administrateur de "Kaspersky Administration Kit 5.0").

- *Serveurs de mise à jour de Kaspersky Lab* : sites Internet spéciaux qui hébergent les mises à jour des signatures des menaces et des modules de l'application pour tous les logiciels de Kaspersky Lab.
- *Serveurs HTTP ou FTP, répertoires locaux ou de réseau :* serveur ou répertoire local contenant une sélection récente de mise à jour.

Si vous n'avez pas accès au serveur de mise à jour de Kaspersky Lab (par exemple, pas de connexion Internet), vous pouvez contacter notre bureau principal aux numéros de téléphone +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 afin d'obtenir les coordonnées d'un partenaire de Kaspersky Lab qui pourra vous proposer ces mises à jour sur une disquette ou un cédérom dans une archive zip.

Attention !

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.

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

La sélection de la source de la mise à jour s'opère dans l'onglet **Source de mise à jour** (cf. Illustration 30).

Par défaut la mise à jour s'opère depuis les serveurs de mise à jour de Kaspersky Lab. Cette liste n'est pas modifiable. Lors de la mise à jour, Kaspersky Anti-Virus consulte cette liste, contacte le premier serveur de la liste et tente de télécharger les mises à jour. Lorsque l'adresse sélectionnée ne répond pas, le logiciel choisit le serveur suivant et tente à nouveau de télécharger les bases antivirus.

Pour réaliser la mise à jour au départ d'un site FTP ou HTTP quelconque :

1. Cliquez sur **Ajouter…**;
2. Sélectionnez le site ftp- ou http- dans la fenêtre **Sélection de la source de la mise à jour** ou indiquez son adresse IP, son nom symbolique ou l'URL dans le champ **Source**. Si un site ftp est choisi en tant que source, il est permis d'indiquer les paramètres d'autorisation dans l'URL selon le format ftp://<nom_d'utilisateur>:<mot de passe>@<hôte>:<port>.

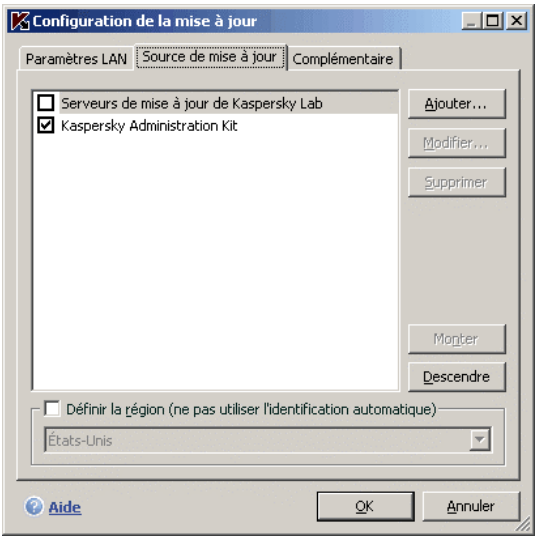


Illustration 30. Sélection de la source de la mise à jour

Attention !

Si vous avez sélectionné une ressource située en dehors du réseau local, vous devrez absolument avoir une connexion Internet pour procéder à la mise à jour.

Pour actualiser le logiciel au départ d'un répertoire quelconque :

1. Cliquez sur **Ajouter…** ;
2. Sélectionnez le répertoire dans la fenêtre **Sélection de la source de la mise à jour** ou saisissez son chemin d'accès complet dans le champ **Source**.

Kaspersky Anti-Virus ajoute la nouvelle source de mise à jour au début de la liste et l'active automatiquement (la case en regard est cochée).

Si plusieurs ressources ont été sélectionnées en guise de source 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. Vous pouvez modifier l'ordre des sources dans la liste à l'aide des boutons **Monter**/**Descendre**

Modifiez la liste des sources à l'aide des boutons **Ajouter…**, **Modifier…**, **Supprimer**. Les serveurs de mise à jour de Kaspersky Lab et Kaspersky Administration Kit sont des sources qui ne peuvent pas être modifiées ou supprimées.

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. Kaspersky Lab possède des serveurs dans 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.

Afin de sélectionner le serveur le plus proche, cochez la case ☑ **Définir la région (ne pas utiliser l'identification automatique)** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle. Si la case est cochée, alors la mise à jour sera réalisée en tenant compte de la région sélectionnée. La case est désélectionnée par défaut et lors de la mise à jour, la région est définie sur la base des informations reprises dans la base de registres système.

10.4.2. Sélection du mode et des objets de la mise à jour

La définition des objets à mettre à jour et du mode de mise à jour est l'un des moments décisifs de la configuration de la mise à jour.

Les objets de la mise à jour (cf. Illustration 31) désignent les objets qui seront actualisés :

- Les signatures de menaces ;
- Les modules de l'application.

Les signatures des menaces sont toujours actualisées tandis que la mise à jour des modules de l'application se produit uniquement si l'option a été configurée.

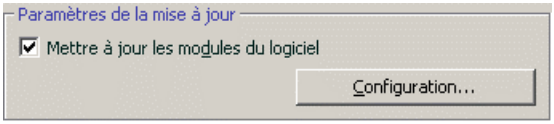


Illustration 31. Sélection des objets de la mise à jour

Pour copier et installer les mises à jour des modules de l'application pendant la mise à jour :

Cochez la case ☑ **Mettre à jour les modules du logiciel** dans la fenêtre de configuration du composant **Mise à jour**.

Si une mise à jour des modules de l'application est présente à ce moment dans la source, le programme 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.

Le mode de mise à jour du logiciel (cf. Illustration 32) désigne la manière dont la mise à jour sera lancée. Choisissez l'un des modes suivants dans le bloc **Mode de lancement** :

- **Automatique**. Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source (cf. point 10.4.1, p. 112). Lorsque Kaspersky Anti-Virus découvre de nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur.

  Si vous vous connectez à Internet à l'aide d'un modem et que vous avez choisi une ressource de réseau en tant que source de mise à jour, Kaspersky Anti-Virus tentera de réaliser la mise à jour selon un intervalle défini lors de la mise à jour antérieure. Les mises à jour réalisées au départ d'une source locales ont lieu à l'intervalle défini lors de la mise à jour précédente. 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 signatures des menaces, des modules de l'application ou des attaques de réseau, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

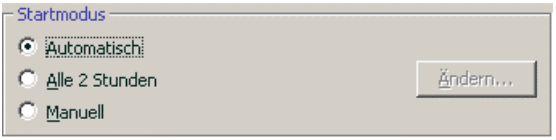


Illustration 32. Sélection du mode de lancement de la mise à jour

- **Toutes les 2 heures.** La mise à jour du logiciel est réalisée selon un horaire défini. Si vous souhaitez activer ce mode, la mise à jour sera réalisée par défaut toutes les 2 heures. Pour composer un autre horaire, cliquez sur **Modifier** à côté du nom du mode et réalisez les modifications souhaitées dans la boîte de dialogue qui s'ouvre (pour de plus amples renseignements, consultez le point 6.5 à la page 70). Ce mode de mise à jour est utilisé par défaut.
- **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 :

- Tout d'abord, une infobulle apparaît (si les notifications ont été activées) au-dessus de l'icône de l'application dans la barre des tâches (cf. point 11.8.1, p. 145);
- Ensuite, le deuxième indice dans la fenêtre principale de l'application vous signale que la protection de l'ordinateur est dépassée (cf. point 5.1.1, p. 45);
- Troisièmement, la section des commentaires et des conseils de la fenêtre principale affiche des conseils sur la mise à jour du logiciel (cf. point 4.3, p. 39).

10.4.3. Configuration des paramètres de connexion

Si vous avez sélectionné les serveurs de mise à jour de Kaspersky Lab ou un serveur FTP ou HTTP quelconque en tant que source de mise à jour, nous vous conseillons de vérifier les paramètres de connexion à Internet.

Tous les paramètres sont regroupés sur l'onglet spécial **Paramètres LAN** (cf. Illustration 33).

Le paramètre ☑ **Utiliser le FTP en mode passif, si possible** est utilisé lorsque vous téléchargez les mises à jour depuis un serveur FTP auquel vous vous connectez en mode passif (par exemple, via un pare-feu). Si la connexion s'effectue en mode actif, vous pouvez désélectionnez cette case.

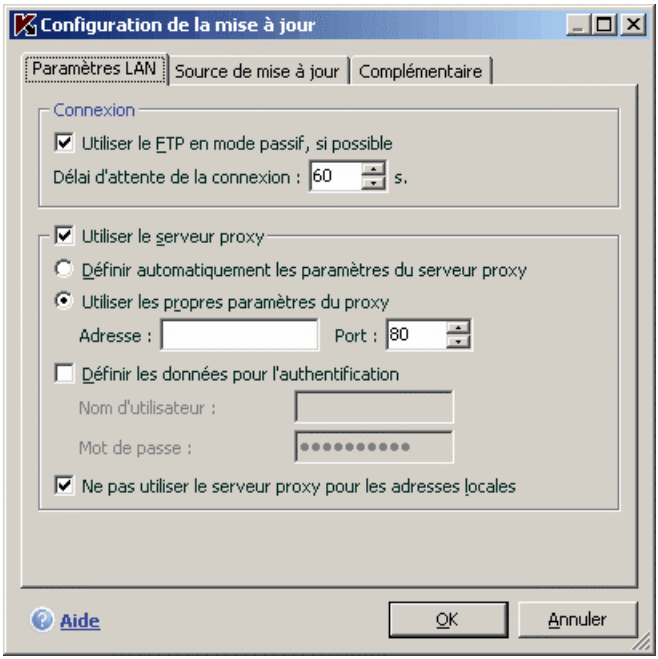


Illustration 33. Configuration des paramètres de réseau de la mise à jour

Précisez dans le champ **Délai d'attente de la connexion (s.)** la durée limite pour établir une connexion avec le serveur de mise à jour. Si la connexion n'a pu être établie à l'issue de cet intervalle, l'application tentera d'établir la connexion avec le serveur de mise à jour suivant. Ce processus se poursuit tant qu'une connexion n'a pu être établie et tant que tous les serveurs disponibles n'ont pas été sollicités.

Si la connexion à Internet s'opère via un serveur proxy, cochez la case ☑ **Utiliser le serveur proxy** et, le cas échéant, configurez les paramètres suivants :

- Sélectionnez les paramètres du serveur proxy qu'il faudra utiliser pour la mise à jour :

  ◉ **Définir automatiquement les parametres du serveur proxy** : Lorsque cette option est sélectionnée, les paramètres du serveur proxy sont définis automatiquement à l'aide du protocole WPAD (Web Proxy Auto-Discovery Protocol). S'il est impossible de définir les paramètres à l'aide de ce protocole, Kaspersky Anti-Virus utilisera alors les paramètres du serveur proxy définis dans Microsoft Internet Explorer.

- **Utiliser les propres paramètres du proxy** : utilise un serveur proxy différent de celui indiqué dans les paramètres de connexion du navigateur. Saisissez l'adresse IP ou le nom symbolique dans le champ **Adresse** et dans le champ **Port**, le port du serveur proxy.

- Indiquez si l'authentification est requise sur le serveur proxy. L'*authentification* est une procédure de vérification des données d'enregistrement de l'utilisateur afin de contrôler l'accès.

  Si la connexion au serveur proxy requiert une authentification, cochez la case ☑ **Définir les données pour l'authentification** et saisissez dans les champs de la partie inférieure le nom et le mot de passe. Dans ce cas, une tentative d'authentification NTLM sera réalisée avant la tentative d'authentification BASIC.

  Si la case n'est pas cochée ou si les données ne sont pas définies, le système procédera à une tentative d'utilisation NTML en utilisant le compte utilisateur au nom duquel la mise à jour est lancée (cf. point 6.4, p. 68).

  Si l'autorisation sur le serveur proxy est indispensable et que vous n'avez pas saisi le nom et le mot de passe ou que les données saisies ont été rejetées pour une raison quelconque par le serveur, une fenêtre de saisie du nom et du mot de passe pour l'autorisation apparaîtra au lancement de la mise à jour. Si l'autorisation réussit, le nom et le mot de passe saisis seront utilisés à l'avenir. Dans le cas contraire, il faudra à nouveau saisir les paramètres d'autorisation.

Afin de ne pas utiliser le serveur proxy lors de la mise à jour depuis un répertoire local ou de réseau, désélectionnez la case ☑ **Ne pas utiliser le serveur proxy pour les adresses locales**.

10.4.4. Copie des mises à jour

Le service de copie des mises à jour permet d'optimaliser la charge du réseau de l'entreprise. La copie s'opère en deux étapes :

1. Un des ordinateurs du réseau obtient les mises à jour pour l'application et les signatures des menaces depuis les serveurs de Kaspersky Lab ou depuis 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.

Pour activer la copie des mises à jour, cochez la case ☑ **Copier dans le répertoire** de l'onglet **Complémentaire** (cf. Illustration 34) et dans le champ

situé en dessous, indiquez le chemin d'accès au dossier partagé dans lequel les mises à jour seront sauvegardées. Le chemin d'accès peut être saisi manuellement ou dans la fenêtre qui s'ouvre dès que vous aurez cliqué sur **Parcourir…**. Si la case est cochée, les nouvelles mises à jour seront copiées automatiquement dans ce répertoire.

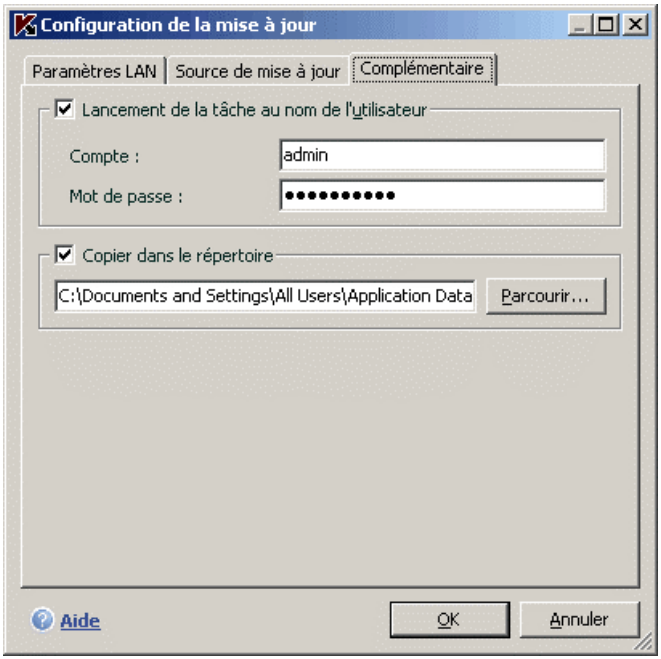


Illustration 34. Configuration du service de copie des mises à jour

N'oubliez pas que Kaspersky Anti-Virus 6.0 reçoit des serveurs de Kaspersky Lab uniquement les fichiers de mise à jour pour la version 6.0. Si vous souhaitez copier les mises à jour pour d'autres applications de Kaspersky Lab, il est conseillé d'utiliser Kaspersky Administration Kit.

Afin que les autres ordinateurs du réseau puissent utiliser les fichiers de mise à jour du dossier partagé, il faut réaliser les opérations suivantes :

1. Donner l'accès à ce dossier.
2. Désigner le dossier partagé en tant que source de la mise à jour dans les paramètres de la mise à jour des ordinateurs du réseau.

10.4.5. Actions exécutées après la mise à jour du logiciel

Chaque mise à jour des signatures des menaces contient de nouvelles définitions capables de protéger votre ordinateur contre les menaces récentes.

Les experts de Kaspersky Lab vous recommandent d'analyser *les objets en quarantaine et les objets de démarrage directement* après la mise à jour.

Pourquoi ces objets et pas d'autres ?

La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infectés (cf. point 11.1, p. 123). Il se peut que la version actualisée des signatures des menaces de Kaspersky Anti-Virus puisse reconnaître et neutraliser le danger.

Par défaut, le logiciel analyse les objets en quarantaine après chaque mise à jour des signatures des menaces connues. Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et être à nouveau utilisés.

Pour annuler l'analyse des objets en quarantaine, désélectionnez ☑ la case **Analyser les fichiers en quarantaine** dans le bloc **Action après la mise à jour**.

Les objets de démarrage représentent un secteur critique dans le domaine de la sécurité de votre ordinateur. Si ce secteur est infecté par un programme malicieux, il se peut que vous ne parveniez plus à lancer le système d'exploitation. Kaspersky Anti-Virus propose une tâche d'analyse des objets de démarrage (cf. Chapitre 8, p. 89). Il est conseillé de configurer le lancement automatique de cette tâche après chaque mise à jour des signatures des menaces (cf. point 6.5, p. 70).

CHAPITRE 11. POSSIBILITES COMPLEMENTAIRES

En plus de protéger vos données, le logiciel propose des services complémentaires qui élargissent les possibilités de Kaspersky Anti-Virus.

Au cours de ses activités, le logiciel place certains objets dans des répertoires spéciaux. L'objectif suivi est d'offrir une protection maximale avec un minimum de pertes.

- Le dossier de sauvegarde contient les copies des objets qui ont été modifiés ou supprimés par Kaspersky Anti-Virus (cf. point 11.2, p. 127). Si un objet qui contenait des informations importantes n'a pu être complètement préservé pendant le traitement antivirus, vous pourrez toujours le restaurer au départ de la copie de sauvegarde.
- La quarantaine contient les objets potentiellement infectés qui n'ont pas pu être traités avec les signatures actuelles des menaces (cf. point 11.1, p. 123).

Il est conseillé de consulter régulièrement la liste des objets ; certains ne sont peut-être plus d'actualité tandis que d'autres peuvent être restaurés.

Une partie des services est orientée vers l'assistance pour l'utilisation du logiciel, par exemple :

- Le Service d'assistance technique offre une aide complète pour l'utilisation de Kaspersky Anti-Virus (cf. point 11.5, p. 139). Les experts de Kaspersky Lab ont tenté d'inclure tous les moyens possibles d'apporter cette assistance : assistance en ligne, forum de questions et de suggestions des utilisateurs, etc.
- Le service de notification des événements permet de configurer la notification aux utilisateurs des événements importants dans le fonctionnement de Kaspersky Anti-Virus (cf. point 11.8.1, p. 145). Il peut s'agir d'événements à caractère informatif ou d'erreurs qui nécessitent une réaction immédiate et dont il faut avoir conscience.
- L'autodéfense du logiciel et la restriction de l'accès protège les propres fichiers du logiciel contre les modifications réalisées par des personnes mal intentionnées, interdit l'administration externe du logiciel par des services et introduit des restrictions d'administration du serveur sur l'exécution de certaines actions à l'aide de Kaspersky Anti-Virus (cf. point 11.8.2, p. 148). Par exemple, une modification du niveau de

protection peut fortement influencer la sécurité des données sauvegardées sur votre ordinateur.

- Le service d'administration des clés de licence vous permet d'obtenir des informations complémentaires sur la licence utilisée, d'activer votre copie du logiciel et d'administrer les fichiers des clés de licence (cf. point 11.5, p. 139).

Le logiciel propose également une aide (cf. point 11.4, p. 138) détaillée et des rapports complets (cf. point 11.3, p. 130) sur le fonctionnement de l'Antivirus Fichiers et l'exécution de toutes les tâches liées à la recherche de virus ou à la mise à jour.

Vous pouvez également modifier l'aspect extérieur de Kaspersky Anti-Virus et configurer les paramètres de l'interface actuelle (cf. point 11.7, p. 143).

Examinons en détails ces différents services.

11.1. Quarantaine pour les objets potentiellement infectés

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 signatures des menaces connues 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 signatures, 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 signatures des menaces 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 le classe comme un objet potentiellement infecté.

L'analyseur heuristique de code détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est relativement efficace et donne très rarement de fausses alertes.

L'objet potentiellement infecté peut-être identifié et mis en quarantaine par l'antivirus de fichiers.

Vous pouvez vous-même placer un objet en quarantaine en cliquant sur **Quarantaine** dans la notification spéciale qui apparaît à l'écran suite à la découverte d'un objet potentiellement infecté.

Lors d'une mise en quarantaine, le fichier est déplacé et non pas simplement copié : l'objet est supprimé du disque ou du message électronique et conservé dans le dossier de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

11.1.1. Manipulation des objets en quarantaine

Le nombre total d'objets placés en quarantaine est repris dans les **Rapports** de la section **Service**. Dans la partie droite de la fenêtre principale, on retrouve le bloc spécial **Quarantaine** avec les informations suivantes :

- Le nombre d'objets potentiellement infectés découverts par Kaspersky Anti-Virus;
- La taille actuelle de la quarantaine.

Il est possible ici de supprimer tous les objets de la quarantaine à l'aide du bouton **Purger**. N'oubliez pas que cette action entraîne la suppression des objets du dossier de sauvegarde et des fichiers de rapport.

Pour manipuler les objets en quarantaine :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Quarantaine**.

Vous pouvez réaliser les opérations suivantes dans l'onglet quarantaine (cf. Illustration 35) :

- Mettre en quarantaine un fichier que vous croyez être infecté par un virus et qui n'aurait pas été découvert par le logiciel. Cliquez pour ce faire sur **Ajouter…** et sélectionnez le fichier souhaité. Il sera ajouté à la liste sous le signe *Ajouté par l'utilisateur*.

Si le fichier, qui s'avère sain après l'analyse suivante, a été mis manuellement en quarantaine, son état ne deviendra pas immédiatement *ok*. Cela se produira uniquement si l'analyse a lieu un certain temps après la mise en quarantaine du fichier (au moins trois jours).

- Analyser et réparer à l'aide des signatures actuelles des menaces connues tous les objets potentiellement infectés qui se trouvent en quarantaine. Il suffit simplement de cliquer sur **Analyser tous**

  L'état de chaque objet en quarantaine après l'analyse et la réparation peut être soit *infecté*, *probablement infecté*, *fausse alerte, ok, etc*. Dans ce cas, un message de circonstance apparaît à l'écran et propose différents traitements possibles.

  L'état *infecté* signifie que l'objet est bien infecté mais qu'il n'a pas pu être réparé. Il est recommandé de supprimer de tels objets.

  Tous les objets dont l'état est qualifié de *fausse alerte* peuvent être restaurés sans crainte car leur état antérieur, à savoir *Probablement infecté* n'a pas été confirmé par le logiciel lors de la nouvelle analyse.

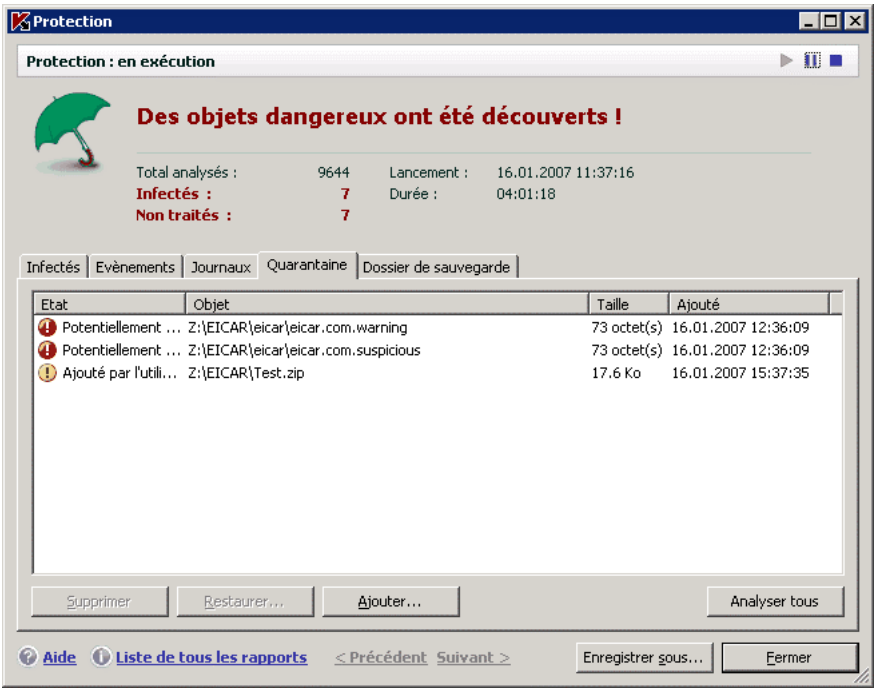


Illustration 35. Liste des objets en quarantaine

- Restaurer les fichiers dans un répertoire défini ou dans le répertoire d'origine où ils se trouvaient avant d'être mis en quarantaine. Pour restaurer un objet, sélectionnez-le dans la liste et cliquez sur **Restaurer…**. Pour restaurer des objets issus d'archives, de bases de données de messagerie électronique ou de courriers individuels et placés en quarantaine, il est indispensable de désigner le répertoire dans lequel ils seront restaurés.

> Conseil
>
> Nous vous conseillons de restaurer uniquement les objets dont l'état correspond à *fausse alerte, ok ou réparé*. La restauration d'autres types d'objets pourrait entraîner l'infection de votre ordinateur !

- Supprimer n'importe quel objet ou groupe d'objets de la quarantaine. Supprimez uniquement les objets qui ne peuvent être réparés. Afin de supprimer un objet, sélectionnez-le dans la liste puis cliquez sur **Supprimer**.

11.1.2. Configuration de la quarantaine

Vous pouvez configurer les paramètres de constitution et de fonctionnement de la quarantaine, à savoir :

- Définir le mode d'analyse automatique des objets en quarantaine après chaque mise à jour des signatures des menaces (pour de plus amples informations, consultez le point 10.4.4 à la page 119)

  > Attention !
  >
  > Le logiciel ne peut analyser les objets en quarantaine directement après la mise à jour des signatures des menaces si vous utilisez la quarantaine à ce moment.

- Définir la durée de conservation maximum des objets en quarantaine.

  Par défaut, la durée de conservation des objets en quarantaine est fixée à 30 jours au terme desquels les objets sont supprimés. Vous pouvez modifier la durée de conservation des objets potentiellement infectés ou supprimer complètement cette limite.

  Pour ce faire :

  1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
  2. Sélectionnez **Rapports** dans l'arborescence.
  3. Définissez dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. Illustration 36) le délai de conservation au terme duquel les objets seront automatiquement supprimés.

Illustration 36. Configuration de la conservation des objets en quarantaine

11.2. 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.

11.2.1. Manipulation des copies de sauvegarde

Le nombre total de copies de sauvegarde placées dans le dossier est repris dans les **Rapports** de la section **Services**. Dans la partie droite de la fenêtre principale, on retrouve le bloc spécial **Dossier de sauvegarde** avec les informations suivantes :

- Le nombre de copies de sauvegarde créées par Kaspersky Anti-Virus;
- La taille actuelle du dossier.

Il est possible ici de supprimer toutes les copies du dossier à l'aide du bouton **Purger…**. N'oubliez pas que cette action entraîne la suppression des objets du dossier de quarantaine et des fichiers de rapport.

Pour accéder aux copies des objets dangereux :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Dossier de sauvegarde**.

La partie centrale de l'onglet (cf. Illustration 37) reprend la liste des copies de sauvegarde. Les informations suivantes sont fournies pour chaque copie : nom complet de l'objet avec indication du chemin d'accès à son emplacement d'origine, l'état de l'objet attribué suite à l'analyse et sa taille.

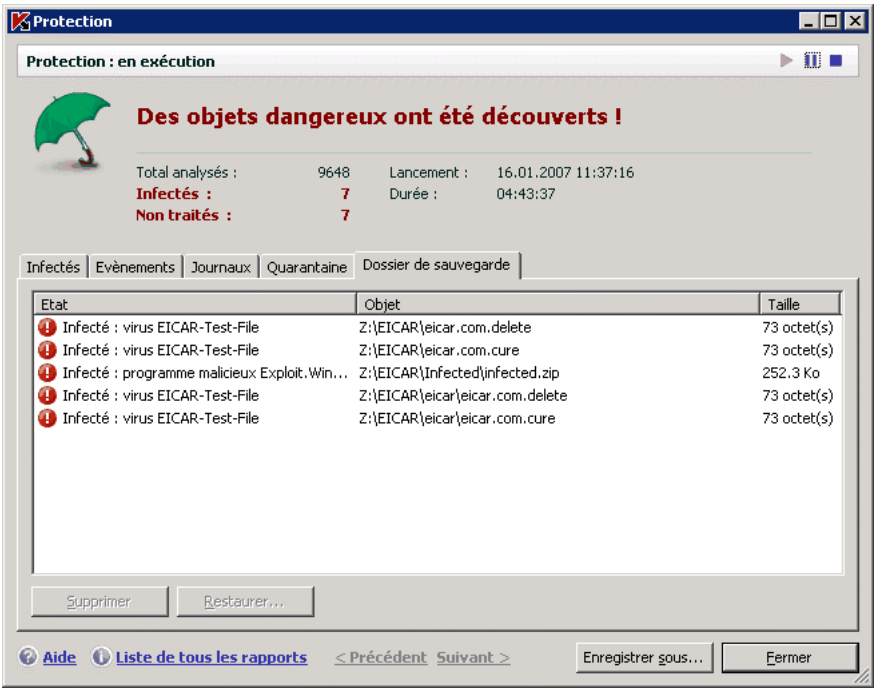


Illustration 37. Copies de sauvegarde des objets supprimés ou réparés

Vous pouvez restaurer les copies sélectionnées à l'aide du bouton **Restaurer…**. L'objet est restauré au départ du dossier de sauvegarde avec le même nom qu'il avait avant la réparation.

Si l'emplacement d'origine contient un objet portant le même nom (cette situation est possible en cas de restauration d'un objet dont la copie avait été créée avant la réparation), l'avertissement de rigueur apparaîtra à l'écran. Vous pouvez modifier l'emplacement de l'objet restauré ainsi que son nom.

Nous vous recommandons de rechercher la présence d'éventuels virus directement après la restauration. Il sera peut-être possible de le réparer avec les signatures les plus récentes tout en préservant son intégrité.

Nous ne vous recommandons pas de restaurer les copies de sauvegarde des objets si cela n'est pas nécessaire. Cela pourrait en en effet entraîner l'infection de votre ordinateur.

Il est conseillé d'examiner fréquemment le contenu du dossier et de le nettoyer à l'aide du bouton **Supprimer**. Vous pouvez également configurer le logiciel afin qu'il supprime lui-même les copies les plus anciennes du répertoire (cf. point 11.2.2, p. 130).

11.2.2. Configuration des paramètres du dossier de sauvegarde

Vous pouvez définir la durée maximale de conservation des copies dans le dossier de sauvegarde.

Par défaut, la durée de conservation des copies des objets dangereux est fixée à 90 jours au terme desquels les copies sont supprimées. Vous pouvez modifier la durée de conservation maximale des copies ou supprimer complètement toute restriction. Pour ce faire :

1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Rapports** dans l'arborescence.
3. Définissez le délai de conservation des copies de sauvegarde dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. Illustration 36) dans la partie droite de la fenêtre.

11.3. Utilisation des rapports

Le fonctionnement de l'Antivirus Fichiers de Kaspersky Anti-Virus et l'exécution de chaque tâche liée à la recherche de virus et à la mise à jour est consignée dans un rapport.

Le total des rapports composés par le logiciel en ce moment ainsi que leur taille totale (en octets) sont repris dans les **Rapports** de la section **Services** de la fenêtre principale du logiciel. Ces informations sont reprises dans le bloc **Rapports**.

Pour consulter les rapports :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Rapports**.

La fenêtre s'ouvre sur l'onglet **Rapports** (cf. Illustration 38). Vous y verrez les derniers rapports sur l'Antivirus Fichiers et les tâches antivirus et de mise à jour lancées au cours de cette session de Kaspersky Anti-Virus. Le résultat du fonctionnement est affiché en regard l'Antivirus Fichiers ou de la tâche. Exemple, *interrompu(e)* ou *terminée.* Si vous souhaitez consulter l'historique complet des

rapports pour la session en cours, cochez la case ☑ **Afficher l'historique des rapports**.

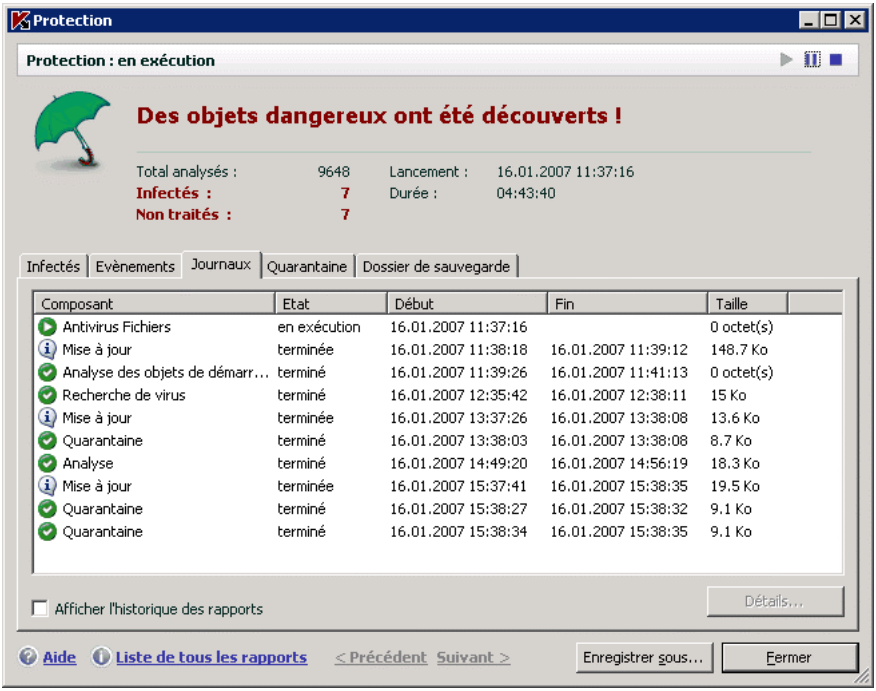


Illustration 38. Rapports sur le fonctionnement des composants du programme

Pour voir tous les événements consignés dans le rapport et relatifs à l'Antivirus Fichiers ou à l'exécution d'une tâche :

sélectionnez l'Antivirus Fichiers ou de la tâche dans l'onglet **Rapports** et cliquez sur **Détails…**.

Cette action entraîne l'ouverture d'une fenêtre contenant des informations détaillées sur le fonctionnement de l'Antivirus Fichiers ou 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:

- L'onglet **Infectés** contient la liste des objets dangereux découverts par le logiciel ou la tâche de recherche de virus.
- **Evénements** illustre les événements survenus pendant l'exécution de la tâche ou le fonctionnement de l'Antivirus Fichiers

- L'onglet **Statistiques** reprend les statistiques détaillées de tous les objets analysés.
- L'onglet **Paramètres** reprend les paramètres qui définissent le fonctionnement de l'Antivirus Fichiers, de la recherche de virus ou de la mise à jour des signatures des menaces.
- L'onglet **Blocage de l'utilisateurs** reprend la liste des utilisateurs dont les ordinateurs ont été bloqués lors d'une tentative de copie d'un fichier infecté ou potentiellement infecté sur le serveur.

Tout le rapport peut être exporter dans un fichier au format texte. Cela peut-être utile lorsque vous ne parvenez pas à résoudre vous même un problème survenu pendant l'exécution d'une tâche ou le travail de l'Antivirus Fichiers et que vous devez vous adressez au service d'assistance technique . Vous devrez envoyer le rapport au format texte afin que nos experts puissent étudier le problème en profondeur et le résoudre le plus vite possible.

Pour exporter le rapport au format texte :

cliquez sur **Enregistrer sous** et indiquez où vous souhaitez enregistrer le fichier.

Lorsque vous en avez terminé avec le rapport, cliquez sur **Fermer**.

En plus des boutons **Paramètres** et **Statistiques**, ces onglets présentent également le bouton **Actions** que vous pouvez réaliser sur les objets de la liste. Ce bouton ouvre un menu contextuel qui reprend les points suivants (le contenu de la liste varie en fonction du rapport consulté; la liste ci-dessus est une énumération globale de tous ces points):

Réparer : tentative de réparation de l'objet dangereux. S'il est impossible de neutraliser l'objet, vous pouvez le laisser dans la liste en vue d'un traitement différé à l'aide des signatures des menaces actualisées ou le supprimer. Vous pouvez appliquer cette action à un seul objet de la liste ou à une sélection d'objets.

Supprimer de la liste : supprime l'enregistrement relatif à la découverte de l'objet.

Ajouter à la zone de confiance : ajoute l'objet en tant qu'exclusion de la protection. Ce choix entraîne l'ouverture de la fenêtre de la règle d'exclusion pour cet objet.

Réparer tous : neutralise tous les objets de la liste. Kaspersky Anti-Virus tente de traiter les objets à l'aide des signatures des menaces.

Purger : supprime le rapport sur les objets découverts. Tous les objets dangereux découverts demeurent sur l'ordinateur.

Afficher : ouvre Microsoft Windows Explorer au répertoire qui contient l'objet en question**.**

Consulter www.viruslist.com/fr : ouvre la description de l'objet dans l'Encyclopédie des virus sur le site de Kaspersky Lab.

Rechercher sur www.google.com : recherche d'informations relatives à l'objet à l'aide du moteur de recherche.

Rechercher : définit les termes de recherche des objets dans la liste en fonction du nom ou de l'état.

Vous pouvez également trier les informations présentées en ordre croissant ou décroissant pour chaque colonne.

Le traitement des objets dangereux découverts par Kaspersky Anti-Virus s'opère à l'aide du bouton **Réparer** (pour un objet ou une sélection d'objets) ou **Réparer tous** (pour le traitement de tous les objets de la liste). Le traitement de chaque objet s'accompagne d'un message qui vous permet de choisir les actions ultérieures à appliquer à cet objet.

Si vous cochez la case ☑ **Appliquer à tous les cas similaires** dans le message, alors l'action sélectionnée sera appliquée à tous les objets au statut identique.

11.3.1. Configuration des paramètres du rapport

Afin de configurer les paramètres de constitution et de conservation des rapports:

Ouvrez la boîte de dialogue de configuration de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale du logiciel.

1. Sélectionnez **Rapports** dans l'arborescence des paramètres.
2. Dans le bloc **Journaux** (cf. Illustration 39), procédez à la configuration requise :
   - Consignez ou non les événements à caractère informatif. En règle générale, ces événements ne jouent pas un rôle crucial dans la protection. Afin de les consigner dans le rapport, cochez la case ☑ **Consigner les événements non critiques**;
   - Activez 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. Si la case ☑ **Conserver uniquement les événements courants** est cochée, les informations reprises dans le rapport seront actualisées à chaque redémarrage de la tâche. Toutefois, seules les informations relatives aux événements non critiques seront écrasées.

- Définissez le délai de conservation des rapports. Par défaut, ce délai est établi à 90 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.

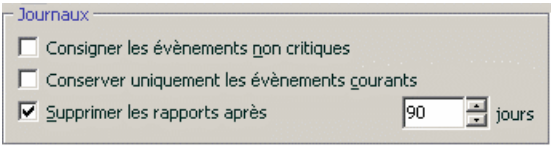


Illustration 39. Configuration des paramètres de constitution des rapports

11.3.2. Onglet Infectés

Cet onglet (cf. Illustration 40) contient la liste des objets dangereux découverts par Kaspersky Anti-Virus. Le nom complet et le statut attribué par le logiciel après l'analyse/le traitement est indiqué pour chaque objet.

Afin que la liste affiche, en plus des objets dangereux, les objets qui ont été réparés, cochez la case **Afficher les objets réparés**.

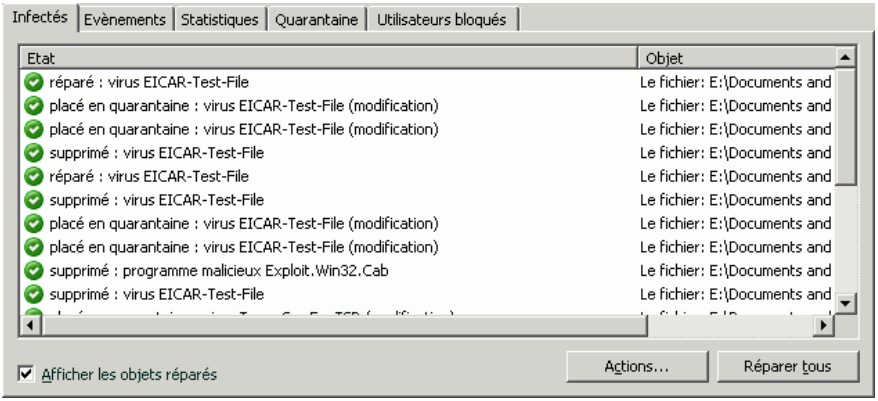


Illustration 40. Liste des objets dangereux découverts

Le traitement des objets dangereux découverts par Kaspersky Anti-Virus s'opère à l'aide du bouton **Réparer** (pour un objet ou une sélection d'objets) ou **Réparer tous** (pour le traitement de tous les objets de la liste). Le traitement de chaque objet s'accompagne d'un message qui vous permet de choisir les actions ultérieures à appliquer à cet objet.

Si vous cochez la case ☑ **Appliquer à tous les cas similaires** dans le message, alors l'action sélectionnée sera appliquée à tous les objets au statut identique.

11.3.3. Onglet Evénements

Cet onglet (cf. Illustration 41) reprend la liste de tous les événements importants survenus pendant le fonctionnement de l'Antivirus Fichiers, lors de l'exécution d'une tâche liée à la recherche de virus ou de la mise à jour des signatures des menaces.

Les événements prévus sont :

Evénements critiques. Evénements critiques qui indiquent un problème dans le fonctionnement du logiciel ou une vulnérabilité dans la protection de l'ordinateur. Exemple : *virus découvert, échec de fonctionnement*.

Evénements importants. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le fonctionnement du logiciel. Exemple : *interruption*.

Evénements informatifs. Evénements à caractère purement informatif qui ne contiennent aucune information cruciale. Exemple : *ok, non traité*. Ces événements sont repris dans le journal des événements uniquement si la case ☑ **Afficher tous les événements** est cochée.

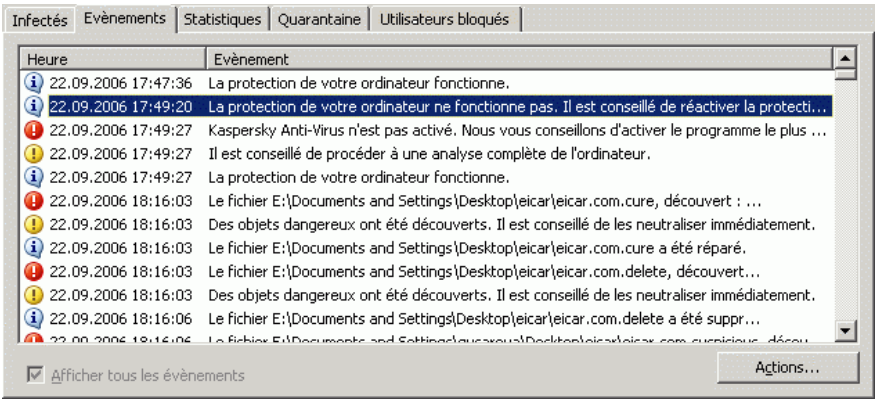


Illustration 41. Evénements survenus pendant

Le format de présentation de l'événement dans le journal des événements peut varier en fonction du composant ou de la tâche. Ainsi, pour la mise à jour, les informations reprises sont :

- Le nom de l'événement;
- Le nom de l'objet pour lequel cet événement a été consigné;
- L'heure à laquelle l'événement est survenu;
- La taille du fichier téléchargé.

Pour les tâches liées à la recherche de virus, le journal des événements contient le nom de l'objet analysé et le statut attribué à l'objet suite à l'analyse/au traitement.

11.3.4. Onglet Statistiques

Cet onglet reprend les statistiques détaillées du fonctionnement de l'Antivirus Fichiers ou de l'exécution des tâches liées à la recherche de virus (cf. Illustration 42). Vous pouvez voir :

- Le nombre d'objets soumis à l'analyse antivirus pendant la session actuelle de l'Antivirus Fichiers ou lors de l'exécution de la tâche. Ce chiffre reprend le nombre d'archives, de fichiers compactés, de fichiers protégés par un mot de passe et d'objets corrompus analysés.
- Le nombre d'objets dangereux découverts, le nombre d'entre eux qui n'a pas pu être réparés, le nombre supprimés et le nombre mis en quarantaine.

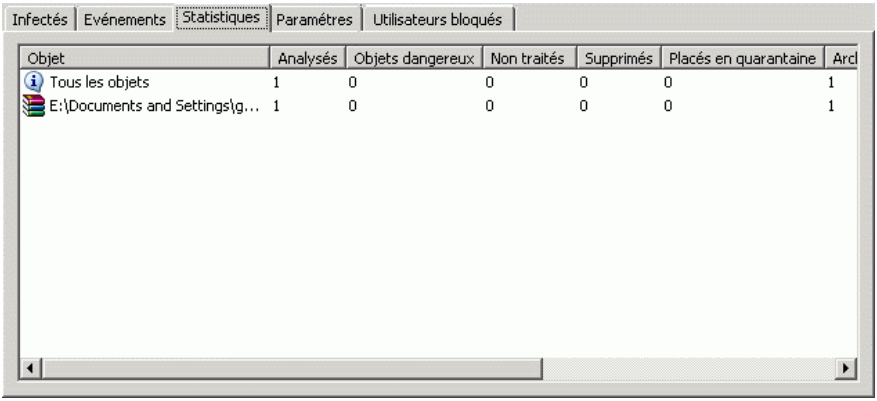


Illustration 42. Statistique du composant

11.3.5. Onglet Paramètres

Cet onglet (cf. Illustration 43) présente tous les paramètres qui définissent le fonctionnement de l'Antivirus Fichiers ou l'exécution des tâches liées à la recherche de virus ou à la mise à jour. Vous pouvez voir le niveau de protection offert par l'Antivirus Fichiers ou le niveau de protection défini pour la recherche de virus, les actions exécutées sur les objets dangereux, les paramètres appliqués à la mise à jour, etc. Pour passer à la configuration des paramètres, cliquez sur Modifier les paramètres.

Pour la recherche de virus, vous pouvez configurer des conditions complémentaires d'exécution :

- Etablir la priorité d'exécution d'une tâche d'analyse en cas de charge du processeur. Par défaut, la case ☑ **Céder les ressources aux autres applications** est cochée. Le programme surveille la charge du processeur et des sous-système des disques pour déceler l'activité d'autres applications. Si l'activité augmente sensiblement et gêne le fonctionnement normal de l'application de l'utilisateur, le programme réduit l'activité liée à l'analyse. Cela se traduit par une augmentation de la durée de l'analyse et le transfert des ressources aux applications de l'utilisateur.

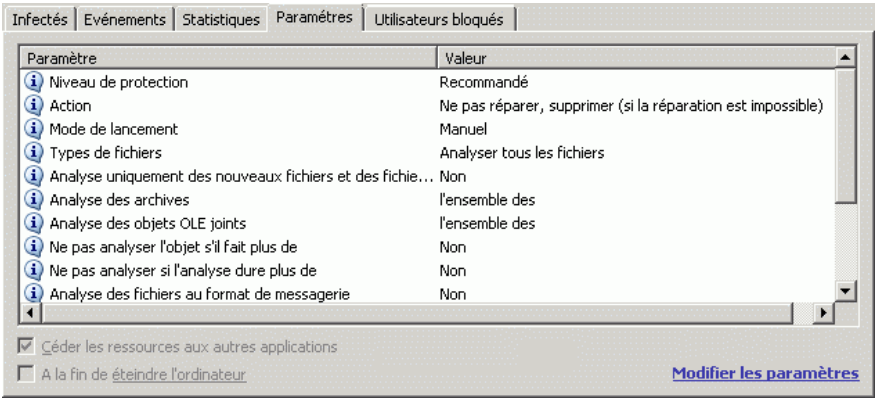


Illustration 43. Paramètres de fonctionnement du composant

- Définir le mode de fonctionnement de l'ordinateur après la recherche de virus. Vous pouvez configurer la désactivation/le redémarrage de l'ordinateur ou le passage en mode de veille. Pour opérer votre choix, cliquez avec le bouton gauche de la souris sur le lien jusqu'à ce qu'il prenne la valeur voulue.

11.3.6. Onglet *Utilisateurs bloqués*

La liste des utilisateurs dont l'accès au serveur a été provisoirement suspendu est reprise sur l'onglet **Utilisateurs bloqués** (cf. Illustration 44). Le blocage concerne chaque ordinateur au départ duquel la tentative de copie d'un objet infecté ou potentiellement infecté sur le serveur a été réalisée. Le blocage peut être appliqué en plus des autres actions liées au traitement de cet objet (suppression ou réparation).

L'onglet indique les ordinateurs bloqués, la date et l'heure du blocage et le nombre d'heures restant avant le déblocage.

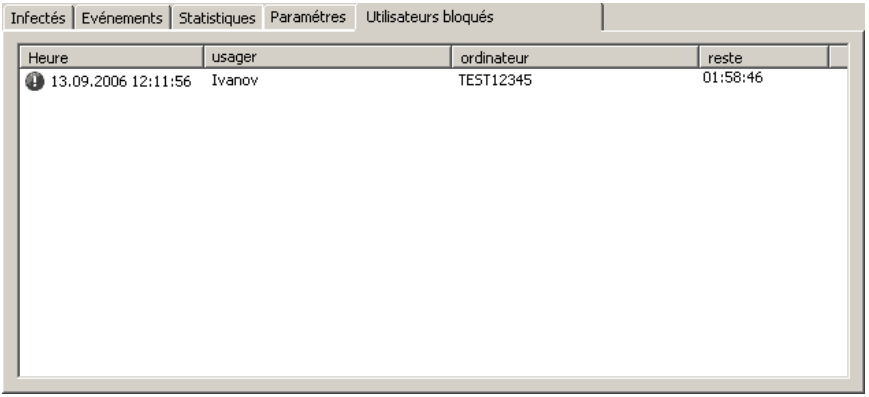


Illustration 44. Liste des utilisateurs bloqués

11.4. Informations générales sur le logiciel

La section **Services** de la fenêtre principale affiche des informations générales sur le logiciel (cf. Illustration 45).

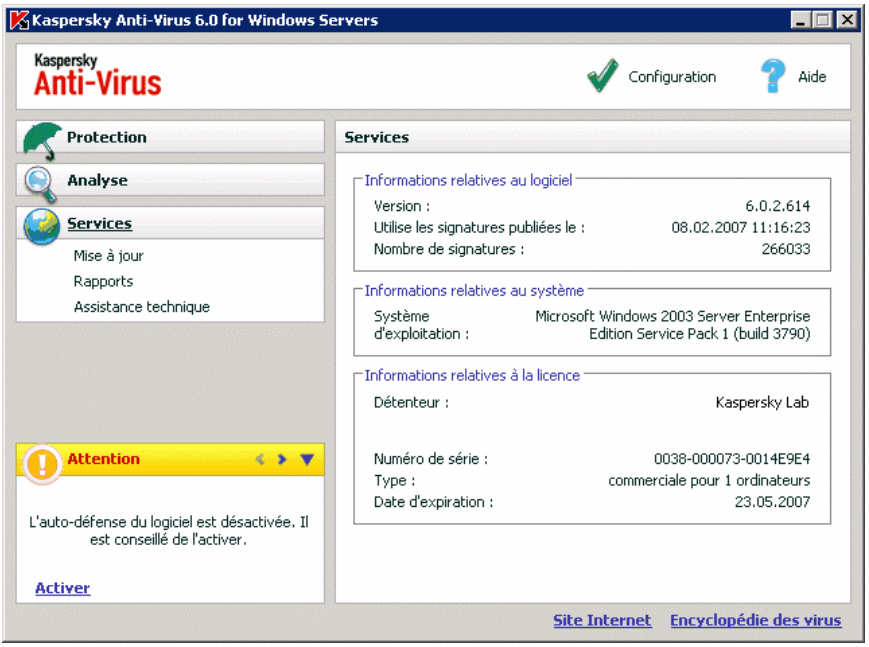


Illustration 45. Informations relatives au logiciel, à la licence et au système sur lequel il est installé

Ces informations sont scindées en trois blocs :

- La section **Informations relatives au logiciel** affiche la version du logiciel, la date de la dernière mise à jour et la quantité de menaces connues à ce moment.
- Le bloc **Informations relatives au système** reprend de brèves informations sur le système d'exploitation installé sur votre ordinateur.
- La section **Informations relatives à la licence** fournit des informations sur votre licence d'utilisation de Kaspersky Anti-Virus.

Toutes ces informations sont nécessaires lors des contacts avec le service d'Assistance technique de Kaspersky Lab (cf. point 11.5, p. 139).

11.5. Administration des licences

Kaspersky Anti-Virus fonctionne grâce à une *clé de licence*. La clé vous est attribuée après l'achat du logiciel et elle vous donne le droit d'utiliser l'application dès l'installation de la clé.

Sans la clé de licence et sans activation de la version d'évaluation, Kaspersky Anti-Virus ne réalisera qu'une seule mise à jour. Les mises à jour ultérieures ne seront pas téléchargées.

Si la version d'évaluation a été activée, Kaspersky Anti-Virus ne fonctionnera plus une fois le délai de validité écoulé.

Une fois la licence commerciale expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettra à jour les signatures des menaces. Vous pourrez toujours analyser le serveur à l'aide de la recherche de virus et utiliser l'Antivirus Fichiers, mais uniquement sur la base des signatures des menaces 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. Au cours des deux semaines suivantes, le programme affichera à chaque démarrage le message de circonstance.

Afin de renouveler la licence, vous devez absolument obtenir et installer une nouvelle clé de licence pour l'application et indiquer le code d'activation de l'application. Pour ce faire :

Contactez la société où vous avez acheté le logiciel et achetez une clé de licence pour l'utilisation du logiciel ou un code d'activation.

ou:

Achetez une nouvelle clé de licence ou un code d'activation directement chez Kaspersky Lab en cliquant sur le lien Activer dans la fenêtre des clés de licence (cf. Illustration 46). Remplissez le formulaire qui s'affiche dans notre site. Dès que le paiement aura été reçu, un message contenant un lien sera envoyé à l'adresse électronique indiquée dans le formulaire de commande. Ce lien vous permettra de télécharger la clé de licence ou d'obtenir le code d'activation de l'application.

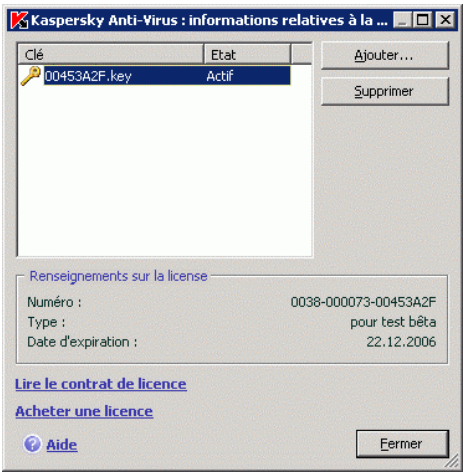


Illustration 46. Informations relatives à la licence

Les informations relatives à la clé de licence utilisée figurent dans le bloc **Informations relatives à la licence** de la section **Services** dans la fenêtre principale de l'application. Pour ouvrir la fenêtre d'administration des licences, cliquez avec le bouton gauche de la souris n'importe où dans le bloc. La fenêtre qui s'ouvre (cf. Illustration 46) vous permet de consulter les informations sur la clé active, d'en ajouter une ou de la supprimer

Lorsque vous sélectionnez une clé dans la liste du bloc **Informations relatives à la licence**, vous pourrez voir le numéro de la clé, son type et sa durée de validité. Pour ajouter une nouvelle clé de licence, cliquez sur le bouton **Ajouter…** et activez l'application à l'aide de l'Assistant d'activation (cf. point 11.5, p. 139). Pour supprimer une clé de la liste, cliquez sur **Supprimer**.

Afin de prendre connaissance des termes du contrat de licence, cliquez sur le lien Lire le contrat de licence. Afin d'acheter une nouvelle clé via le site Internet de Kaspersky Lab, cliquez sur Acheter une licence.

11.6. Service d'assistance technique aux utilisateurs

Kaspersky Anti-Virus vous offre un large éventail de possibilités pour régler les problèmes et les questions liées à l'utilisation du logiciel. Ils sont tous repris sous **Assistance technique** (cf. Illustration 47) dans la section **Services**.

En fonction du problème que vous voulez résoudre, nous vous proposons plusieurs services :

Base de connaissance. Il s'agit également d'une rubrique distincte du site Web de Kaspersky Lab qui contient les recommandations du service d'assistance technique sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées.
Site internet : http://kb.kaspersky.fr

Assistance Technique en ligne. Cette solution permet une approche pas à pas de la définitions du souci rencontré afin de vous offrir la solution adéquate.

Site internet : http://case.kaspersky.fr

Site du Support Technique. Ce site regroupe toutes les informations concernant les outils d'information vous permettant de nous contacter par téléphone ou par email, vous y trouverez aussi des sites associés, des données sur les mises à jour, etc.

Site internet : http://support.kaspersky.fr

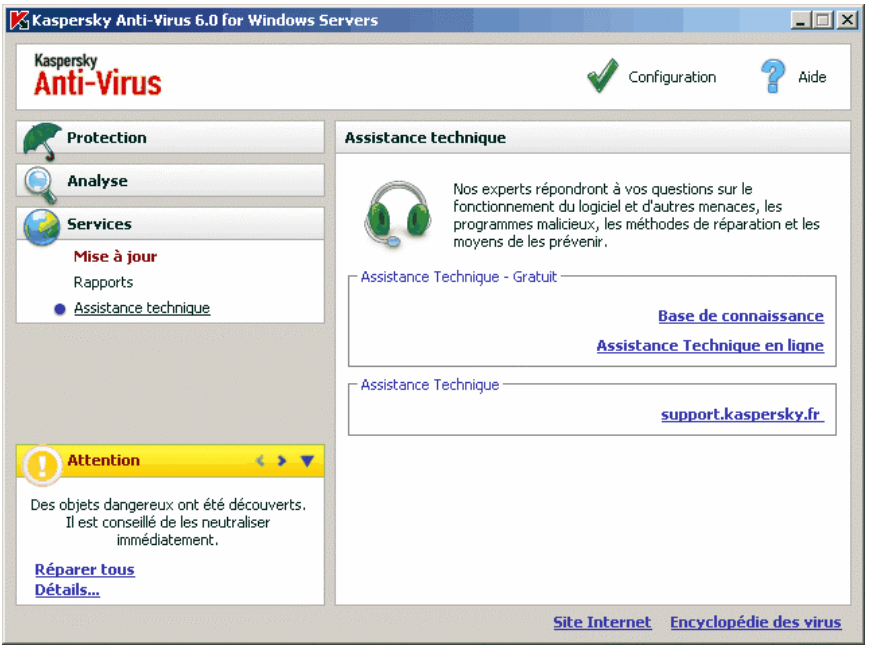


Illustration 47. Informations relatives à l'assistance technique

11.7. Configuration de l'interface de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet de modifier l'aspect extérieur du logiciel à l'aide de divers éléments graphiques et d'une palette de couleurs. Il est également possible de configurer l'utilisation des éléments actifs de l'interface tels que l'icône de l'application dans la barre des tâches et les infobulles.

Pour configurer l'interface du logiciel :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Anti-Virus à l'aide du lien Configuration de la fenêtre principale.
2. Sélectionnez **Apparence** dans le groupe **Services** de l'arborescence des paramètres du logiciel (cf. Illustration 48).

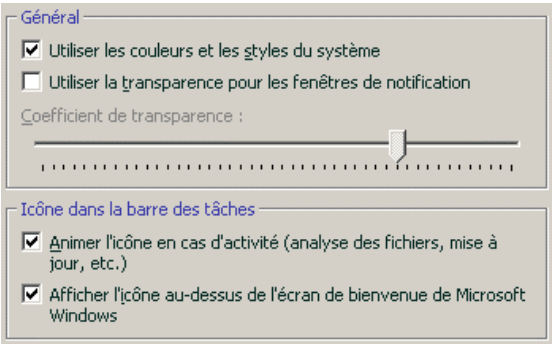


Illustration 48. Configuration de l'interface du programme

Dans la partie droite de la fenêtre des paramètres, vous pouvez décider d':

- Afficher ou non l'indicateur de la protection de Kaspersky Anti-Virus lors du démarrage du système d'exploitation.

  Par défaut, cet indicateur apparaît dans le coin supérieur droit de l'écran au moment du démarrage du logiciel. Il indique que la protection de l'ordinateur contre n'importe quelle menace est activée. Si vous ne souhaitez pas afficher l'indicateur de protection, désélectionnez la case ☑ **Afficher l'icône au-dessus de l'écran de bienvenue de Microsoft Windows**.

- Animer ou nom l'icône de l'application dans la barre des tâches.

  L'icône de l'application dans la barre des tâches varie en fonction de l'opération exécutée. Si vous ne souhaitez pas utiliser l'animation,

désélectionnez la case **Animer l'icône en cas d'activité**. Dans ce cas, l'icône indiquera uniquement l'état de la protection de votre ordinateur. Lorsque la protection est activée, l'icône est en couleur. Lorsque la protection est suspendue ou désactivée, l'icône apparaît est grisée.

- Degré de transparence des infobulles.

  Toutes les opérations de Kaspersky Anti-Virus au sujet desquelles vous devez être alerté immédiatement ou qui nécessitent une prise de décision rapide sont annoncées sous la forme d'une infobulle qui apparaît au-dessus de l'icône de l'application dans la barre des tâches. Ces infobulles sont transparentes afin de ne pas vous perturber dans votre travail. Le fond de l'infobulle devient solide dès que vous placer le curseur de la souris sur la fenêtre. Il est possible de modifier le degré de transparence de ces infobulles. Pour ce faire, faites glisser le curseur de l'échelle **Coefficient de transparence** jusqu'au niveau requis. Afin de supprimer la transparence des messages, désélectionnez la case **Utiliser la transparence pour les fenêtres de notification**.

- Utilisation d'éléments graphiques propres et de la palette des de couleurs dans l'interface du logiciel.

  Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de Kaspersky Anti-Virus peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel, localiser l'interface dans la langue de votre choix. Pour activer votre propre environnement graphique, indiquez le répertoire avec ses paramètres dans le champ **Répertoire avec la description des "Skins"**. Cliquez sur **Parcourir** pour sélectionner le répertoire

  Les couleurs et les styles du système sont utilisés par défaut. Si vous souhaitez en utiliser d'autres, désélectionnez la case **Utiliser les couleurs et les styles du système**. Dans ce cas, le système utilisera les styles que vous aurez indiqués lors de la configuration de l'environnement graphique.

N'oubliez pas que la modification des paramètres de l'interface de Kaspersky Anti-Virus n'est pas préservée lors du rétablissement des paramètres de fonctionnement par défaut ou de la suppression du programme.

11.8. Utilisation des services complémentaires

Kaspersky Anti-Virus vous propose également les services complémentaires suivants :

- Avertissement de l'utilisateur par courrier électronique en cas d'événements particuliers.
- Autodéfense de Kaspersky Anti-Virus contre la désactivation, la suppression ou la modification des modules et protection de l'accès au logiciel par mot de passe.
- Résolution des problèmes de compatibilité entre Kaspersky Anti-Virus 6.0 et d'autres applications.

Pour passer à la configuration des services cités :

1. Ouvrez la boîte de dialogue de configuration de l'application à l'aide du lien Configuration de la fenêtre principale.
2. Sélectionnez le point **Services** dans l'arborescence.

La partie de droite vous permet de définir si vous voulez utiliser ou non les services complémentaires dans l'application.

11.8.1. Notifications relatives aux événements de Kaspersky Anti-Virus

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus. Ces notifications peuvent avoir un caractère purement informatif ou présenter des informations plus importantes. 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.

Afin d'être au courant de ce qui se passe dans le cadre du fonctionnement de Kaspersky Anti-Virus, vous pouvez activer le service de notification.

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

- Infobulles au-dessus de l'icône du logiciel dans la barre des tâches.
- Notification sonore.

- Messages électroniques.
- Consignation des informations dans le journal des événements.

Pour utiliser ce service :

1. Cochez la case **Activer les notifications sur les événements** dans le bloc **Interaction avec l'utilisateur**(cf. Illustration 49).

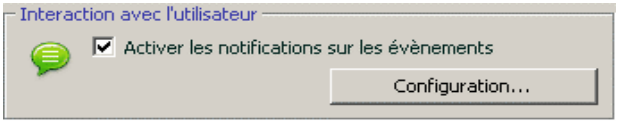


Illustration 49. Activation des notifications

2. Définir le type d'événements de Kaspersky Anti-Virus au sujet desquels vous souhaitez être averti, ainsi que le mode de notification (cf. point 11.8.1.1, p. 146).
3. Configurez les paramètres d'envoi des notifications par courrier électronique si vous avez choisi ce mode (cf. point 11.8.1.2, p. 148).

11.8.1.1. Types de notification et mode d'envoi des notifications

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus.

Evénements critiques. Evénements 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, *signatures des menaces corrompues* ou *expiration de la validité de la licence*.

Refus de fonctionnement. Evénement qui empêche le fonctionnement de l'application. Par exemple, absence de licence ou de signatures des menaces.

Evénements importants. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le fonctionnement du logiciel. Exemple : *protection désactivée* ou *l'analyse antivirus de l'ordinateur a été réalisée il y a longtemps*.

Evénements informatifs. Evénements à caractère purement informatif qui ne contient aucune information cruciale. Exemple : *tous les objets dangereux ont été réparés*.

Afin d'indiquer les événements au sujet desquels vous souhaitez être averti et de quelle manière :

1. Cliquez sur le lien Configuration dans la fenêtre principale du logiciel.
2. Dans la boîte de configuration du logiciel, sélectionnez la section **Services**, cochez la case ☑ **Activer les notifications sur les événements** et passez à la configuration détaillée en cliquant sur **Complémentaire**.

Dans la fenêtre **Configuration des notifications** (cf. Illustration 50), vous pouvez définir les modes d'envoi suivants pour les notifications :

- *Infobulles au-dessus* de l'icône du logiciel dans la barre des tâches contenant les informations relatives à l'événement ;

  Pour utiliser ce mode, cochez la case ☑ dans le schéma **Ecran** en regard de l'événement au sujet duquel vous souhaitez être averti.

- *Notification sonore*.

  Si vous voulez accompagner cette infobulle d'un effet sonore, cochez la case ☑ dans la partie **Son** en regard de l'événement.

- *Notification par courrier électronique*.

  Pour utiliser ce mode, cochez la case ☑ **Message** en regard de l'événement au sujet duquel vous souhaitez être averti et configurez les paramètres d'envoi des notifications (cf. point 11.8.1.2, p. 148).

- Consignation des informations dans le journal des événements.

  Pour consigner les informations relatives à un événement quelconque, cochez la case en regard ☑ dans le bloc **Journal** et configurez les paramètres du journal des événements (cf. point 11.8.1.3, p. 149).

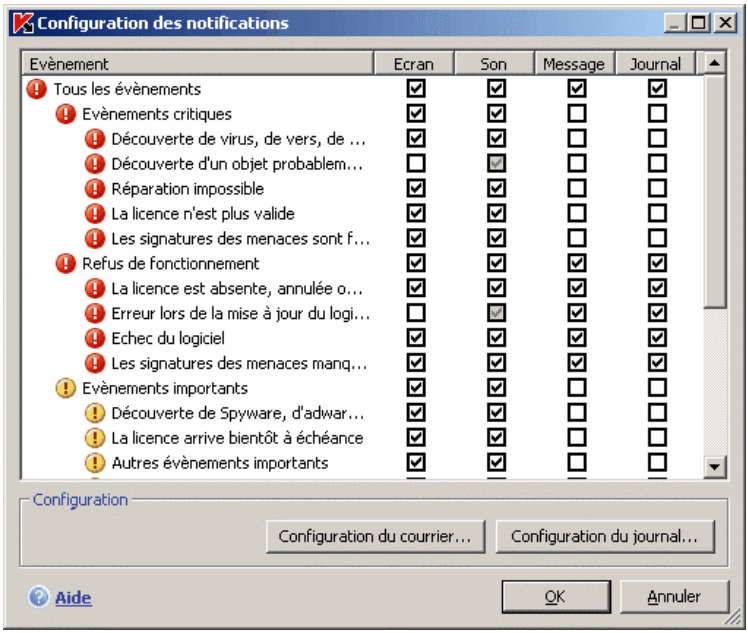


Illustration 50. Evénement survenus pendant le fonctionnement du logiciel et modes de notification choisis.

11.8.1.2. Configuration de l'envoi des notifications par courrier électronique

Après avoir sélectionné les événements (cf. point 11.8.1.1, p. 146)au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications. Pour ce faire :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Complémentaire** dans le bloc **Interaction avec l'utilisateur** de la partie droite de la fenêtre.
4. Sur l'onglet **Configuration de notifications**, cochez la case ☑ dans la partie **E-mail** pour les événements qui déclencheront l'envoi d'une notification par courrier électronique.

5. Dans la fenêtre qui s'ouvre à l'aide du bouton **Configuration du courrier**, définissez les paramètres suivants pour l'envoi des notifications par courrier:

   - Définissez les paramètres d'expédition de la notification dans le bloc **Envoi de la notification au nom de l'utilisateur**.

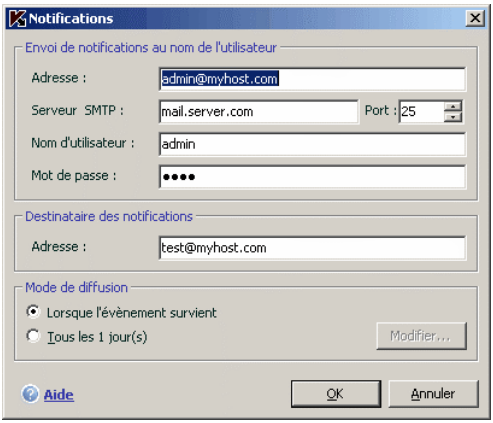


Illustration 51. Configuration de la notification par courrier électronique

   - Saisissez l'adresse électronique vers laquelle la notification sera envoyée dans le bloc **Destinataire des notifications**.

   - Définissez le mode d'envoi de la notification par courrier électronique dans le bloc **Mode de diffusion**. Afin que l'application envoie un message lorsqu'un événement se produit, sélectionnez **Lorsque l'événement survient**. Pour être averti des événements après un certain temps, programmez la diffusion des messages d'informations en cliquant sur le bouton **Modifier…**. Par défaut, les notifications sont envoyées chaque jour.

11.8.1.3. Configuration du journal des événements

Pour configurer le journal des événements :

1. Cliquez sur le lien Configuration dans la fenêtre principale afin d'ouvrir la fenêtre de configuration de l'application.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.

3. Cliquez sur le bouton **Complémentaire** du bloc **Interaction avec l'utilisateur** dans la partie droite de la fenêtre.

Dans la fenêtre **Configuration des notifications**, sélectionnez le type d'événements que vous voulez enregistrer dans le journal et cliquez sur le bouton **Configuration du journal**.

Kaspersky Anti-Virus permet d'enregistrer les informations relatives aux événements survenus pendant l'utilisation de l'application dans le journal général de Microsoft Windows (**Applications**) ou dans le journal séparé des événements de Kaspersky Anti-Virus (**Kaspersky Event Log**).

La consultation des journaux s'opère dans la fenêtre standard de Microsoft Windows **Observateur d'événements** qui s'ouvre à l'aide de la commande **Démarrer/Paramètres/Panneau de configuration/Administration/Observateur d'événements**.

11.8.2. Autodéfense du logiciel et restriction de l'accès

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

De plus, 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 ses paramètres peut considérablement réduire le niveau de la protection globale de l'ordinateur.

Afin de garantir la stabilité du système de protection de votre ordinateur, le logiciel incorpore un mécanisme d'autodéfense contre les interactions distantes ainsi que la protection de l'accès via un mot de passe.

Afin d'activer l'utilisation des mécanismes d'autodéfense du logiciel :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.

Opérez la configuration requise dans le bloc **Auto-défense** (cf. Illustration 52) :

- ☑ **Activer l'autodéfense**. Lorsque cette case est cochée, 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 est activée.

☑ **Interdire l'administration externe par un service**. En cochant cette case, vous bloquez toute tentative d'administration à distance des services du programme

Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la barre des tâches en cas de tentative d'exécution des actions citées (pour autant que l'utilisateur n'ait pas désactivé les notifications).

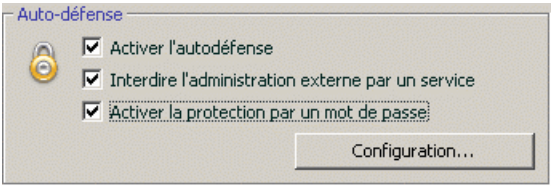


Illustration 52. Configuration de la protection du programme

Afin de limiter l'accès au logiciel à l'aide d'un mot de passe, cochez la case ☑ **Activer la protection par un mot de passe** et dans la fenêtre qui s'ouvre une fois que vous aurez cliqué sur Configuration, précisez le mot de passe et le secteur d'application de celui-ci (cf. Illustration 53).

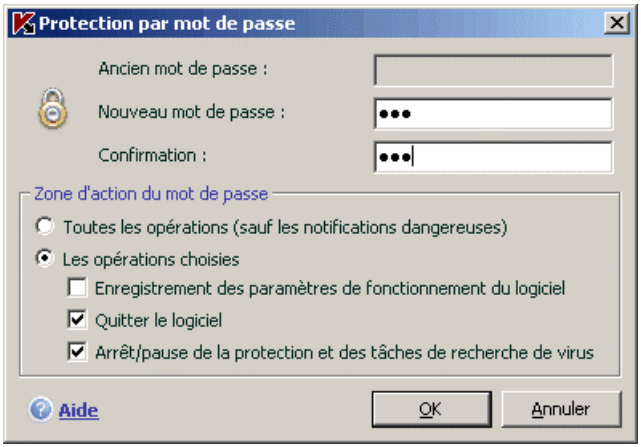


Illustration 53. Configuration de la protection par mot de passe

Vous pouvez bloquer n'importe quelle action du programme, à l'exception des notifications en cas de découverte d'objets dangereux ou interdire l'une des actions suivantes :

- Modifier les paramètres de fonctionnement du logiciel.
- Arrêter Kaspersky Anti-Virus.

- Désactiver la protection de votre ordinateur ou la suspendre pour un certain temps.

Chacune de ces actions entraîne une réduction du niveau de protection de votre ordinateur , aussi vous devez définir un groupe de personnes qui seront autorisées à travailler sur le serveur.

Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions que vous avez sélectionnées sur le serveur, il devra saisir le mot de passe.

11.8.3. Résolution des problèmes de compatibilité entre Kaspersky Anti-Virus et d'autres applications

Des conflits peuvent survenir dans certains cas entre Kaspersky Anti-Virus et d'autres applications installées sur l'ordinateur. Cela est dû à la présence de mécanismes d'autodéfense intégrés à ces applications qui réagissent lorsque Kaspersky Anti-Virus tente de s'y introduire. Parmi les programmes réagissant ainsi, citons le module externe Authentica pour Adobe Reader qui se charge de l'analyse de l'accès aux fichiers PDF, Oxygen Phone Manager II, le programme d'administration des téléphones mobiles, et certains types de jeux protégés contre le crackage.

Pour résoudre ce problème, cochez la case **Compatibilité avec les applications auto-protégées** dans la section **Services** de la fenêtre de configuration de l'application. La modification de ce paramètre entrera en vigueur après le redémarrage du système d'exploitation.

11.9. Exportation/importation des paramètres de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet d'exporter et d'importer ses paramètres de fonctionnement.

Les paramètres sont enregistrés dans un fichier de configuration spécial.

Pour exporter les paramètres actuels de fonctionnement du logiciel :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus.

2. Cliquez sur le lien Configuration dans la section **Services**.
3. Cliquez sur le bouton **Exporter** dans le bloc **Administration de la configuration.**
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

Pour importer les paramètres du fichier de configuration :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus.
2. Cliquez sur le lien Configuration dans la section **Services**.
3. Cliquez sur **Importer** et sélectionnez le fichier contenant les paramètres que vous souhaitez importer dans Kaspersky Anti-Virus.

11.10. Restauration des paramètres par défaut

Vous pouvez toujours revenir aux paramètres recommandés du logiciel. 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.

Pour restaurer les paramètres de protection :

1. Sélectionnez la section **Services** et ouvrez la fenêtre des paramètres du logiciel à l'aide du lien Configuration.
2. Cliquez sur le bouton **Restaurer** dans la section **Administration de la configuration**.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et de quels composants que vous souhaitez conserver en plus de la restauration du niveau de protection recommandé.

Par défaut, tous les paramètres uniques présentés dans la liste seront conservés (la case correspondante n'est pas sélectionnée). Si certains paramètres n'ont pas besoin d'être conservés, cochez la case située en regard de ceux-ci.

Une fois la configuration terminée, cliquez sur **Suivant**. Cela lancera l'Assistant de configuration initiale du logiciel (cf. point 3.2, p. 27). Suivez les instructions affichées.

Lorsque vous aurez quitté l'Assistant, l'Antivirus Fichiers fonctionnera selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidé de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

CHAPITRE 12. 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 Anti-Virus 6.0 for Windows Servers 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 6.0 for Windows Servers 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, cons).
- Installez Kaspersky Anti-Virus 6.0 for Windows Servers et *l'Agent d'administration* (faisant partie de Kaspersky Administration Kit) sur les serveurs de fichiers du réseau. 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, quittez la console d'administration.

L'administration de l'application via Kaspersky Administration Kit s'opère grâce à la console d'administration (cf. Illustration 54). Cette console se présente sous la forme d'une **interface** standard **intégrée au MMC** (Microsoft Management Console). Grâce à elle, l'administrateur peut exécuter les tâches suivantes :

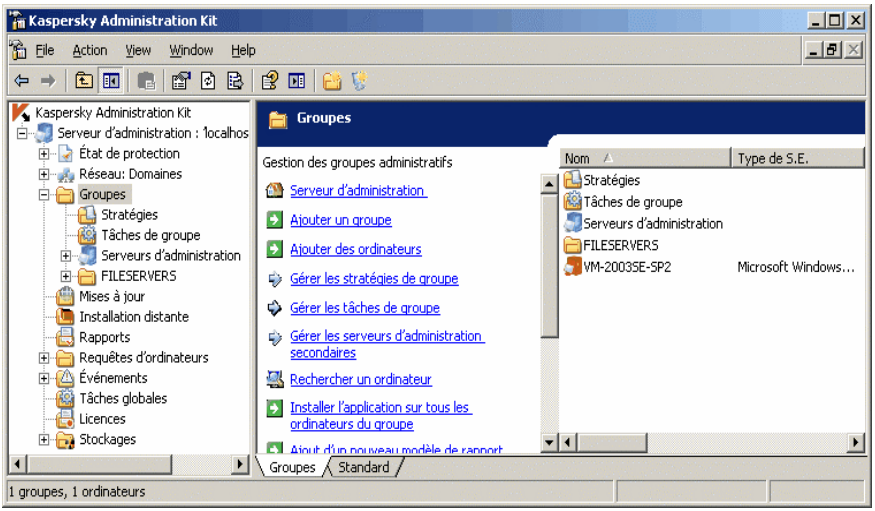


Illustration 54. Console d'administration de Kaspersky Administration Kit

- Installation à distance de Kaspersky Anti-Virus 6.0 for Windows Servers et de *l'Agent d'administration* sur les ordinateurs du réseau ;
- Configuration à distance de Kaspersky Anti-Virus sur les ordinateurs du réseau ;
- Mise à jour des signatures des menaces et des modules de Kaspersky Anti-Virus ;
- Administration des licences d'utilisation de l'application sur les ordinateurs du réseau ;
- Consultation des informations relatives à l'activité de l'application sur les ordinateurs client.

En cas d'administration centralisée via Kaspersky Administration Kit, c'est l'administrateur qui définit les paramètres de la stratégie, des tâches et de l'application.

Les paramètres de l'application regroupent les paramètres généraux de fonctionnement de l'application, y compris les paramètres globaux de la protection, les paramètres du dossier de sauvegarde et de la quarantaine, les paramètres de constitution des rapports, etc.

Une **Tâche** est une action exécutée par l'application. Les tâches de Kaspersky Anti-Virus for Windows Servers sont réparties en différents types (recherche de virus, mise à jour de l'application, remise à l'état antérieur à la mise à jour, installation de la clé de licence). A chaque tâche correspond un groupe de

paramètres de fonctionnement de Kaspersky Anti-Virus pendant l'exécution de la tâche. Il s'agit des *paramètres de la 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 pour les ordinateurs des groupes du réseau logique 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 intègre la configuration complète de toutes les fonctions de l'application. Elle porte sur les paramètres de l'application et les paramètres de tous les types de tâche, à l'exception des tâches spécifiques.

12.1. Administration de l'application

Kaspersky Administration Kit permet de gérer à distance le lancement et l'arrêt de Kaspersky Anti-Virus sur chaque ordinateur client, de même que la configuration des paramètres généraux de fonctionnement de l'application tels que l'activation ou la désactivation de la protection, la configuration du dossier de sauvegarde et de la quarantaine et la composition des rapports.

Pour administrer les paramètres de l'application :

1. Dans le dossier **Groupes** (cf. Illustration 54), sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.
2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez modifier les paramètres. Sélectionnez l'option **Propriétés** dans le menu contextuel ou dans le menu **Actions**.
3. L'onglet **Applications** (cf. Illustration 55) de la fenêtre des propriétés de l'ordinateur client reprend la liste complète des logiciels Kaspersky Lab installés sur l'ordinateur client. Sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers.**

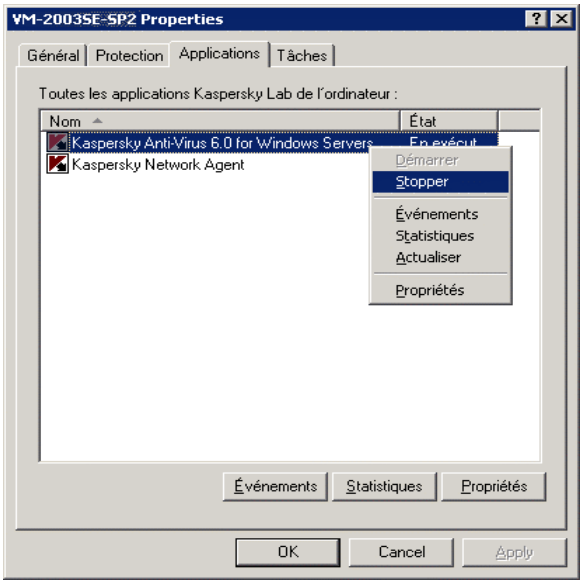


Illustration 55. Liste des applications de Kaspersky Lab

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 enregistrées sur le Serveur d'administration ;
- Consulter les statistiques actuelles sur l'activité de l'application ;
- Configurer l'application (cf. point 12.1.2, p. 158).

12.1.1. Lancement et arrêt de l'application

L'administration du lancement et de l'arrêt de Kaspersky Anti-Virus sur un ordinateur distant s'opère via les commandes du menu contextuel de la fenêtre des p**ropriétés de l'ordinateur** (cf. Illustration 55).

Des actions identiques peuvent être obtenues grâce aux boutons **Lancer**/**Arrêter** de l'onglet **Général** (cf. Illustration 56) dans la fenêtre de configuration de l'application.

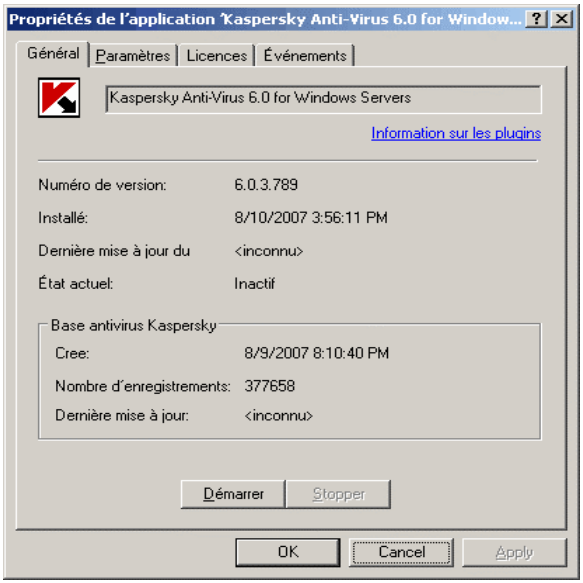


Illustration 56. Configuration de Kaspersky Anti-Virus. Onglet **Général**

La partie supérieure de la fenêtre indique le nom de l'application installée, la version, la date d'installation, le statut (application lancée ou arrêtée sur l'ordinateur local) et l'état des bases de signatures des menaces.

12.1.2. Configuration de l'application

Afin de consulter ou de modifier les paramètres de l'application :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Applications** (cf. Illustration 54).
2. Sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers.** Cliquez sur le bouton **Propriétés** afin d'ouvrir la fenêtre de configuration de l'application.

Tous les onglets (à l'exception de l'onglet **Paramètres**) sont standard pour Kaspersky Administration Kit. Vous trouverez une description détaillée des onglets standard dans le manuel de l'administrateur de Kaspersky Administration Kit.

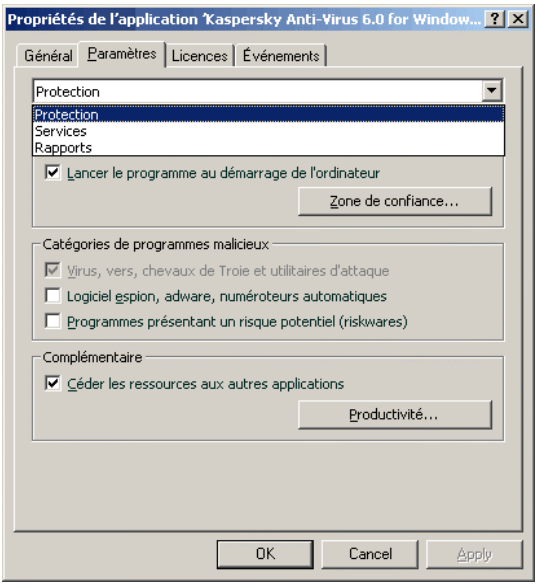


Illustration 57. Configuration de Kaspersky Anti-Virus. Onglet **Paramètres**

Si une stratégie interdisant la modification de certains paramètres a été créée (cf. point 12.3.1, p. 168), la modification de la configuration de l'application sera impossible.

Vous pouvez, sur l'onglet **Paramètres**, définir les paramètres généraux et de service pour la protection assurée par Kaspersky Anti-Virus, les paramètres du dossier de sauvegarde et de la quarantaine, les paramètres de composition des rapports. Il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure :

Protection
Il est possible de : • Activer ou de désactiver la protection de l'ordinateur (cf. point 6.1, p. 55); • Configurer le lancement automatique de l'application au démarrage de l'ordinateur (cf. point 6.1.5, p. 59). • Constituer une zone de confiance et une liste d'exclusion (cf. point 6.3, p. 61);

- Sélectionner les catégories de programmes malveillants qui seront contrôlés par l'application (cf. point 6.2, p. 59);
- Configurer les paramètres de performances de l'application ainsi que les paramètres de la configuration multiprocesseur (cf. point 6.7, p. 73).

Services

La configuration des services comporte:

- Configurer la réceptions des notifications relatives aux événements survenus (cf. point 11.8.1, p. 145).
- L'administration de l'autodéfense de l'application et la restriction de l'accès aux paramètres de l'application grâce à l'instauration d'un mot de passe (cf. point 11.8.2, p. 150).
- Configurer l'apparence de l'application (cf. point 11.7, p. 143).
- Configurer les paramètres de compatibilités entre Kaspersky Anti-Virus et d'autres applications (cf. point 11.8.3, p. 152).

Fichiers de données

Cette fenêtre permet de configurer la composition des rapports statistiques sur le fonctionnement de l'application (cf. point 11.3.1, p. 133), ainsi que l'heure de placement des fichiers dans le dossier de sauvegarde (cf. point 11.2.2, p. 130) ou en quarantaine (cf. point 11.1.2, p. 127).

12.1.3. Configuration des paramètres spécifiques

Si vous administrez Kaspersky Anti-Virus via Kaspersky Administration Kit, vous pouvez activer ou désactiver l'interaction entre l'application et l'utilisateur ainsi que modifier les informations relatives à l'assistance technique. Pour ce faire :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Applications** (cf. Illustration 55).
2. Sélectionnez **Kaspersky Anti-Virus 6.0 for Windows Servers** puis, cliquez sur le bouton **Propriétés.** La boîte de dialogue de configuration de l'application s'affichera (cf. Illustration 56). Dans la liste déroulante de la partie supérieure, sélectionnez **Services**.

L'activation ou la désactivation du mode de fonctionnement interactif de Kaspersky Anti-Virus sur l'ordinateur distant s'opère au départ de l'onglet

Service dans le groupe **Apparence** : affichage de l'icône de Kaspersky Anti-Virus dans la barre des tâches et notifications des événements survenus pendant l'utilisation de l'application (par exemple, découverte d'un objet dangereux).

Si la case ☑ **Autoriser l'interaction avec l'utilisateur** est cochée, l'utilisateur qui travaille sur l'ordinateur distant verra l'icône de l'application, les infobulles et il pourra décider de l'action à prendre après chaque événement. Annulez la sélection de cette case pour désactiver le mode interactif.

Vous pouvez adapter les informations relatives à l'assistance techniques présentées sous le point **Assistance technique** de la rubrique **Service** au départ de l'onglet **Informations personnalisées pour l'assistance technique** (cf. Illustration 47) de la fenêtre qui s'ouvre après avoir cliqué sur **Configuration**.

Il suffit de modifier le texte du champ supérieur. Dans le champ inférieur, modifiez la liste des liens qui apparaissent dans le groupe **Assistance technique en ligne** du point **Assistance technique** dans la rubrique **Services**.

Les boutons **Ajouter**, **Modifier** et **Supprimer** vous permettent de modifier le contenu de la liste. Kaspersky Anti-Virus ajoute le nouveau lien en tête de liste. Il est possible de modifier l'ordre de la liste grâce au bouton **Monter**/**Descendre**.

Si aucune information n'est reprise dans la fenêtre, alors les informations proposées par défaut sur l'assistance technique ne seront pas modifiées.

12.2. Administration des tâches

Cette rubrique est consacrée à l'administration de tâches pour Kaspersky Anti-Virus 6.0 for Windows Servers. Pour obtenir de plus amples informations sur l'administration des tâches via Kaspersky Administration Kit 6.0, veuillez consulter le manuel de l'administrateur de ce logiciel.

Une sélection de tâche système pour chaque ordinateur est créée lors l'installation de l'application. Cette liste (cf. Illustration 58) comprend les tâches liées à la protection en temps réel (Antivirus Fichiers), des tâches en rapport avec la recherche de virus (Analyser mon poste de travail, analyse des objets de démarrage, analyse des secteurs critiques) ainsi que les tâches de mise à jour (mise à jour des signatures des menaces et des modules de l'application, retour à l'état antérieur à la mise à jour et la copie des mises à jour).

Vous pouvez lancer les tâches système, configurer les paramètres et les programmer. La suppression de ces tâches est impossible.

De plus, vous pouvez créer vos propres tâches, par exemple des tâches de recherche de virus, de mise à jour de l'application, d'annulation de la mise à jour ou d'installation des clés de licence.

Afin de consulter la liste des tâches créées pour l'ordinateur client :

1. Dans le dossier **Groupes** (cf.Illustration 54), sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.
2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez créer une tâche locale et utilisez la commande **Tâches** du menu contextuel ou l'élément correspondant du menu **Actions**. Cette action entraîne l'ouverture de la fenêtre des propriétés de l'ordinateur client dans la fenêtre principale de l'application.

Toutes les tâches créées pour cet ordinateur client figurent sur l'onglet **Tâches** (cf. Illustration 58)

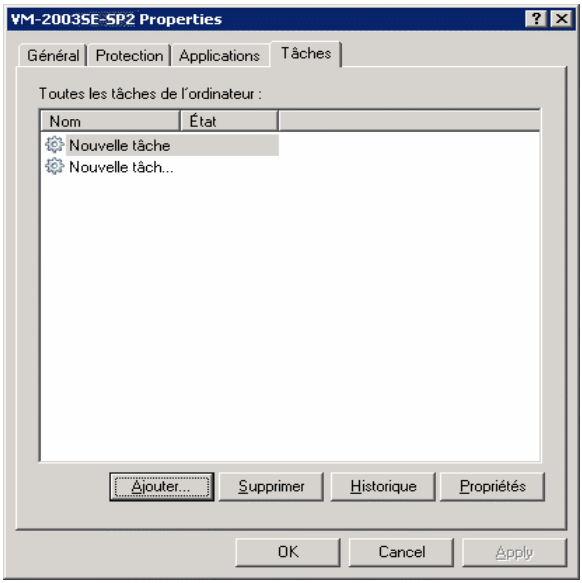


Illustration 58. Liste des tâches de l'application

12.2.1. Lancement et arrêt des tâches

Le lancement d'une tâche sur l'ordinateur client est possible uniquement si l'application correspondante est lancée (cf. point 12.1.1, p. 157). En cas d'arrêt de l'application, l'exécution de toutes les tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide de la commande du menu

contextuel), ainsi que depuis la fenêtre d'examen des paramètres de la tâche. Vous pouvez également suspendre l'exécution d'une tâche puis la reprendre.

Afin de lancer /arrêter/interrompre/reprendre manuellement une tâche :

> Sélectionnez la tâche souhaitée, ouvrez le menu contextuel et cliquez sur **Lancer / Arrêter / Suspendre / Reprendre** ou utilisez une des commandes équivalentes du menu **Action**.

Les mêmes actions peuvent être réalisées au départ de la fenêtre de configuration de la tâche, dans l'onglet **Général** (cf. Illustration 59) à l'aide des boutons identiques.

12.2.2. Création de tâches

En utilisant l'application via Kaspersky Administration Kit, vous pouvez créer :

- Des tâches locales : définies pour un ordinateur distinct;
- Des tâches de groupe, définies pour des ordinateurs repris au sein d'un groupe logique ;
- Des tâches globales : définies pour un ensemble aléatoire d'ordinateurs issus de groupes aléatoires du réseau local.

Vous pouvez modifier les paramètres des tâches, observer leur exécution, copier et déplacer les tâches d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Actions**.

12.2.2.1. Création d'une tâche locale

Pour créer une tâche locale, exécutez les opérations suivantes :

1. :Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Tâches** (cf. Illustration 58).
2. Cliquez sur **Ajouter** pour ajouter une nouvelle tâche. Cette action entraîne l'ouverture de la boîte de dialogue de création d'une nouvelle tâche. Son interface 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 **Préc.** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter le programme à n'importe quel stade, cliquez sur **Annuler**.

Etape 1.Saisie des données générales sur la tâche

La première fenêtre de l'Assistant est une fenêtre d'introduction : il faut saisir ici le nom de la tâche (champ **Nom**).

Etape 2.Sélection de l'application et du type de tâche

Au cours de cette étape, vous devez préciser l'application pour laquelle vous créez la tâche, à savoir Kaspersky Anti-Virus 6.0 for Windows Servers. Il faut également sélectionner le type de tâche. Les tâches suivantes peuvent être créées pour Kaspersky Anti-Virus 6.0 :

- *Recherche de virus* : recherche de virus dans les secteurs définis par l'utilisateur.
- *Mise à jour* : réception et installation des mises à jour pour l'application.
- *Remise à l'état antérieur à la mise à jour* : annulation de la dernière mise à jour effectuée.
- *Installation de la clé de licen*ce : ajout d'une nouvelle clé de licence d'utilisation de l'application.

Etape 3.Configuration des paramètres du type de tâche sélectionné

Le contenu des fenêtres suivantes varie en fonction du type de tâche sélectionné à l'étape précédente.

RECHERCHE DE VIRUS

Dans la fenêtre de configuration de la recherche de virus, il faut constituer la liste des objets à analyser (cf. point 8.2, p. 90) et préciser l'action qui sera exécutée par Kaspersky Anti-Virus lors de la détection d'un objet dangereux (cf. point 8.4.4, p. 99).

MISE A JOUR

Pour la mise à jour des signatures des menaces et des modules de l'application, il faut indiquer la source utilisée pour le téléchargement des fichiers de mise à jour (cf. point 10.4.1, p. 112). Les mises à jour sont téléchargées par défaut du serveur de mise à jour de l'application Kaspersky Administration Kit.

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR

La tâche liée à l'annulation de la dernière mise à jour effectuée ne dispose pas de paramètres particuliers.

INSTALLATION DE LA CLE DE LICENCE

Afin d'ajouter une clé de licence, cliquez sur **Parcourir** pour indiquer le chemin d'accès au fichier de clé. Pour que la nouvelle clé soit considérée comme une clé de réserve, cochez la case ☑ **Ajouter en tant que clé de réserve**. La clé de licence de réserve prendra la place de la clé actuelle dès que cette dernière sera arrivée à échéance.

Les informations relatives à la clé ajoutée (numéro de licence, type de licence et durée de validité) sont reprises dans le champ inférieur.

Etape 4. Configuration du lancement d'une tâche au nom d'un autre compte

Cette étape vous permet de configurer le lancement de la tâche au nom d'un autre compte jouissant de privilèges d'accès suffisant à l'objet à analyser ou à la source de la mise à jour (pour de plus amples informations, consultez le point 6.4 à la page 68).

Etape 5. Programmation de la tâche

Une fois que vous aurez configuré la tâche, vous aurez la possibilité de programmer son lancement automatique.

Pour ce faire, sélectionnez la fréquence de lancement dans le menu déroulant et précisez les paramètres de la programmation dans la partie inférieure.

Etape 6. Fin de la création d'une tâche

La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche.

12.2.2.2. Création d'une tâche de groupe

Suivez les étapes décrites ci-après pour créer une tâche de groupe :

1. Sélectionnez le groupe pour lequel vous souhaitez créer la tâche dans l'arborescence de la console.
2. Sélectionnez le répertoire **Tâches de groupe** qui en fait partie, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Actions**. Cette action entraîne l'ouverture de l'Assistant de création de tâches semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 12.2.2.1 à la page 163). Suivez les instructions affichées.

Une fois que vous aurez quitté l'Assistant, la tâche sera ajoutée au dossier **Tâches de groupe** du groupe correspondant et de tous les groupes repris dans ce groupe et reprise dans le panneau des résultats.

12.2.2.3. Création d'une tâche globale

Suivez les étapes décrites ci-après pour créer une tâche globale:

1. Sélectionnez le nœud **Tâches globales** dans l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Actions**.
2. Cette action entraîne l'ouverture de l'Assistant de création de tâches semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 12.2.2.1 à la page 163). La seule différence se situe au niveau de l'existence d'une étape permettant de dresser la liste des ordinateurs clients du réseau logique pour lesquels vous créez la tâche globale.
3. Sélectionnez les ordinateurs du réseau logique sur lesquels la tâche sera exécutée. Vous pouvez sélectionner des ordinateurs issus de différents dossiers ou sélectionner directement le dossier entier (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit).

Les tâches globales sont exécutées uniquement sur le groupe d'ordinateurs sélectionnés. 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.

A la fin de la création de la tâche, la nouvelle tâche globale sera reprise dans le nœud **Tâches globales** de l'arborescence de la console et apparaîtra dans le panneau des résultats.

12.2.3. Configuration de tâches

Afin de consulter et de modifier les paramètres des tâches de l'ordinateur client :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Tâches** (cf. Illustration 58).
2. Sélectionnez la tâche dans la liste puis cliquez sur **Propriétés**. La boîte de dialogue de configuration des tâches s'affichera (cf. Illustration 59).

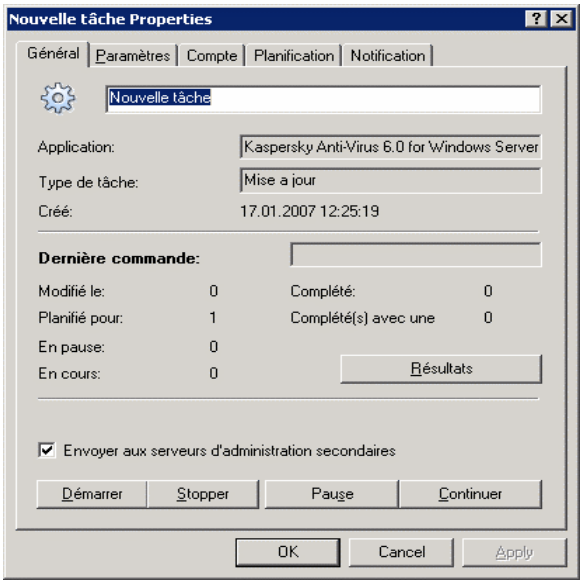


Illustration 59. Configuration des tâches

Ces onglets (à l'exception de l'onglet **Paramètres**) sont des onglets standard pour Kaspersky Administration Kit 6.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit. L'onglet **Paramètres** contient les paramètres propres à Kaspersky Anti-Virus. Le contenu de cet onglet varie en fonction du type de tâche sélectionnée.

La configuration des tâches de l'application via l'interface de Kaspersky Administration Kit est identique à la configuration via l'interface de Kaspersky Anti-Virus à l'exception des paramètres propres à cette tâche en question. Pour obtenir de plus amples informations sur la configuration des tâches, consultez les Chapitre 7 - Chapitre 10 aux pages 74 - 108 de ce manuel.

Si une stratégie interdisant la modification de certains paramètres a été créée (cf. point 12.3, p. 167), la modification de la configuration de la tâche sera impossible.

12.3. Administration des stratégies

La définition de stratégie est un moyen permettant d'appliquer une configuration des tâches et de l'application identique à tous les ordinateurs client faisant partie d'un groupe du réseau logique.

Cette rubrique est consacrée à la création et à la configuration de stratégies pour Kaspersky Anti-Virus 6.0 for Windows Servers. Pour obtenir de plus amples informations sur l'administration des stratégies via Kaspersky Administration Kit 6.0, veuillez consulter le manuel de l'administrateur de ce logiciel.

12.3.1. Création d'une stratégie

Afin de créer une stratégie pour Kaspersky Anti-Virus, procédez comme suit :

1. Dans le dossier **Groupes** (cf. Illustration 54), sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez créer la stratégie.
2. Sélectionnez le dossier **Stratégies** appartenant au groupe sélectionné, ouvrez le menu contextuel et cliquez sur **Créer→Stratégie** La fenêtre de création d'une nouvelle stratégie apparaîtra à l'écran.

   L'interface du programme de création des stratégies 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 **Préc.** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

A chaque étape de la création de la stratégie, il est possible de verrouiller les paramètres définis à l'aide du bouton  . Si le cadenas est fermé, cela signifie que les paramètres appliqués aux ordinateurs client lors de l'utilisation de la stratégie seront ceux définis dans cette stratégie.

Etape 1. Saisie des données générales sur la stratégie

Les premières fenêtres de l'Assistant sont des fenêtres d'introduction. Il faut saisir ici le nom de la stratégie (champ **Nom**) et sélectionner l'application **Kaspersky Anti-Virus 6.0 for Windows Servers** dans la liste déroulante **Nom de l'application**. Pour que la configuration de la stratégie entre en vigueur directement après sa création, cochez la case **Activer la stratégie**.

Etape 2. Sélection de l'état de la stratégie

Cette fenêtre vous permet de définir le statut de la stratégie à l'aide des cases adéquates : stratégie active ou stratégie inactive.

Plusieurs stratégies peuvent être créées dans le groupe pour une application mais il ne peut y avoir qu'une seule politique active.

Etape 3. Sélection et la configuration des composants de la protection

Cette étape vous permet d'activer ou de désactiver la protection de l'ordinateur ainsi que l'Antivirus Fichiers. La protection est activée par défaut et l'Antivirus Fichiers fonctionne.

Pour passer à une configuration détaillée de la protection ou de l'Antivirus Fichiers, sélectionnez l'élément souhaité dans la liste et cliquez sur **Configuration…**.

Etape 4. Configuration paramètres de recherche de virus

Cette étape correspond à la configuration des paramètres utilisés par les tâches de recherche de virus.

Sélectionnez, dans le bloc **Niveau de protection** un des trois niveaux proposés (cf. point 7.1, p. 75). Pour procéder à une configuration détaillée du niveau sélectionné, cliquez sur **Configuration**. Afin de restaurer les paramètres du niveau **Recommandé**, cliquez sur **Par défaut**.

Dans le groupe **Action**, indiquez l'action qui sera exécutée par Kaspersky Anti-Virus lors de la découverte d'un objet dangereux (cf. point 8.4.4, p. 99)

Etape 5. Configuration de la mise à jour

Cette étape correspond à la configuration de la mise à jour de Kaspersky Anti-Virus.

Dans le groupe **Paramètres de la mise à jour**, indiquez s'il faut actualiser les modules de l'application (cf. point 10.4.2, p. 115). Dans la fenêtre qui s'ouvre après avoir cliqué sur **Configuration**, définissez les paramètres de l'intranet (cf. point 10.4.3, p. 117) et désignez la source de la mise à jour (cf. point 10.4.1, p. 112).

Dans le groupe **Actions après la mise à jour**, activez ou désactivez l'analyse de la quarantaine après la réception de la dernière mise à jour (cf. point 10.4.4, p. 119).

Etape 6. Application des stratégies

Cette étape vous permet de sélectionner le mode de diffusion des stratégies sur les ordinateurs client du groupe (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit).

Etape 7. Fin de la création d'une stratégie

La dernière fenêtre de l'Assistant vous informe sur la réussite de la création de la stratégie.

Lorsque vous quittez l'Assistant de création de stratégie pour Kaspersky Anti-Virus, le dossier **Stratégie** du groupe correspondant sera ajouté et repris dans le panneau des résultats.

Vous pouvez modifier les paramètres de la stratégie créée et limiter la possibilité de modification des paramètres à l'aide du bouton  pour chaque groupe de paramètres. L'utilisateur sur l'ordinateur client ne pourra pas modifier les paramètres marqués de cette manière. La stratégie sera diffusée sur les ordinateurs client lors de la première synchronisation des clients avec le serveur.

Vous pouvez copier et déplacer les stratégies d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Actions**.

12.3.2. Consultation et modification des paramètres de la stratégie

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.

Afin de consulter et de modifier les paramètres d'une stratégie :

1. Sélectionnez le groupe d'ordinateur dans le dossier **Groupes** de l'arborescence de la console pour lequel vous souhaitez modifier les paramètres.
2. Sélectionnez le dossier **Stratégies** faisant partie de ce groupe. Toutes les stratégies définies pour ce groupe seront reprises dans le panneau des résultats.
3. Sélectionnez dans la liste la stratégie souhaitée pour l'application **Kaspersky Anti-Virus 6.0 for Windows Servers** (le nom de l'application est indiqué dans le champ **Application**).
4. Sélectionnez l'élément **Propriétés** dans le menu contextuel de la stratégie sélectionnée. Cette action entraîne l'ouverture de la fenêtre de configuration de la stratégie pour Kaspersky Anti-Virus 6.0 (cf. Illustration 60).

Ces onglets (à l'exception de l'onglet **Configuration**) sont des onglets standard pour Kaspersky Administration Kit 6.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit.

L'onglet **Configuration** reprend les paramètres de la stratégie pour Kaspersky Anti-Virus 6.0. Les paramètres de la stratégie reprennent les paramètres de l'application (cf. point 12.1.2, p. 158) et les paramètres des tâches (cf. point 12.2, p. 161).

Pour configurer les paramètres, il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure.

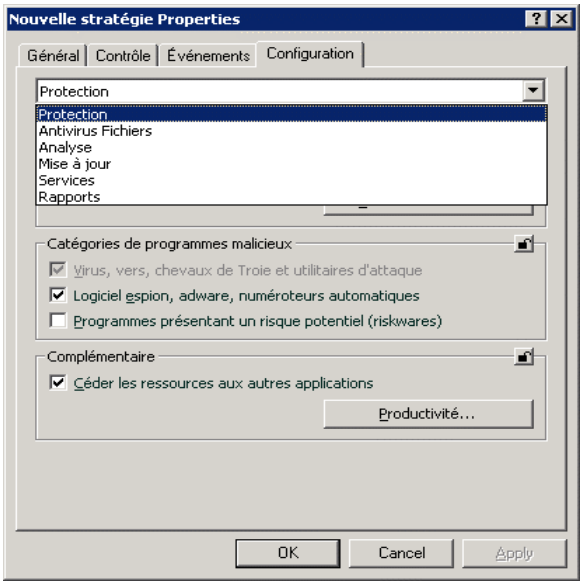


Illustration 60. Configuration des stratégies

CHAPITRE 13. UTILISATION DU PROGRAMME AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Anti-Virus à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- lancement, arrêt, suspension et reprise de l'Antivirus Fichiers;
- lancement, arrêt, suspension et reprise de l'exécution des tâches liées à la recherche de virus;
- obtention d'informations relatives à l'état actuel de l'Antivirus Fichiers et aux tâches et à leur statistiques;
- Analyse des objets sélectionnés;
- Mise à jour des signatures des menaces et des modules du programme;
- 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;

La syntaxe de la ligne de commande est la suivante :

```
avp.com <commande> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit ête réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

Où <**commande**> peut être remplacé par :

ADDKEY	Activation du programme à l'aide du fichier de la clé (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
ACTIVATE	Activation de l'application via Internet à l'aide du code d'activation

START	lancement de l'Antivirus Fichiers ou de la tâche
PAUSE	suspension de l'Antivirus Fichiers ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
RESUME	reprise du fonctionnement de l'Antivirus Fichiers ou de la tâche
STOP	arrêt de l'Antivirus Fichiers ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
STATUS	affichage de l'état actuel de l'Antivirus Fichiers ou de la tâche
STATISTICS	affichage des statistiques de l'Antivirus Fichiers ou de la tâche
HELP	aide sur la syntaxe de la commande ou la liste des commandes.
SCAN	Analyse antivirus des objets
UPDATE	Lancement de la mise à jour du programme
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 l'application).
EXIT	Quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mode passe défini via l'interface du programme)
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)

EXPORT	exportation des paramètres de protection de Kaspersky Anti-Virus

Chaque commande possède ses propres paramètres, propres à chaque composant de Kaspersky Anti-Virus.

13.1. Activation du logiciel

L'application peut être activée de deux manières :

- Via Internet à l'aide d'un code d'activation (commande ACTIVATE);
- A l'aide du fichier de clé de licence (commande ADDKEY).

Syntaxe de la commande :

```
ACTIVATE <code_d'activation>
ADDKEY <nom_du_fichier>
/password=<votre_mot_de_passe>
```

Description des paramètres:

<nom_du_fichier>	Nom nom du fichier de clé de l'activation avec l'extension **.key*.
<code_d'activation>	Code d'activation de l'application fourni à l'achat
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application.
N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.	

Exemple :

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<votre mot de passe>
```

13.2. Administration de l'Antivirus Fichiers et des tâches

Syntaxe de la commande :

```
avp.com <commande> <profil|nom_de_la_tâche>
[/R[A]:<fichier_de_rapport>]
avp.com STOP|PAUSE <profil|nom_de_la_tâche>
/password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

Description des paramètres:

<commande>	L'administration des composants et des tâches de Kaspersky Anti-Virus via la ligne de commande s'opère à l'aide de la sélection de commande suivante : **START** : lance le composant de protection en temps réel ou une tâche. **STOP** : arrête le composant de protection en temps réel ou une tâche. **PAUSE** : suspend le composant de protection en temps réel ou une tâche. **RESUME** : reprend le composant de protection en temps réel ou une tâche. **STATUS** : affichage de l'état actuel du composant de protection en temps réel ou de la tâche. **STATISTICS** : affichage des statistiques du composant de protection en temps réel ou de la tâche. La commande PAUSE ou STOP ne pourra être exécutée sans la saisie du mot de passe.
<profil|nom_de_la_tâche>	En guise de valeur pour le paramètre **<profil>**, vous pouvez indiquez n'importe lequel des composants de la protection en temps réel de l'application ainsi que les tâches d'analyse à la demande ou de mise à jour faisant partie des composants (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après). Le paramètre **<nom_de_la_tâche>** peut prendre comme valeur le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour créée par l'utilisateur.

<votre mot de passe>	mot de passe de Kaspersky Anti-Virus défini dans l'interface de l'application.
/R[A]:<fichier_de_rapport>	**R:<fichier_de_rapport>** : consigne uniquement les événements importants dans le rapport. **/RA:<fichier_de_rapport>** : consigne tous les événements dans le rapport. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les résultats de l'analyse seront affichés à l'écran et tous les événements seront repris.

Le paramètre **<profil>** peut prendre une des valeurs suivantes :

RTP	Tous les composants de la protection La commande `avp.com START RTP` lance Antivirus Fichiers lorsque celui-ci a été interrompu pendant un certain temps à l'aide du bouton ❚❚ de l'interface graphique ou via la commande `PAUSE` de la ligne de commande. Si le composant a été arrêté à l'aide du bouton ■ de l'interface graphique ou via la commande `STOP` de la ligne de commande, il faudra le redémarrer à l'aide de la commande `avp.com START FM`.
FM	Antivirus de fichiers
UPDATER	Mise à jour
RetranslationCfg	Copie des mises à jour de l'application dans une source locale de mise à jour
Rollback	Remise à l'état antérieure à la dernière mise à jour de l'application
SCAN_OBJECTS	Tâche "Recherche de virus"
SCAN_MY_COMPUTER	Tâche "Mon poste de travail"
SCAN_CRITICAL_AREAS	Tâche "Secteurs critiques"

SCAN_STARTUP	Tâche "Objets de démarrage"
SCAN_QUARANTINE	Tâche d'analyse des objets en quarantaine
Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.	

Exemples:

Par exemple, pour activer l'antivirus de fichiers via la ligne de commande, saisissez :

```
avp.com START FM
```

Pour arrêter la tâche Mon poste de travail via la ligne de commande, saisissez :

```
avp.com STOP SCAN_MY_COMPUTER
/password=<votre_mot_de_passe>
```

13.3. Analyse antivirus des fichiers

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>] [<fichier de
configuration>] [<paramètres du rapport>]
[<paramètres complémentaires>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans Kaspersky Anti-Virus en lançant la tâche requise via la ligne de commande (cf. point 13.1, page 174). Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface du logiciel.

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.
/MEMORY	objets de la mémoire vive.
/STARTUP	objets de démarrage.
/MAIL	bases de données de messagerie électronique.
/REMDRIVES	tous les disques amovibles.
/FIXDRIVES	tous les disques locaux.
/NETDRIVES	tous les disques de réseau.
/QUARANTINE	objets en quarantaine.
/ALL	Analyse complète de l'ordinateur.
/@:<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 entre 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 **/i8.**	

/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 exécutée 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.	
/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:<seconds>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<seconds>.**
-es:<size>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre **<size>**.

Le paramètre **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse.

Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus.

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 Kaspersky Anti-Virus qui seront utilisées.

/C:<nom_du_fichier>	Utiliser les valeurs des paramètres définies dans le fichier de configuration **<nom_du_fichier>**.

Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse.

La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les résultats de l'analyse seront affichés à l'écran et tous les événements seront repris.

/R:<fichier_de_rapport>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<fichier_de_rapport>	Consigner tous les événements dans le rapport.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
/iChecker=<on|off>	Activer/désactiver l'utilisation de la technologie iChecker.
/iSwift=<on|off>	Activer/désactiver l'utilisation de la technologie iSwift.

Exemples:

*Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des bases de messagerie et des répertoires **My Documents, Program Files** et du fichier **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Suspendre l'analyse des objets sélectionnés, lancer une nouvelle analyse de l'ordinateur à la fin de laquelle il faudra poursuivre la recherche d'éventuels virus dans les objets sélectionnés :

```
avp.com PAUSE SCAN_OBJECTS
/password=<votre_mot_de_passe>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*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
```

13.4. Mise à jour du logiciel

La commande de mise à jour des modules du logiciel et des signatures des menaces de Kaspersky Anti-Virus possède la syntaxe suivante :

```
avp.com UPDATE [<souce_des_mises_à_jour>]
[/R[A]:<fichier_du_rapport>] [/C:<nom_du_fichier>] [/APP]
```

Description des paramètres:

[<source_des_mises_à_jour>]	Serveur HTTP, serveur FTP pou 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 ou une 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 l'application.
/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner uniquement les événements importants dans le rapport. **/R[A]:<fichier_de_rapport>** : consigner tous les événements dans le rapport. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les résultats de l'analyse seront affichés à l'écran et tous les événements seront repris.

/C:<nom_du_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de l'application lors de la mise à jour. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application. 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 Kaspersky Anti-Virus qui seront utilisées.
/APP	Mettre a jour les modules du logiciel

Exemples:

Mettre à jour les signatures de menaces, consigner tous les événements 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 /C:updateapp. ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app
```

13.5. Remise du programme à l'état antérieur à la mise à jour

Syntaxe de la commande:

```
ROLLBACK [/R[A]:<fichier_de_rapport>]
[/password=<votre_mot_de_passe>]
```

/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : uniquement consigner les événements importants dans le rapport. **/R[A]:<fichier_de_rapport>** : 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.
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application.
N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.	

Exemple :

```
avp.com ROLLBACK /RA:rollback. txt /password=<votre mot de
passe>
```

13.6. Exportation des paramètres

Syntaxe de la commande :

```
avp.com EXPORT <profil> <nom_du_fichier>
```

Description des paramètres:

<profil>	Antivirus Fichiers ou tâche dont les paramètres sont exportés. Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point 13.2 à la page 174.

<nom_du_fichier>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu. Le fichier de configuration est enregistré au format binaire (*dat*), si aucun autre format n'est indiqué ou défini, et peut servir au transfert des paramètres sur d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension *txt*. N'oubliez pas que l'importation de paramètres depuis un fichier texte n'est pas prise en charge, ce fichier peut être utilisé uniquement pour consulter les paramètres principaux de fonctionnement de l'application.

Exemple:

```
avp.com EXPORT c:\kis60settings.txt
```

13.7. Importation des paramètres

Syntaxe de la commande :

```
avp.com IMPORT <nom_du_fichier>
[/password=<votre_mot_de_passe>]
```

< nom_du_fichier>	Chemin d'accès au fichier duquel sont importés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu. L'importation des paramètres de protection est possible uniquement depuis un fichier au format binaire. Lors de l'installation de l'application en mode caché via la ligne de commande ou l'éditeur d'objet de stratégie de groupe, le nom du fichier de configuration doit être *install.cfg*, sans quoi il ne sera pas reconnu par l'application.
<votre_mot_de_passe>	Mot de passe Kaspersky Anti-Virus défini via l'interface de l'application.

N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.

Exemple :

```
avp.com IMPORT c:\ settings.dat /password=<mot_de_passe>
```

13.8. Lancement de l'application

Syntaxe de la commande :

```
avp.com
```

13.9. Arrête de l'application

Syntaxe de la commande :

```
EXIT /password=<votre_mot_de_passe>
```

<votre_mot_de_passe>	Mot de passe Kaspersky Anti-Virus défini via l'interface de l'application.

N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.

13.10. Obtention du fichier de trace

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de l'application. 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>]
```

[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 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages). Lorsque vous contactez le service d'assistance

	technique, l'expert doit vous préciser le niveau qu'il souhaite. S'il n'a rien recommandé en particulier, il est conseillé de choisir le niveau 500.
Attention ! Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et un débordement du disque dur.	

Exemple:

Désactiver la constitution de fichiers de trace :

```
avp.com TRACE file off
```

Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :

```
avp.com TRACE file on 500
```

13.11. 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>
```

13.12. Codes de retour de la ligne de commande

Cette rubrique décrit les 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

CHAPITRE 14. MODIFICATION, REPARATION OU SUPPRESSION DU LOGICIEL

Vous pouvez supprimer l'application à l'aide d'un des moyens suivants :

- à l'aide de l'assistant d'installation de l'application(cf. point 14.1, p. 189) ;
- au départ de la ligne de commande (cf. point 14.2, p. 192) ;
- via Kaspersky Administration Kit (cf. "Manuel de déploiement de Kaspersky Administration Kit");
- via les stratégies de domaine de groupe de Microsoft Windows Server 2000/2003 (cf. point 3.4.3, p. 35).

14.1. Modification, réparation ou suppression du logiciel à 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 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 dans cette source et que vous y avez accès.
2. Sélectionnez **Démarrez → Programmes → Kaspersky Anti-Virus 6.0 for Windows Servers → 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. Fenêtre 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. Cliquez sur **Suivant** pour poursuivre.

Etape 2. Sélection de l'opération

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 (cf. point Etape 7, p. 25) qui vous permet de sélectionner les composants que vous voulez installer ou supprimer.

La réparation du programme 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.

Attention !

Le redémarrage automatique du serveur n'a pas lieu lors d'une désinstallation à distance de Kaspersky Anti-Virus 6.0. Toutefois, pour la suppression complète des composants de l'application et le bon fonctionnement de l'ordinateur, il est conseillé de le redémarrer manuellement.

Lors de la suppression du logiciel, 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 l'application complète**. 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* : informations sur l'activation de l'application.
- *Signatures des menaces* : 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 l'Antivirus Fichiers.
- *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.

> Attention.
>
> 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 réparation, 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**.

14.2. Procédure de suppression de l'application via la ligne de commande

Afin de supprimer Kaspersky Anti-Virus 6.0 for Windows Servers au départ de la ligne de commande, saisissez :

```
msiexec /x <nom_du_paquetage>
```

Cette action lancera l'Assistant d'installation qui vous permettra de supprimer l'application (cf. Chapitre 14, p. 189).

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_paquetage> /qn
```

Pour supprimer l'application en mode non interactif avec redémarrage de l'ordinateur, saisissez :

```
msiexec /x <nom_du_paquetage> 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 avec définition d'un mot de passe confirmant le privilège de suppression de l'application, saisissez :

`msiexec /x <nom_du_paquetage> KLUNINSTPASSWD=******` : supprime l'application en mode interactif ;

`msiexec /x <nom_du_paquetage> KLUNINSTPASSWD=****** /qn` : supprime l'application en mode non interactif.

ANNEXE A. AIDE

Cette annexe contient des informations sur le format des fichiers analysés, sur les masques autorisés et sur l'utilisation de ceux-ci lors de la configuration de Kaspersky Anti-Virus.

A.1. Liste des objets analysés en fonction de l'extension

Si vous avez coché la case **Analyser les programmes et les documents (selon l'extension),** Antivirus Fichiers ou la tâche de recherche de virus réalisera une analyse minutieuse des fichiers portant l'extension suivante :

com : fichier exécutable d'un logiciel .

exe : fichier exécutable, archive autoextractible.

sys : pilote système.

prg : texte du programme dBase, Clipper ou Microsoft Visual FoxPro, programme de la suite WAVmaker.

bin : fichier binaire.

bat : fichier de paquet.

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2.

dpl : bibliothèque Borland Delphi compactée.

dll : bibliothèque dynamique.

scr : fichier d'économiseur d'écran de Microsoft Windows.

cpl : module du panneau de configuration de Microsoft Windows.

ocx : objet Microsoft OLE (Object Linking and Embedding).

tsp : programme qui fonctionne en mode de partage du temps.

drv : pilote d'un périphérique quelconque.

vxd : pilote d'un périphérique virtuel Microsoft Windows.

pif : fichier contenant des informations sur un logiciel.

lnk : fichier lien dans Microsoft Windows.

reg : fichier d'enregistrement des clés de la base de registres système de Microsoft Windows.

ini : fichier d'initialisation.

cla : classe Java.

vbs : script Visual Basic.

vbe : extension vidéo BIOS.

js, jse : texte source JavaScript.

htm : document hypertexte.

htt : préparation hypertexte de Microsoft Windows.

hta : programme hypertexte pour Microsoft Internet Explorer.

asp : script Active Server Pages.

chm : fichier HTML compilé

pht : fichier HTML avec scripts PHP intégrés.

php : script intégré dans les fichiers HTML.

wsh : fichier Microsoft Windows Script Host.

wsf : script Microsoft Windows.

hlp : fichier d'aide au format Win Help.

eml : message électronique de Microsoft Outlook Express.

nws : nouveau message électronique de Microsoft Outlook Express.

msg : message électronique de Microsoft Mail.

plg : message électronique

mbx : extension des messages Microsoft Office Outlook sauvegardés.

*doc** : document Microsoft Office Word, par exemple: *doc* – document Microsoft Office Word, *docx* – document Microsoft Office Word 2007 compatible avec XML, *docm* – document Microsoft Office Word 2007 compatible avec les macros.

*dot** : modèle de document Microsoft Office Word, например, *dot* – modèle de document Microsoft Office Word, *dotx* – modèle de document Microsoft Office Word 2007, *dotm* – modèle de document Microsoft Office Word 2007 compatible avec les macros.

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro.

rtf : document au format Rich Text Format.

shs : fragment de Shell Scrap Object Handler.

dwg : base de données de dessins AutoCAD.

msi : paquet Microsoft Windows Installer.

otm : projet VBA pour Microsoft Office Outlook.

pdf : document Adobe Acrobat.

swf : objet d'un paquet Shockwave Flash.

jpg, jpeg : fichier graphique de conservation de données compressées.

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows. Les fichiers EMS ne sont pas pris en charge par Microsoft Windows 16 bit.

ico : fichier d'icône de l'objet

ov? : fichiers exécutable MS DOC

*xl** : documents et fichiers de Microsoft Office Excel tels que : *xla*, extension Microsoft Excel ; *xlc* , schéma ; *xlt* , modèle de document, *xlsx* – feuille de calcul Microsoft Office Excel 2007, *xltm* – feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, *xlsb* – feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), *xltx* – modèle Microsoft Office Excel 2007, *xlsm* – modèle Microsoft Office Excel 2007 compatible avec les macros, *xlam* – modèle externe Microsoft Office Excel 2007 compatible avec les macros.

*pp** : documents et fichiers de Microsoft Office PowerPoint tels que : *pps* , dia Microsoft Office PowerPoint ; *ppt* , présentation, *pptx* – présentation Microsoft Office PowerPoint 2007, *pptm* – présentation Microsoft Office PowerPoint 2007 compatible avec les macros, *potx* – modèle de présentation Microsoft Office PowerPoint 2007, *potm* – modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, *ppsx* – diaporama Microsoft Office PowerPoint 2007, *ppsm* – diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, *ppam* – module externe Microsoft Office PowerPoint 2007 compatible avec les macros.

*md** : documents et fichiers de Microsoft Office Access tels que : *mda* , groupe de travail de Microsoft Office Access ; mdb, base de données, etc.

sldx : diaporama Office PowerPoint 2007.

sldm : diaporama Office PowerPoint 2007 compatible avec les macros.

thmx : thème Microsoft Office 2007.

N'oubliez pas que le format du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

A.2. Masques autorisés pour l'exclusion de fichiers

Voici des exemples de masques que vous utilisez lors de la constitution de la liste d'exclusions des fichiers :

- Masques sans chemin vers les fichiers :
  - ***.exe** : tous les fichiers **.exe*
  - ***.exe?** tous les fichiers **.ex?* où " ? " représente n'importe quel caractère
  - **test** : tous les fichiers portant le nom *test*

- Masque avec chemin d'accès absolu aux fichiers :
  - **C:\dir*.*** ou **C:\dir* C:\dir** : tous les fichiers du répertoire *C:\dir*
  - **C:\dir*.exe** : tous les fichiers *.exe du répertoire *C:\dir*
  - **C:\dir*.ex?** tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère unique
  - **C:\dir\test** : uniquement le fichier *C:\dir\test*

  Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case ☑ **Sous-répertoires compris**.
- Masque avec chemin d'accès relatifs 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 **.exe* dans tous les répertoires *dir*
  - **dir*.ex?** tous les fichiers **.ex?* dans tous les répertoires *dir* où " ? " peut représenter n'importe quel caractère unique

  Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case ☑ **Sous-répertoires compris**.

Conseil.

L'utilisation du masque ***.*** ou * est autorisée uniquement lorsque l'exclusion est indiquée selon la classification de l'encyclopédie des virus. Dans ce cas, la menace indiquée ne sera pas identifiée dans les objets. L'utilisation de ces menaces sans indication de la classification revient à désactiver la protection en temps réel.

Il est également déconseillé de sélectionner parmi les exclusions le disque virtuel créé sur la base du répertoire du système de fichiers à l'aide de la commande *subst*. Cela n'a pas de sens car pendant l'analyse, le logiciel considère ce disque virtuel comme un répertoire et, par conséquente, l'analyse.

A.3. Masques d'exclusion autorisés selon la classification de l'encyclopédie des virus

Pour ajouter des menaces en guise d'exclusion selon la classification de l'encyclopédie des virus, vous pouvez indiquer :

- le nom complet de la menace, tel que **repris** dans l'encyclopédie des virus sur http://www.viruslist.com/fr (ex. **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.

A.4. Description des paramètres du fichier *setup.ini*

Le fichier *setup.ini* situé dans le répertoire de fichier d'installation de Kaspersky Anti-Virus intervient lors de l'installation de l'application en mode non interactif via la ligne de commande (cf. point 3.3 à la page 33) ou via l'éditeur d'objet de stratégie de groupe (cf. point 3.4, p. 34). Il contient les paramètres suivants :

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

InstallDir=<chemin d'accès au répertoire d'installation de l'application >.

Reboot=yes|no – détermine s'il faut redémarrer au non l'ordinateur à la fin de l'installation de l'application (le redémarrage n'a pas lieu par défaut).

SelfProtection=yes|no – détermine s'il faut activer l'autodéfense de Kaspersky Anti-Virus lors de l'installation (l'autodéfense est activée par défaut).

MSExclusions=yes|no – détermine s'il faut ajouter à la liste des exclusions de Kaspersky Anti-Virus les exclusions recommandées par Microsoft pour les serveurs.

AddPath=yes|no – détermine s'il faut ajouter le chemin d'accès à avp.com à la variable %Path%.

[Components] : sélection des composants de l'application à installer. Si ce groupe ne contient aucun élément, alors l'application sera installée en entier.

FileMonitor=yes|no : installation du composant Antivirus Fichiers.

[Tasks] : activation des tâches de Kaspersky Anti-Virus. Si aucune tâche n'est sélectionnée, toutes les tâches seront activées après l'installation. Si une touche est activée, les autres tâches ne le seront pas.

ScanMyComputer=yes|no : tâche d'analyse complète de l'ordinateur.

ScanStartup=yes|no : tâche d'analyse des objets de démarrage.

ScanCritical=yes|no : tâche d'analyse des secteurs critiques.

Updater=yes|no : tâche de mise à jour des signatures de menace 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** .

ANNEXE B. 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, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : 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. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la “météo” des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d’informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S’abonner et se désabonner aux canaux d’information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d’informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l’information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s’agit d’un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l’ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l’analyse, l’utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l’analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.
- Surveiller les modifications de la base de registres système grâce au contrôle de l'état de la base de registres.

- **Le** contrôle **des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique**. Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.
- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles

est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont:

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel :** tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;

- **Protection contre les sms et mms indésirables.**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;

- *Génération de rapports détaillés* ;
- *Mise à jour automatique des bases* de l'application.

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable.* ;
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;

- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Blocage des fenêtres pop up et des bannières publicitaires* pendant la navigation sur Internet ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Outils de création d'un disque de démarrage* capable de restaurer le système après une attaque de virus ;
- *Système développé de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables* (technologie Intel® Centrino® Duo pour ordinateurs portables) ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Répartition de la charge entre les processeurs du serveur* ;
- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases*.

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers* ;
- *Protection des serveurs de messagerie Sendmail, Qmail, Posftix et Exim* ;
- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Prévention des épidémies de virus et des diffusions massives* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Utilisation sécurisée des réseaux sans fil* Wi-Fi ;
- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes dans le système* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;
- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™);
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino,

Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Filtrage des messages non sollicités* ;
- *Analyse des messages et des pièces jointes du courrier entrant et sortant* ;
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Filtrage des messages* en fonction du type de pièce jointe ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* du logiciel ;
- *Prévention des épidémies de virus* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Système de rapports* sur l'activité de l'application ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.

- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Analyse du trafic Internet* (HTTP/FTP) en temps réel ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* ;
- *Système de rapports sur le fonctionnement de l'application* ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

B.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la

mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique*.

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez,

fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

--- Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.