KASPERSKY LAB

Kaspersky Anti-Virus 7.0

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS 7.0

Manuel de l'utilisateur

NB : Cette documentation, traduite en français à partir du russe, décrit les fonctionnalités et services inclus avec la version russe. Il se peut que certaines fonctionnalités ou services décrits, ne soient pas disponibles en France.

http://www.kaspersky.com

Révision date: décembre, 2007

Contents

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 soumises au risque. Les particuliers peuvent également devenir des victimes. Les criminels, grâces à divers moyens, peuvent accéder 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'élément 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 ou 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 ou le particulier qui utilise son ordinateur. 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 ordinateurs personnels ou des serveurs d'entreprise distants. 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.

La popularité croissante des cartes de crédit et des paiements électroniques utilisés pour régler des achats en ligne (magasins en ligne, ventes aux enchères, sites de banque, etc.) s'accompagne d'une augmentation du nombre d'escroqueries en ligne qui sont devenues l'un des crimes les plus répandus.

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 plus important. 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.

En plus du risque d'être infecté par un programme malveillant, il y a également le problème lié à la réception de messages non sollicités. Bien que le courrier indésirable ne constitue pas une menace directe, il augmente la charge des serveurs de messagerie, génère un trafic complémentaire, encombre les boîtes aux lettres et entraîne une perte de temps productif, ce qui peut avoir des répercussions financières sérieuses.

Il convient de noter que les individus mal intentionnés ont commencé à recourir aux technologies de diffusion massive du courrier indésirable et à

l'ingénierie sociale pour amener l'utilisateur à ouvrir le message, à cliquer sur un lien vers un site quelconque, etc. Pour cette raison, la possibilité de filtrer le courrier indésirable est importante en elle-même mais également pour lutter contre les nouveaux types d'escroquerie en ligne comme le phishing ou la diffusion de programmes malveillants.

Média amovibles

Les disques amovibles (disquettes, cédéroms/DVD, 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 courrier électronique. Cette technique permet à de nombreux vers de se diffuser à une très grande vitesse.

Ils s'introduisent dans l'ordinateur, relèvent les adresses de réseau des autres ordinateurs 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. Il vous est certainement déjà arrivé de cliquer de vouloir accéder à un site particulier et de vous retrouvez sur la page d'accueil d'un site totalement différent.

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 préviennent souvent les utilisateurs d'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 outils de dissimulation d'activité 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 réseau ou du système attaqué.

Kaspersky Anti-Virus identifie et bloque ces différentes menaces en exploitant deux méthodes :

- *méthode réactive* : cette méthode repose sur la recherche des objets malicieux à l'aide des bases de l'application actualisées en permanence.

Cette méthode requiert au moins une infection pour ajouter la signature de la menace aux bases et diffuser la mise à jour.

- *méthode proactive* : au contraire de la méthode réactive qui repose sur l'analyse du code de l'objet, l'analyse proactive implique l'analyse du comportement de l'objet dans le système. Cette méthode permet d'identifier de nouvelles menaces qui ne sont pas encore reprises dans les bases.

En adoptant ces deux méthodes, Kaspersky Anti-Virus peut garantir la protection sophistiquée de votre ordinateur contre les nouvelles menaces ou les menaces inconnues.

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.

1.4. Signes d'une infection

Il existe toute une série d'indices qui peuvent indiquer l'infection de l'ordinateur. Si vous remarquez que votre ordinateur a un comportement bizarre, comme

- Des messages, des images ou des sons imprévus se manifestent ;
- L'ouverture et la fermeture inattendue du lecteur de CD/DVD-ROM;
- Le lancement aléatoire d'une application quelconque sans votre intervention;
- L'affichage d'un avertissement relatif à la tentative réalisée par un programme de se connecter à Internet bien que vous n'ayez pas lancé cette action,
- vous êtes alors plus que probablement victime d'un virus informatique.

Certains symptômes laissant présager une infection se manifestent également via le courrier électronique :

- Vos amis ou vos connaissances parlent de vos messages alors que vous ne leur avez rien envoyé ;
- Votre boîte aux lettres contient énormément de messages sans objet et sans adresse d'expéditeur.

Il convient de préciser que ces signes n'indiquent pas toujours la présence de virus. Ils peuvent être en effet la manifestation d'un autre problème. Ainsi, il est

possible que les messages infectés reprennent votre adresse en tant qu'adresse de l'expéditeur même s'ils ont été envoyés depuis un autre ordinateur.

L'infection de votre ordinateur peut également se manifester au travers de toute une série de signes secondaires :

- Gel et échecs fréquents dans le fonctionnement de l'ordinateur ;
- Lenteur au moment du lancement des logiciels ;
- Impossibilité de charger le système d'exploitation ;
- Disparition de fichiers et de répertoires ou altération de leur contenu ;
- Requêtes fréquentes vers le disque dur (la petite lampe sur la tour clignote fréquemment) ;
- Le navigateur (par exemple, Microsoft Internet Explorer) « plante » ou se comporte bizarrement (ex. :impossible de fermer les fenêtre du logiciel).

Dans 90% des cas, ces symptômes sont causés par des problèmes matériels ou logiciels. Même si ces symptômes ne sont pas nécessairement la manifestation d'une infection, il est fortement conseillé de réaliser une analyse complète de l'ordinateur (cf. point 5.3, p. 55).

1.5. Que faire lorsque les symptômes d'une infection sont présents ?

Si vous remarquez que votre ordinateur a un comportement suspect :

1. Ne paniquez pas ! La règle d'or dans ce type de situation est de garder son calme afin d'éviter de supprimer des données importantes.
2. Déconnectez l'ordinateur d'Internet et, le cas échéant, du réseau local.
3. Si le symptôme observé vous empêche de démarrer l'ordinateur depuis le disque dur (un message d'erreur apparaît lorsque vous allumez l'ordinateur), essayez de démarrer en mode Sans échec ou au départ du disque de secours de Microsoft Windows que vous avez créé au moment de l'installation du système d'exploitation.
4. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD/DVD, une carte Flash, etc.
5. Installez Kaspersky Anti-Virus, si cela n'a pas encore été fait.

6. Actualisez les bases (cf. point 5.6, p. 58) et les modules du programme. Dans la mesure du possible, réalisez cette opération depuis l'ordinateur sain d'un ami, d'un cybercafé ou du travail. Il est en effet préférable d'utiliser un autre ordinateur car si le vôtre est bel et bien infecté, sa connexion à Internet permettra plus que probablement au virus d'envoyer des informations importantes à une personne mal intentionnée ou de se propager en envoyant une copie à tous les contacts de votre carnet d'adresses. C'est pour cette même raison qu'il est toujours conseillé de déconnecter votre ordinateur d'Internet si vous soupçonnez une infection. Il est possible également d'obtenir les mises à jour sur une disquette ou sur un disque en s'adressant à Kaspersky Lab ou à l'un de ses distributeurs. Dans ce cas, la mise à jour s'effectue localement.
7. Définissez le niveau de protection défini par les experts de Kaspersky Lab.
8. Lancez l' analyse complète de l'ordinateur (cf. point 5.3, p. 55).

1.6. Préventions des infections de votre ordinateur

Il n'existe aucune mesure fiable et raisonnable qui puisse réduire à zéro le risque d'infection de votre ordinateur par des virus ou des chevaux de Troie. Toutefois, vous pouvez réduire considérablement ce risque en suivant un certain nombre de règles.

Tout comme en médecine, la *prévention* est une des méthodes de base à appliquer pour lutter contre les virus. La prévention informatique repose sur un nombre restreint de règles dont le respect réduira fortement le risque d'infection par un virus et le danger de perdre des données quelconques.

Vous trouverez ci-après des règles de base en matière de sécurité informatique qui vous permettront d'éviter le risque d'attaques de virus.

Règle N°1 : *Protégez votre ordinateur à l'aide d'un antivirus et de logiciels assurant la sécurité de l'utilisation d'Internet. Pour ce faire* :

- Installez sans plus attendre Kaspersky Anti-Virus.
- Actualisez (cf. point 5.6, p. 58) régulièrement les signatures des menaces livrées avec le logiciel. Réalisez cette opération plusieurs fois par jour en cas d'épidémie (les bases de l'applications sont publiées sur les serveurs de mises à jour de Kaspersky Lab immédiatement dans ce genre de situation).

- Configurez les paramètres de protection recommandés par les experts de Kaspersky Lab. La protection en temps réel est active dès le démarrage de l'ordinateur et complique la tâche des virus qui souhaiteraient l'infecter.
- Appliquez les paramètres recommandés par les experts de Kaspersky Lab pour l'analyse complète de l'ordinateur et prévoyez son exécution au moins une fois par semaine.

Règle N°2 : *Soyez prudent lors de l'enregistrement de nouvelles données sur l'ordinateur* :

- Recherchez la présence d'éventuels virus dans tous les disques amovibles (cf. point 5.5, p. 57) (disquettes, CD/DVD, cartes Flash, etc.) avant de les utiliser.
- Traitez les courriers électroniques avec prudence. N'ouvrez jamais les fichiers que vous recevez par courrier électronique si vous n'êtes pas certain qu'ils vous sont bel et bien destinés, même s'ils ont été envoyés par vos connaissances.
- Soyez attentif aux données reçues depuis Internet. Si un site Internet vous invite à installer une nouvelle application, veillez à vérifier son certificat de sécurité.
- Lorsque vous copiez un fichier exécutable depuis Internet ou depuis un répertoire local, analysez-le avec Kaspersky Anti-Virus avant de l'ouvrir.
- Soyez prudent dans le choix des sites que vous visitez. En effet, certains sites sont infectés par des virus de script dangereux ou par des vers Internet.

Règle N°3 : *Suivez attentivement les informations diffusées par Kaspersky Lab*.

Généralement, Kaspersky Lab avertit ses utilisateurs de l'existence d'une nouvelle épidémie bien longtemps avant qu'elle n'atteigne son pic. A ce moment, le risque d'infection est encore faible et le téléchargement des bases de l'application actualisées en temps opportun vous permettra de vous protéger.

Règle N°4 : *Ne croyez pas les canulars présentés sous la forme d'un message évoquant un risque d'infection*.

Règle N°5 : *Utilisez Windows Update et installez régulièrement les mises à jour du système d'application Microsoft Windows*.

Règle N°6 : *Achetez les copies d'installation des logiciels auprès de vendeurs agréés*.

Règle N°7 : *Limitez le nombre de personnes autorisées à utiliser votre ordinateur*.

Règle N°8 : *Réduisez le risque de mauvaises surprises en cas d'infection* :

- Réalisez régulièrement des copies de sauvegarde de vos données. Celles-ci vous permettront de restaurer assez rapidement le système en cas de perte de données. Conservez en lieu sûr les CD/DVD et les disquettes d'installation ainsi que tout média contenant des logiciels et des informations de valeur.

- Créez un disque de secours (cf. point 15.4, p. 190) qui vous permettra, le cas échéant, de redémarrer l'ordinateur à l'aide d'un système d'exploitation « sain ».

Règle N°9 : *Consultez régulièrement la liste des programmes installés sur votre ordinateur*. Pour ce faire, vous pouvez utiliser le service **Ajouter/Supprimer des programmes** dans le **Panneau de configuration** ou ouvrez simplement le répertoire **Programmes**, le dossier de démarrage automatique. Vous pourrez ainsi découvrir les logiciels qui ont été installés sur votre ordinateur à votre insu, par exemple pendant que vous utilisiez Internet ou installiez un autre programme. Certains d'entre eux sont probablement des riskwares.

CHAPITRE 2. KASPERSKY ANTI-VIRUS 7.0

Kaspersky Anti-Virus 7.0 représente la nouvelle génération de solution de protection des données.

Ce qui différencie Kaspersky Anti-Virus 7.0 des produits existants, et notamment des autres logiciels de Kaspersky Lab, Ltd., c'est l'approche complexe adoptée pour protéger les données de l'utilisateur. Ce logiciel assure la protection contre tous les types de menaces existantes à l'heure actuelle, mais également contre les menaces à découvrir, ce qui est tout aussi important.

2.1. Nouveautés de Kaspersky Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 représente une approche révolutionnaire dans le domaine de la protection des données. Tout d'abord, ce programme regroupe toutes les fonctions de tous les logiciels de la société au sein d'une solution de protection complexe. Ce programme vous protégera non seulement contre les virus, mais également contre le courrier indésirable et les attaques des pirates informatiques. Les nouveaux modules offrent également une protection contre les menaces inconnues, contre certains types d'escroqueries en ligne ainsi qu'un contrôle de l'accès des utilisateurs à Internet.

Il n'est plus indispensable d'installer plusieurs logiciels afin d'assurer la sécurité complète. Il suffit simplement d'installer Kaspersky Anti-Virus 7.0.

Tous les canaux de transfert d'informations sont couverts par la protection sophistiquée. La souplesse de la configuration de chacun des composants permet d'adapter au maximum Kaspersky Anti-Virus aux besoins de chaque utilisateur. La configuration unique de tous les composants est possible également.

Examinons maintenant en détails les nouveautés de Kaspersky Anti-Virus 7.0.

Nouveautés au niveau de la protection

- Désormais, Kaspersky Anti-Virus vous protège non seulement contre les programmes malveillants connus, mais également contre ceux qui ne le sont pas encore. Le composant de défense proactive (cf. Chapitre 10, p. 121) constitue le principal avantage du logiciel. Il analyse le comportement des applications installées, est à l'affût de changement dans la base de registre et lutte contre les menaces dissimulées. Le compo-

sant exploite un module d'analyse heuristique qui permet d'identifier divers types de programmes malveillants. Il maintient un historique de l'activité malveillante pour annuler les actions des programmes malveillants et rétablir le système à son état antérieur à l'intervention du code malveillant.

- Modification de la technologie de protection des fichiers sur l'ordinateur de l'utilisateur : de réduire la charge sur le processeur central et les sous-systèmes de disque. Ce résultat est obtenu grâce au recours aux technologies iChecker ™ et iSwift ™. Ainsi, les fichiers qui n'ont pas été modifiés depuis la dernière analyse peuvent être ignorés.

- 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'utilisateur 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 et des objets de démarrage, ceux dont l'infection entraînerait des conséquences irréversibles ainsi que la découverte de Rootkit qui cachent les programmes malveillants dans le système, sont reprises dans une tâche séparée. Vous pouvez configurer ces tâches de telle sorte qu'elles soient lancées automatiquement à chaque démarrage du système.

- La protection du courrier sur l'ordinateur de l'utilisateur, tant contre les programmes malveillants que contre le courrier indésirable, a été considérablement améliorée. Le logiciel analyse n'importe quel message et recherche les messages non sollicités dans le flux de messagerie des protocoles suivants :

  - IMAP, SMTP et POP3 quel que soit le client de messagerie utilisé ;

  - NNTP (recherche de virus uniquement), quel que soit le client de messagerie ;

  - Quel que soit le type de protocole (y compris MAPI, HTTP) dans le cadre des plug-ins intégrés à Microsoft Office Outlook et TheBat!.

- Des plug-ins permettant de configurer directement la protection du courrier contre les virus et le courrier indésirable dans le système de messagerie ont été intégrés aux clients de messagerie les plus connus comme Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) et The Bat!

- Protection contre les programmes de dissimulation, les dialers vers des sites Web payant, blocage des fenêtres pop up, des bannières publicitaires et des scripts dangereux téléchargés depuis des pages Web et

identification des sites de phishing ainsi que la protection contre le transfert non autorisé des données confidentielles (par exemple, mot de passe d'accès à Internet, aux boîtes de messagerie, aux serveurs ftp).

- Elargissement de la fonction de notification de l'utilisateur (cf. point 15.9.1, p. 203) 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.
- Analyse du trafic transitant sur les connexions sécurisées via SSL.
- Ajout de la technologie d'autodéfense du logiciel, de protection contre l'administration à distance non-autorisée du service de Kaspersky Anti-Virus 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.
- Possibilité de créer un disque de secours pour la restauration du système. Ce disque vous permettra de réaliser le chargement initial du système d'exploitation après une attaque de virus et de rechercher la présence d'objets malveillants sur l'ordinateur.
- Ajout du NewsAgent, un module conçu pour diffuser les informations de Kaspersky Lab

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 créant et 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 et offre une rubrique d'aide détaillée. L'Assistant de sécurité, inclus dans l'application, dresse le tableau complet de la protection actuelle de l'ordinateur et permet de résoudre les problèmes immédiatement.

Nouveautés au niveau de la mise à jour du programme

- Cette version du logiciel intègre une procédure de mise à jour améliorée : Kaspersky Anti-Virus vérifie automatiquement la présence de fichiers de mise à jour sur la source. S'il identifie des actualisations récentes, l'application 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.

- Il est désormais possible de ne pas utiliser un serveur proxy si la mise à jour du logiciel est réalisée au départ d'une source locale. Cela permet de réduire considérablement le volume du trafic qui transite via le serveur proxy.
- 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 bases de l'application.
- 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 est configurée en fonction de la source de la menace. Autrement dit, un composant est prévu pour chaque source. Ce composant contrôle la source et prend les mesures qui s'imposent pour éviter toute action malveillante en provenance de cette source sur les données de l'utilisateur. Cette conception du système de protection permet d'utiliser en souplesse et de configurer l'application en fonction des besoins d'un utilisateur particulier ou de l'entreprise dans son ensemble.

Kaspersky Anti-Virus comprend :

- Des composants de protection en temps réel (cf. point 2.2.1, p. 24) qui protège tous les canaux de transfert de données de et vers votre ordinateur.
- Des tâches de recherche de virus (cf. point 2.2.2, p. 25) qui procède à la recherche d'éventuels virus dans l'ordinateur ou dans des fichiers, des répertoires, des disques ou des secteurs particuliers.
- La mise à jour (cf. chapitre 2.2.3 à la page 26), garantit l'actualité des modules internes de l'application et des bases utilisées pour la recherche des programmes malveillants, l'identification des attaques de réseau et le filtrage du courrier indésirable.
- Des services (cf. point 2.2.3, p. 26) qui garantissent le soutien information dans le cadre de l'utilisation du logiciel et qui permettent d'en élargir les fonctions.

2.2.1. Composants de protection en temps réel

La protection en temps réel de l'ordinateur est assurée par les composants de la protection suivants :

Antivirus Fichiers

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

L'antivirus fichiers est le composant qui contrôle le système de fichiers de l'ordinateur. Il analyse tous les fichiers ouverts, exécutés et enregistrés sur l'ordinateur et tous les disques connectés. Chaque requête adressée à un fichier sera interceptée par l'application et le fichier sera soumis à une analyse antivirus pour trouver des virus connus. 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 15.2, p. 179)ou mis en quarantaine (cf. point 15.1, p. 175).

Antivirus Courrier

Le courrier électronique est souvent utilisé par les personnes malveillantes pour diffuser les programmes malveillants. Il s'agit d'un des principaux vecteurs de diffusion des vers. Pour cette raison, il est capital de contrôler tous les messages électroniques.

L'*antivirus de courrier électronique* est le composant qui analyse tout le courrier entrant et sortant de l'ordinateur. Il recherche la présence éventuelle de programmes malicieux dans les messages électroniques. Le destinataire pourra accéder au message uniquement si ce dernier ne contient aucun objet dangereux.

Antivirus Internet

Lorsque vous ouvrez différents sites Internet, vous risquez d'infecter votre ordinateur avec les virus associés aux scripts exécutés sur le site ou de télécharger des objets dangereux.

L'antivirus Internet a été tout spécialement conçu pour éviter de telles situations. Ce composant intercepte le script du site et bloque son exécution si le script constitue une menace. Tout le trafic http est également surveillé de près.

Défense proactive

Le nombre de programmes malveillants augmente chaque jour, ils deviennent plus sophistiqués, regroupent les propriétés de divers types, les méthodes de diffusion changent et ils deviennent de plus en plus difficile à identifier.

Afin pouvoir identifier un nouveau programme malveillant avant qu'il n'ait pu causer des dégâts, Kaspersky Lab a mis au point un composant spécial : *la défense proactive*. Il repose sur le contrôle et l'analyse du comportement de tous les programmes installés. Sur la base des actions réalisées, Kaspersky Anti-Virus décide s'il s'agit d'un programme potentiellement dangereux ou non. Ainsi, votre ordinateur est protégé non seulement contre les virus connus mais également contre ceux qui n'ont pas encore été étudiés.

2.2.2. Tâches de recherche de virus

En plus de la protection en temps réel 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 les composants de la protection en temps réel en raison d'un niveau de protection trop bas ou de tout autre motif.

Kaspersky Anti-Virus contient 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

Recherche de Rootkit

Recherche la présence éventuelle de Rootkit qui dissimulent les programmes malveillants dans le système d'exploitation. Ces utilitaires s'insèrent dans le système en dissimulant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité.

Il est possible également de créer d'autres tâches de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des boîtes aux lettres de messagerie une fois par semaine ou une tâche pour la recherche d'éventuels virus dans le répertoire **Mes documents**.

2.2.3. Mise à jour

Afin d'être toujours prêt à repousser n'importe quelle attaque de pirate ou à neutraliser tout virus ou programme malveillant, 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 bases et des modules de Kaspersky Anti-Virus utilisés.

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

2.2.4. 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.

Rapports

Un rapport est généré pendant l'utilisation du programme pour chaque composant, chaque tâche de recherche de virus exécutée ou mise à jour. Ce rapport contient les informations relatives aux opérations exécutées et à leur 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 faudra absolument restaurer l'objet ou le scénario de son infection. Les copies de sauvegarde des objets sont également chiffrées afin d'éviter l'infection de l'ordinateur. Il est possible de restaurer la copie de sauvegarde depuis ce dossier vers son emplacement d'origine ou de la supprimer.

Activation

Lorsque vous achetez Kaspersky Anti-Virus, vous entrez dans un contrat de licence entre vous et Kaspersky Lab. Ce contrat vous permet d'utiliser l'application et d'accéder aux mises à jour de l'application et au service d'assistance technique pendant une certaine période. La durée de validité de la licence ainsi que d'autres informations indispensables au fonctionnement de toutes les fonctions sont reprises dans le fichier de licence.

Grâce à la rubrique *Activation*, vous pouvez obtenir de plus amples informations sur la licence que vous utilisez ainsi qu'acheter une nouvelle licence.

Assistance technique

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

A l'aide des liens prévus à cet effet, vous pouvez accéder au forum des utilisateurs des logiciels de Kaspersky Lab, envoyer des messages au service d'assistance technique sur les erreurs rencontrées ou des commentaires à l'aide des formulaires spéciaux prévus sur le site.

Le service d'assistance technique est accessible en ligne tout comme le service de casier personnel de l'utilisateur 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 7.0, l'ordinateur doit répondre aux conditions minimum suivantes :

Configuration générale :

- 50 Mo d'espace disque disponible.

- Lecteur de cédérom (pour installer Kaspersky Anti-Virus 7.0 à partir du cédérom).
- Microsoft Internet Explorer 5.5 ou suivant (pour la mise à jour des bases et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows 2000 Professional (Service Pack 4 ou suivant), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 ou suivant), Microsoft Windows XP Professional x64 Edition :

- Processeur Intel Pentium 300 Mhz ou supérieur (ou compatible).
- 128 Mo de mémoire vive disponible.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Processeur Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) ou supérieur (ou compatible).
- 512 Mo de mémoire vive disponible.

2.4. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus® 7.0 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/DVD ROM d'installation où les fichiers du logiciel sont enregistrés
- Selon le mode d'achat de votre logiciel (téléchargement ou boîte), la licence d'utilisation pour la durée acquise peut se trouver :
    - sous la forme d'un code d'activation de 20 caractères (exemple de format xxxxx-xxxxx-xxxxx-xxxxx) imprimé sur le manuel d'utilisation ou la pochette du CD/DVD-Rom,
    - sur le CD/DVDROM dans un fichier appelé clé de licence (xxxxxxx.key),
    - dans le programme d'installation lui-même,
- Le manuel de l'utilisateur avec le contrat de licence utilisateur imprimé à la fin de ce manuel.

Si vous achetez Kaspersky Anti-Virus® 7.0 en ligne, et dés la réception de votre paiement, vous recevrez un email contenant des liens personnels pointants sur La boutique en ligne de Kaspersky Lab pour télécharger :

- le fichier d'installation,
- la licence d'utilisation pour la durée acquise ,
- la version électronique du manuel (format Adobe PDF).

La licence utilisateur constitue l'accord juridique passé entre vous et Kaspersky Lab, stipulant les conditions d'utilisation du progiciel que vous avez acquis. Lisez la attentivement !

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS 7.0

Kaspersky Anti-Virus 7.0 peut être installé de diverses manières :

- En mode interactif à l'aide de l'Assistant d'installation (cf. point 3.3, p. 42) ; ce mode requiert la participation de l'utilisateur pendant le processus d'installation ;
- En mode silencieux ; l'installation de l'application s'opère au départ de la ligne de commande et ne requiert pas l'intervention de l'utilisateur (cf. point 3.1, p. 30).

Attention !

Avant de lancer l'installation de Kaspersky Anti-Virus, il est conseillé de quitter toutes les applications ouvertes.

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

Remarque.

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

Pour installer Kaspersky Anti-Virus, lancez le fichier d'installation qui se trouve sur le cédérom contenant le logiciel.

Le paquet d'installation (fichier portant l'extension **.msi*) de l'application sera lancé et le cas échéant, vous serez invité à rechercher l'existence d'une version plus récente de Kaspersky Anti-Virus sur les serveurs de Kaspersky Lab. Si un fichier d'installation est introuvable, vous serez invité à le télécharger. L'installation de l'application sera lancée à la fin de téléchargement. Si vous refusez de charger l'installation, l'installation de l'application sera poursuivie en mode normal.

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 entre l'utilisateur et Kaspersky Lab. Lisez-le attentivement est si vous acceptez les dispositions, sélectionnez l'option **J'accepte le 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 type d'installation

Cette étape vous invite à sélectionner le type d'installation le mieux adapté :

Installation rapide. Dans ce mode, Kaspersky Anti-Virus est installé complètement avec les paramètres définis par défaut et recommandés par les experts de Kapsersky Lab. L'Assistant d'activation de l'application (cf. point 3.2.2, p. 36) est lancé à la fin de la procédure.

Installation personnalisée. Dans ce cas, vous serez invité à sélectionner les composants de la protection à installer, le répertoire d'installation et à réaliser l'activation et la configuration initiale à l'aide d'un Assistant spécialisé (cf. point 3.2, p. 35).

En cas de sélection de la première option, l'installation sera réalisée sans intervention de l'utilisateur. Autrement dit, toutes les étapes présentées ci-après seront ignorées. Dans le deuxième cas, vous devrez saisir ou confirmer des données à chaque étape.

Etape 5. 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 7.0** – pour les systèmes 32 bits.
- **<Disque> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 7.0** – 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.

Attention !

Si vous saisissez le nom complet du répertoire manuellement, sachez qu'il ne peut pas contenir plus de 200 caractères, ni des caractères spéciaux.

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

Etape 6. Sélection des composants à installer

Remarque

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. Par défaut, les composants de la protection en temps réel et le composant de recherche de virus sont sélectionnés.

Pour sélectionner un composant à installer, il faut ouvrir le menu en cliquant sur le bouton gauche de la souris sur l'icône située à côté du nom du composant et sélectionner le point **Le composant sera installé sur un 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 sera inaccessible** dans le menu contextuel. N'oubliez pas qu'en décidant de ne pas installer tel ou tel composant, vous vous exposez à toute une série de programmes dangereux.

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

Etape 7. Utilisation des paramètres de l'application sauvegardés de la version antérieure

Cette étape constitue la préparation finale pour l'installation du logiciel sur votre ordinateur. Vous pouvez décider d'utiliser les paramètres de protection et les bases de l'application, si ceux-ci ont été enregistrés sur l'ordinateur lors de la suppression de la version antérieure de Kaspersky Anti-Virus.

Voyons comment utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Anti-Virus était déjà installée sur votre ordinateur et que, au moment de la supprimer, vous avez conservé les bases de l'application, vous pourrez les utiliser avec la version que vous installez. Pour ce faire, cochez la case ☑ **Bases de l'application.** Les bases livrées avec le programme ne seront dès lors pas copiées sur votre ordinateur.

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

Etape 8. Recherche d'autres logiciels antivirus

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation 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 dessous de la liste des logiciels antivirus découverts, vous pourrez décider de les supprimer automatiquement ou manuellement.

Si Kaspersky Anti-Virus 6.0 figure parmi cette liste, il est conseillé de conserver le fichier de licence utilisé par ce logiciel avant de supprimer manuellement. Vous pourrez en effet les utiliser en tant que licence pour Kaspersky Anti-Virus 7.0. Il est conseillé également de conserver les objets de la quarantaine et du dossier de sauvegarde. Ces objets seront placés automatiquement dans les répertoires correspondant de Kaspersky Anti-Virus et vous pourrez continuer à les manipuler.

En cas de suppression automatique de Kaspersky Anti-Virus 6.0, les informations relatives à l'activation seront conservées par le logiciel et saisies lors de l'installation de la version 7.0.

Attention!

Kaspersky Anti-Virus 7.0 est compatible avec les fichiers de clé des versions 6.0 et 7.0. Les clés utilisées pour les applications de la version 5.0 ne sont pas prises en charge.

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

Etape 9. Fin des préparatifs d'installation

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

En cas de première installation de Kaspersky Anti-Virus, 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.

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

Attention !

Pendant l'installation des composants chargés d'intercepter le trafic de réseau, les connexions ouvertes 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** reprend des informations relatives à la fin de l'installation de Kaspersky Anti-Virus sur votre ordinateur.

Si le redémarrage de l'ordinateur s'impose pour finaliser l'installation, le message correspondant s'affichera. Après le redémarrage, l'Assistant de configuration initiale de Kaspersky Anti-Virus sera lancé automatiquement.

Si le redémarrage de l'application n'est pas nécessaire pour finaliser l'installation, cliquez sur Suivant afin de passer à l'Assistant de configuration initiale du logiciel.

3.2. Assistant de configuration initiale

L'Assistant de configuration de Kaspersky Anti-Virus 7.0 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**.

Vous pouvez ignorer la configuration initiale lors de l'installation du programme en fermant l'Assistant. Vous pourrez lancer ultérieurement l'Assistant au départ de l'interface du logiciel en rétablissant les paramètres d'origine de Kaspersky Anti-Virus (cf. point 15.9.4, p. 210).

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 7.0. 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 7.0, cochez les cases adéquates.

3.2.2. Activation de l'application

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

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

La 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 licence ainsi que sa date d'expiration

3.2.2.1. Sélection du mode d'activation du programme

L'activation du logiciel se fait de différentes façons selon votre cas :

- **Activer à l'aide du code d'activation**. Sélectionnez cette option si vous êtes en possession d'un code d'activation. Sur la base de ce code, le fichier de licence qui vous donne accès à l'ensemble des fonctions de l'application pour toute la durée du contrat de licence vous sera envoyé.
- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous recevrez une licence gratuite dont la validité est limitée par le contrat de licence pour la version d'évaluation de l'application.
- **Utiliser la licence obtenue antérieurement**. Activez l'application à l'aide d'un fichier de licence obtenu précédemment pour Kaspersky Anti-Virus 7.0.
- **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 l'application une seule fois après l'installation).

Attention !

En cas de sélection des deux premières variantes d'installation de l'application, une connexion à Internet est requise. Si la connexion à Internet n'est pas disponible, vous pouvez réaliser l'activation plus tard (cf. Chapitre 14 à la page 172) depuis l'interface de l'application ou en vous connectant à Internet depuis un autre ordinateur afin d'obtenir le code d'activation en vous enregistrant sur le site 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 d'un code d'activation. Si vous achetez l'application en ligne, vous recevrez ce code par courrier électronique. Si vous avez le logiciel dans un magasin traditionnel, le code d'activation sera repris sur l'enveloppe contenant le disque d'installation.

Le code d'activation se présente sous la forme d'une série de chiffres et de lettres séparés par des traits d'union en 4 groupes de cinq chiffres, sans espace. Par exemple, 11AA1-11AAA-1AA11-1A111. Le code doit être saisi en caractères latins.

Si vous avez déjà suivi la procédure d'enregistrement des clients de Kaspersky Lab sur le site d'assistance technique et que vous possédez le numéro de client et le mot de passe, cochez la case **J'ai déjà le code client** et dans la partie inférieure de la fenêtre, saisissez les données requises.

Si vous ne vous êtes pas encore enregistré, cliquez sur **Suivant** sans cocher la case. Saisissez dans la partie inférieure de la fenêtre votre numéro de client et votre mot de passe si vous avez déjà suivi la procédure d'enregistrement de client de Kaspersky Lab et que vous possédez ces données. Si vous n'êtes pas encore enregistré, laissez ces champs vides. Dans ce cas, l'Assistant d'activation vous demandera de saisir vos coordonnées et de réaliser l'enregistrement. A la fin de l'enregistrement, vous recevrez un numéro de client et un mot de passe que vous devrez absolument citer pour obtenir l'assistance technique. En cas d'enregistrement via l'Assistant d'activation, le numéro de client sera visible dans la section **Assistance Technique** de la fenêtre principale de l'application (cf. point 15.10, p. 211).

3.2.2.3. Enregistrement de l'utilisateur

A cette étape de l'Assistant, vous devez indiquer vos coordonnées : courrier électronique, pays et ville de résidence. Cette information est requise par le service d'assistance technique de Kaspersky Lab afin de pouvoir vous identifier en tant qu'utilisateur enregistré.

Une fois que vous aurez saisi ces données, l'Assistant les enverra vers un serveur d'activation. Vous recevrez ensuite un numéro de client et un mot de passe d'accès à votre Casier personnel sur le site du service d'assistance technique. Pour obtenir des informations sur le numéro de client, consultez la rubrique **Assistance technique** (cf. point 15.10, p. 211) de la fenêtre principale de l'application.

3.2.2.4. Réception du fichier de licence

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

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

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

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

Remarque

En cas d'activation de cette manière, l'application reçoit du serveur non pas une clé physique avec l'extension **.key*, mais certaines données qui sont copiées dans la base de registres du système d'exploitation et dans le système de fichiers.

Pour obtenir le véritable fichier de clé, vous devez vous enregistrer en tant qu'utilisateur sur le site Internet de Kaspersky Lab.

3.2.2.5. Sélection du fichier de licence

Si vous possédez un fichier 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 avec l'extension *.key :*

Une fois la licence installée, les informations relatives à la licence utilisée 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.

3.2.2.6. 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, test bêta, évaluation, etc.) et date de fin de validité.

3.2.3. Sélection du mode de protection

Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de protection de l'application :

Elémentaire. Ce mode est sélectionné par défaut et répond aux besoins de la majorité des utilisateurs qui ne maîtrisent pas l'ordinateur ou les logiciels antivirus. Il prévoit le fonctionnement des composants de l'application au niveau de protection recommandé et l'alerte des utilisateurs uniquement en cas d'événement dangereux (par exemple, découverte d'un objet malveillants exécutant une action dangereuse).

Interactif. Ce mode offre une protection étendue des données de l'ordinateur par rapport à la protection élémentaire. Il permet de suivre les tentatives de modification des paramètres système et les activités suspectes. Toutes les actions citées ci-dessus peuvent être le résultat de programmes malveillants ou être normales dans le cadre du fonctionnement de logiciels utilisés sur votre ordinateur Vous devrez décider, pour chaque cas, d'autoriser ou non ces actions.

En cas de sélection de ce mode, précisez les cas où il doit être utilisé :

- **Activer la surveillance de Registre système**: affiche une demande de confirmation pour l'utilisateur en cas de découverte d'une tentative de modification des objets de la base de registres système.

  Si l'application est installée sur un ordinateur tournant sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64, les paramètres du mode interactif cités ci-après sont absents.

- **Activer le contrôle de l'intégrité de l'application** : affiche une demande de confirmation pour l'utilisateur en cas de tentative de chargement d'un module dans l'application contrôlée.

- **Activer la protection proactive étendue** : active l'analyse de toutes les activités suspectes des applications du système, y compris le lancement du navigateur avec les paramètres de la ligne de commande, l'insertion dans les processus du programme et l'insertion d'intercepteurs de boîtes de dialogue (ces paramètres sont désactivés par défaut).

3.2.4. Configuration de la mise à jour

La qualité de la protection de votre ordinateur dépend de l'actualité des bases 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 la source de la mise 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, l'application les télécharge et les installe. Ce mode est activé par défaut.
- **Tous les 1 jours** (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 mises à jour (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 la copie de la mise à jour dans un répertoire local), cliquez sur **Configuration**.

3.2.5. 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

L'analyse des objets de démarrage se produit automatiquement par défaut au lancement de Kaspersky Anti-Virus. Les paramètres de la programmation peuvent être modifiés dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **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), 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 de l'ordinateur directement après l'installation du logiciel.

3.2.6. Restriction de l'accès à l'application

Etant donné que l'ordinateur peut être utilisé par plusieurs personnes ne possédant pas toutes la même maîtrise de l'outil informatique et que la protection antivirus pourrait être désactivée par des programmes malveillants, il est possible d'introduire un mot de passe d'accès à Kaspersky Anti-Virus. Le mot de passe protège l'application 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 un mot de passe** et saisissez les informations dans les champs **Mot de passe** et **Confirmation**.

Indiquez ensuite les tâches qui seront concernées :

- **Toutes les opérations (sauf les notifications dangereuses)**. Le mot de passe est nécessaire pour lancer n'importe quelle action de l'application à l'exception de la manipulation des messages relatifs à la découverte d'objets dangereux.
- **Les opérations choisies** :
  - **Modification des paramètres de fonctionnement de l'application :** le mot de passe est requis lorsque l'utilisateur tente d'enregistrer les modifications apportées aux paramètres de l'application.
  - **Arrêt de l'application** : le mot de passe doit être saisi lorsque l'utilisateur tente de quitter l'application.

- **Arrêt/suspension des composants de la protection et des tâches d'analyse** : le mot de passe est requis pour suspendre ou arrêter n'importe quel composant de la protection en temps réel ou n'importe quelle tâche liée à la recherche de virus.

3.2.7. Contrôle de l'intégrité de l'application

A cette étape, Kaspersky Anti-Virus analyse les applications installées sur l'ordinateur (fichiers des bibliothèques dynamiques, signature numérique de l'éditeur), calcule les sommes de contrôle des fichiers des applications et crée une liste de programmes de confiance du point de vue de la sécurité antivirus. Par exemple, cette liste reprendra automatiquement toutes les applications qui possèdent la signature de Microsoft Corporation.

Par la suite, les informations obtenues pendant l'analyse de la structure de l'application seront utilisées par Kaspersky Anti-Virus pour éviter l'introduction de code malveillant dans le module de l'application.

L'analyse des applications installées sur l'ordinateur peut durer un certain temps.

3.2.8. Fin de l'Assistant de configuration

La dernière fenêtre de l'Assistant vous propose de redémarrer l'ordinateur afin de finaliser l'installation de l'application. Ce redémarrage est indispensable à l'enregistrement des pilotes de Kaspersky Anti-Virus.

Vous pouvez reporter le redémarrage de l'application, mais dans ce cas, certains composants de la protection ne fonctionneront pas.

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

Pour installer Kaspersky Anti-Virus, 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. 30). Il faut absolument redémarrer l'ordinateur après l'installation.

Pour installer l'application en mode caché (sans l'Assistant d'installation), saisissez :

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

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 dans la zone de notification de la barre des tâches de Microsoft Windows (cf. point 4.1, p. 43);
- Le menu contextuel (cf. point 4.2, p. 44);
- La fenêtre principale (cf. point 4.3, p. 46);

Fenêtre de configuration des paramètres du logiciel (cf. point 4.4, p. 50).

En plus de l'interface principale du logiciel, il existe des plug-in intégrés :

- Microsoft Office Outlook (cf. point 8.2.2, p. 104) ;
- TheBat! (cf. point 8.2.3, p. 105)
- Microsoft Internet Explorer (cf. Chapitre 9, p. 111).
- Microsoft Windows Explorer (cf. point 11.2, p. 141).

Ceux-ci élargissent les possibilité des programmes cités car ils permettent d'administrer et de configurer les composants correspondants de Kaspersky Anti-Virus directement depuis leur interface respective.

4.1. Icône dans la zone de notification de la barre des tâches

L'icône de Kaspersky Anti-Virus apparaît dans la zone de notification de 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 complètement activée et que tous ses composants fonctionnent. Si l'icô-

ne n'est pas activée (noir et blanc) cela signifie que tous composants de la protection sont désactivés (cf. point 2.2.1, p. 24).

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

	L'analyse d'un message électronique est en cours.
	L'analyse d'un script est en cours.
	L'analyse d'un fichier ouvert, enregistré ou exécuté par vous ou un programme quelconque est en cours.
	La mise à jour des bases et des modules logiciels de Kaspersky Anti-Virus est en cours.
	Il faut redémarrer l'ordinateur pour appliquer les mises à jour.
	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. 44) et la fenêtre principale (cf. point 4.3, p. 46);

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.

Quand des informations de Kaspersky Lab sont disponibles, l'icône apparaît dans la zone de notification de la barre des tâches de Microsoft Windows. Double-cliquez sur le bouton gauche de la souris et lisez le contenu des informations dans la fenêtre qui s'ouvre.

4.2. Menu contextuel

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

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

Analyse 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.

Analyse : passe à la sélection des objets et au lancement de la recherche de virus. Par défaut, la liste comprend toute une série d'objets comme le dossier **Mes documents**, les objets de démarrage, les boîtes aux lettres 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 bases et des modules de Kaspersky Anti-Virus et les installe sur l'ordinateur

Illustration 1. Menu contextuel

Activation : passe à l'activation du logiciel. Pour obtenir le statut d'utilisateur enregistré qui vous donnera droit à toutes les fonctions de l'application et au service d'assistance technique, il est indispensable d'activer votre copie 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. 46).

Suspension de la protection/Activation de la protection : désactive temporairement/active le fonctionnement des composants de la protection en temps réel (cf. point 2.2.1, p. 24). 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.

A propos du logiciel : affichage des informations relatives à Kaspersky Anti-Virus.

Quitter : quitte Kaspersky Anti-Virus (lorsque vous sélectionnez ce point du menu, l'application sera déchargée de la mémoire d'exploitation 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. ill. 2) de Kaspersky Anti-Virus est constituée de trois panneaux :

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

  Il existe trois types d'états de la protection (cf. point Chapitre 5, p. 52) et chacun est clairement indiqué par une couleur identique à celle d'un feu rouge. La lumière verte signale que la protection est assurée au bon niveau, tandis que le jaune et le rouge indiquent un problème de configuration ou de fonctionnement de Kaspersky Anti-Virus

  Pour obtenir des informations détaillées sur ces problèmes et pour les résoudre rapidement, utilisez l'Assistant de sécurité qui s'ouvre à l'aide du lien contenu dans les notifications relatives aux menaces sur la sécurité.

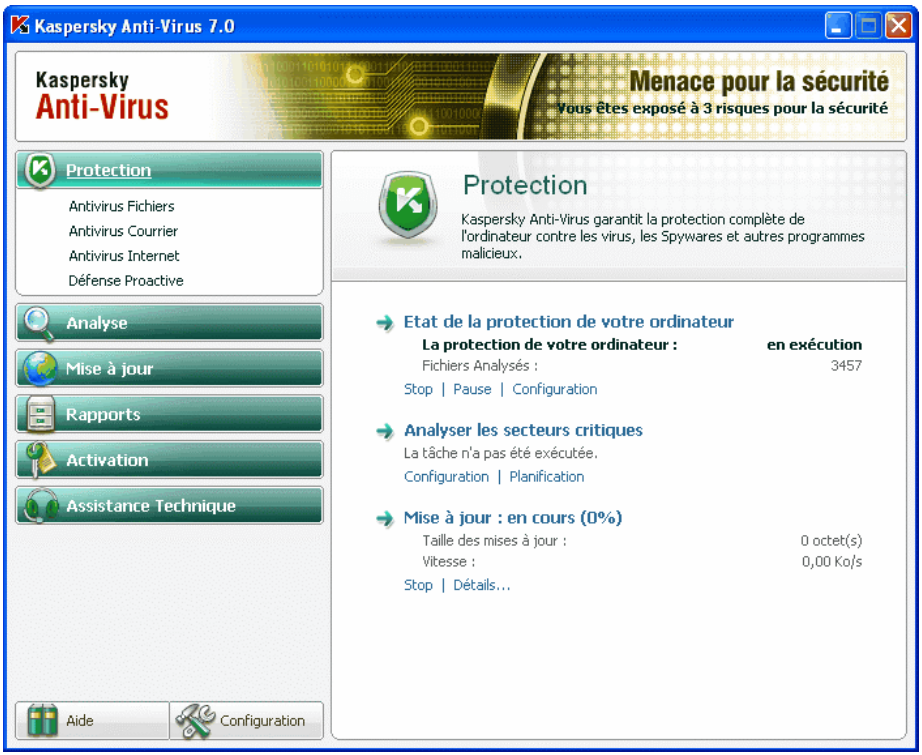
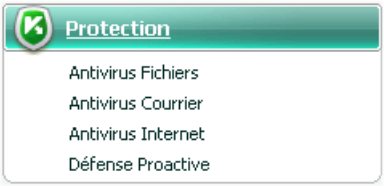


Illustration 2. Fenêtre principale de Kaspersky Anti-Virus

- Le panneau de gauche sert à la navigation et permet d'accéder rapidement et facilement à n'importe que composant, de lancer une mise à jour, une recherche de virus ou d'accéder au service de l'application
- Le panneau de droite est à caractère *informatif* : il contient les informations relatives au composant de la protection 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 licences, etc.

Dès que vous avez sélectionné une section ou un composant 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 principale fonction de la section **Protection** est d'offrir l'accès aux principaux composants de la protection en temps réel de votre ordinateur. Pour consulter les informations sur le fonctionnement d'un composant concret ou d'un de ses modules, pour le configurer ou pour ouvrir le rapport à son sujet, sélectionnez le composant souhaité dans la rubrique **Protection**. De plus, cette section propose des liens qui donnent accès aux tâches les plus souvent utilisées : analyse des objets et mise à jour des bases de l'application. Vous pouvez également consulter les informations sur l'état de ces tâches, les configurer ou les exécuter.
	La section **Analyse** donne accès aux tâches de recherche de virus dans les objets. Vous y retrouverez les tâches créées par les experts de Kaspersky Lab (recherche de virus dans les secteurs critiques et les objets de démarrage, analyse complète de l'ordinateur, recherche de Rootkit) ainsi que les tâches créées par l'utilisateur Suite à la sélection d'une tâche dans la partie droite de la fenêtre, vous pouvez consulter les informations relatives à l'exécution de celle-ci, passer à la configuration des paramètres, composer la liste des objets à analyser et exécuter la tâche. Pour analyser un objet en particulier (fichier, répertoire ou disque), sélectionnez la rubrique **Analyse** et dans la partie droite de la fenêtre, ajoutez l'objet à la liste puis lancez la tâche.

Section du panneau de navigation de la fenêtre principale	Fonction
	Cette rubrique vous permet également de créer un disque de démarrage (cf. point 15.4, p. 190).
	La section **Mise à jour** contient les informations relatives à la mise à jour de l'application : date de création des bases et nombre de signatures de virus contenues dans les bases. Grâce aux liens correspondants, vous pouvez lancer la mise à jour, consulter le rapport détaillé, passer à la configuration de la mise à jour ou revenir à l'état antérieur à la mise à jour.
	La section **Rapports** vous permet d'afficher un rapport détaillé sur le fonctionnement de chaque composant de l'application, sur les tâches de recherche de virus ou de mise à jour (cf. point 15.3, p. 182) et ainsi que de passer à la manipulation des objets qui se trouvent en quarantaine (cf. point 15.1, p. 175) ou dans le dossier de sauvegarde (cf. point 15.2, p. 179).
	La rubrique **Activation** est prévue pour la manipulation des licences indispensables à l'exploitation de toutes les fonctions de l'application (cf. Chapitre 14, p. 172). Si aucune licence n'est installée, il est conseillé d'en acheter une le plus rapidement possible et d'activer l'application (cf. point 3.2.2, p. 36). Si la licence est installée, cette rubrique présente les données relatives au type de licence utilisé et à sa durée de validité. Une fois que la licence est arrivée à son échéance, vous pouvez la renouveler via le site de Kaspersky Lab.

Section du panneau de navigation de la fenêtre principale	Fonction
	La rubrique **Assistance technique** présente les informations sur les services d'assistance technique pour les utilisateurs enregistrés de Kaspersky Anti-Virus.

Chaque élément du panneau de navigation est doté d'un menu contextuel spécial. Ainsi, pour les composants de la protection 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 prévoit un point supplémentaire pour la recherche de virus qui vous permet de personnaliser la tâche sélectionnée.

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

La partie inférieure gauche de la fenêtre contient deux boutons : **Aide** pour accéder au système d'aide de Kaspersky Anti-Virus et **Configuration**, pour ouvrir la fenêtre de configuration de l'application

4.4. Fenêtre de configuration des paramètres du logiciel

La fenêtre de configuration des paramètres de Kaspersky Anti-Virus peut être ouverte depuis la fenêtre principale (cf. point 4.3, p. 46) menu contextuel de l'application (cf. point 4.2, p. 44). Pour ce faire, cliquez sur le bouton **Configuration** dans la partie inférieure de la fenêtre principale ou sélectionnez le point équivalent dans le menu contextuel de l'application.

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

- La partie gauche offre un accès simple et rapide à la configuration de chaque composant de la protection en temps réel, des tâches liées à la recherche de virus, de la mise 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.

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.

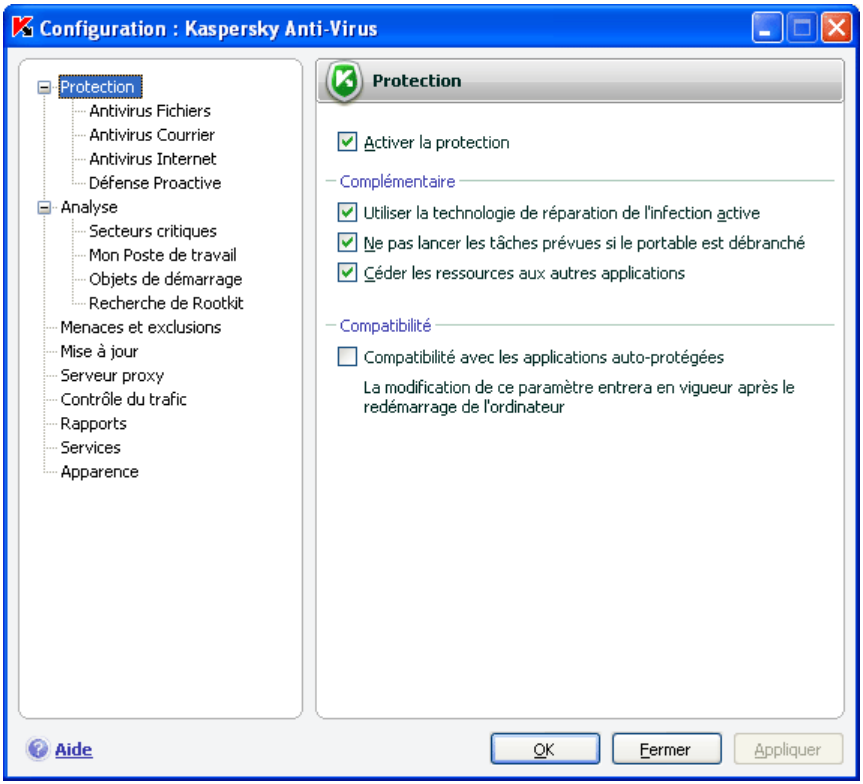


Illustration 3. Fenêtre de configuration de Kaspersky Anti-Virus

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. Ainsi, tout utilisateur, quelles que soient ses connaissances en informatique, peut assurer la protection de son ordinateur dès l'installation du logiciel sans devoir s'encombrer de la configuration.

Toutefois, les particularités de la configuration de votre ordinateur ou des tâches exécutées peuvent être propres. Pour cette raison, nous vous conseillons de réaliser une configuration préalable du logiciel afin de l'adapter le mieux possible à la protection de votre ordinateur.

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. 35). 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. 52) 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 5.6, p. 58).
- Analyser l'ordinateur (cf. point 5.3, p. 55).

5.1. Etat de la protection de l'ordinateur

L'état de la protection de votre ordinateur reflète la présence ou l'absence de menaces qui influencent le niveau général de sécurité du système. Dans ce cas, les menaces sont non seulement les programmes malveillants découverts, mais aussi l'utilisation de bases de l'application dépassées, la désactivation de certains composants, l'utilisation des paramètres minimum de fonctionnement, etc.

L'état de la protection est repris dans la partie supérieure de la fenêtre principale et il est exprimé par des couleurs identiques à celles des feux de circulation. La couleur affichée dépend de la situation et quand une menace existe, la zone de couleur s'accompagne d'un texte qui se présente sous la forme d'un lien vers l'Assistant de sécurité.

La couleur représentant l'état peut prendre une des valeurs suivantes :

- La couleur principale de la fenêtre est *verte*. Cet état signale que votre ordinateur est protégé au niveau requis.

  Cet état indique que vous avez actualisé les bases de l'application en temps voulus, que tous les composants de la protection sont activés, que l'application fonctionne selon les paramètres recommandés par les spécialistes de Kaspersky Lab et que l'analyse complète de l'ordinateur n'a décelé aucun objet malveillant ou que les objets malveillants découverts ont été neutralisés.

- La couleur principale de la fenêtre est *jaune*. Le niveau de protection de votre ordinateur est inférieur au niveau précédent. Cet état signale la présence de quelques problèmes au niveau du fonctionnement ou de la configuration de l'application.

  Par exemple, l'écart par rapport au mode de fonctionnement recommandé est important ou les bases de l'application n'ont plus été actualisées depuis quelques jours.

- La couleur principale de la fenêtre est *rouge*. Votre ordinateur est exposé à un sérieux risque d'infection. Cet état signale l'existence de problèmes qui pourraient entraîner l'infection de l'ordinateur ou la perte de données. Par exemple, le fonctionnement d'un ou de plusieurs composants s'est soldé par un échec, l'application n'a plus été actualisée depuis un certain temps ou des objets malveillants ont été découverts et il faut absolument les neutraliser de toute urgence.

Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se présentent. Pour ce faire, utiliser l'Assistant de sécurité qui s'ouvre grâce au lien signalant la présence de menaces dans le système. L'Assistant de sécurité vous aidera à examiner les menaces existantes et à les éliminer directement. Le niveau de gravité d'une menace est indiqué par un témoin de couleur :

 : *ce témoin attire votre attention sur l'existence d'une menace non-critique* qui peut toutefois réduire le niveau global de protection de l'ordinateur. Veuillez suivre attentivement les recommandations des experts de Kaspersky Lab.

 : *ce témoin signale la présence de menaces sérieuses pour la* sécurité de votre ordinateur. Veuillez respecter scrupuleusement les recommandations

reprises ci-dessous. Elles visent toutes à renforcer la protection de votre ordinateur. Les actions recommandées apparaissent sous la forme d'un lien.

Pour prendre connaissance de la liste des menaces existantes, cliquez sur le lien Détails. Chaque menace est accompagnée d'une description détaillée et les actions suivantes sont proposées :

- *Supprimer la menace immédiatement* A l'aide des liens adéquats, vous pouvez supprimer directement la menace. Pour obtenir de plus amples informations sur les événements liés à l'apparition de cette menace, vous pouvez consulter le rapport correspondant. La suppression immédiate est l'action recommandée.
- *Reporter la suppression de la menace* Si pour une raison quelconque vous ne pouvez pas supprimer la menace directement, il est possible de reporter cette action à plus tard. Pour ce faire, cliquez sur Reporter.

  Sachez toutefois que cette possibilité n'est pas reprise pour les menaces sérieuses. Ces menaces sont par exemple celles posées par des objets malveillants non neutralisés, par l'échec d'un ou de plusieurs composants de la protection ou par la corruption des bases de l'application.

S'il reste des menaces à la fin du fonctionnement de l'Assistant de sécurité, un message dans la partie supérieure de la fenêtre principale vous rappellera que ces menaces doivent être supprimées. Lorsque vous ouvrirez à nouveau l'Assistant de sécurité, les menaces dont le traitement aura été reporté ne figureront pas dans la liste des menaces actives. Néanmoins, vous pouvez revenir à l'examen et à la suppression des anciennes menaces en cliquant sur le lien Consulter les menaces reportées dans la dernière fenêtre de l'Assistant.

5.2. Etat d'un composant particulier de la protection

Pour consulter l'état actuel de n'importe quel composant de la protection en temps réel, ouvrez la fenêtre principale de l'application et, dans la section **Protection**, sélectionnez le composant souhaité. Dans la partie droite de la fenêtre, vous trouverez les informations de synthèse sur le fonctionnement du composant sélectionné.

L'information la plus importante concerne l'état du fonctionnement du composant :

- *<nom du composant> : en exécution* : la protection offerte par le composant est au niveau requis.

- *<nom du composant> : en pause* : le composant a été suspendu pour un temps déterminé. La protection sera rétablie automatiquement une fois ce laps de temps écoulé ou après le redémarrage du logiciel. Vous pouvez activer vous-même le composant. Pour ce faire, cliquez sur le lien Rétablir le fonctionnement.

- *<nom du composant>* : *inactif*. L'utilisateur a arrêté le composant. Vous pouvez activer la protection des fichiers. Pour ce faire, cliquez sur le lien Activer.

- *<nom du composant> : ne fonctionne pas*. La protection offert par ce composant est inaccessible pour une raison quelconque.

- *<nom du composant> : échec*. Le composant s'est arrêté suite à un échec.

  Si une erreur survient pendant le fonctionnement du composant, tentez de le lancer à nouveau. Si la seconde tentative se solde également par un échec, consultez le rapport sur le fonctionnement du composant. Il contiendra peut-être la cause de l'échec. Si vous ne parvenez pas à résoudre le problème seul, enregistrez le rapport à l'aide du bouton **Actions → Enregistrer sous** et contactez le service d'Assistance technique de Kaspersky Lab

En plus des informations sur l'état de fonctionnement du composant, vous pouvez obtenir des renseignements sur sa configuration (par exemple, le niveau de protection, les actions appliquées aux objets dangereux). Si le composant contient plusieurs modules, cette section vous renseigne sur l'état du fonctionnement : sont-ils actifs ou pas. Pour passer à la modification des paramètres de fonctionnement du composant, cliquez sur le lien Personnaliser.

Vous pourrez voir également certaines statistiques sur les résultats du fonctionnement de chaque composant. Pour consulter le rapport détaillé, cliquez sur le lien Ouvrir le rapport.

Si, pour une raison quelconque le composant est désactivé ou suspendu, vous pouvez consulter les résultats de son activité au moment de la désactivation. Pour ce faire, cliquez sur le lien Ouvrir le rapport sur la dernière exécution.

5.3. Recherche d'éventuels virus

Dès que l'installation est terminée, un message spécial dans le coin inférieur gauche vous signale que l'analyse de l'ordinateur n'a pas encore été réalisée et qu'il est conseillé de la lancer immédiatement.

Kaspersky Anti-Virus possède par défaut une tâche de recherche de virus sur l'ordinateur. Elle se trouve dans la section **Analyse** 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 protection sélectionnée, l'action exécutée sur les objets dangereux et ouvrir le rapport sur la dernière exécution de la tâche.

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

1. Dans la fenêtre principale de l'application, sélectionnez la tâche **Mon Poste de travail** dans la rubrique **Analyse**.
2. Cliquez sur le lien Lancer l'analyse.

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.

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

Il existe sur votre ordinateur des secteurs critiques du point de vue de la sécurité. Ils sont infectés par les programmes malveillants qui veulent endommager le système d'exploitation, le processeur, la mémoire, etc.

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 **Analyse** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Secteurs critiques**, vous pouvez consulter les paramètres de la tâche : le niveau de protection 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. Dans la fenêtre principale de l'application, sélectionnez la tâche **Secteurs critiques** dans la rubrique **Analyse**.
2. Cliquez sur le lien Lancer l'analyse.

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.

5.5. 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 où sont enregistrés les logiciels et les jeux, une base de données de messagerie ramenée de l'ordinateur de votre bureau, une archive envoyée par courrier électronique, etc. Vous pouvez sélectionner l'objet à analyser à l'aide des méthodes traditionnelles du système d'exploitation Microsoft Windows (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 d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 4).

Illustration 4. Recherche d'éventuels virus dans un objet sélectionné à l'aide des outils Microsoft Windows

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.

5.6. Mise à jour du logiciel

Kaspersky Lab met à jour les bases 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 mises à jour les plus récentes, Kaspersky Anti-Virus les télécharge et les installe en arrière plan.

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

1. Sélectionnez la rubrique **Mise à jour** dans la fenêtre principale de l'application
2. Cliquez sur le lien Mettre à jour.

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

5.7. Que faire si la protection ne fonctionne pas

En cas de problème ou d'erreur de fonctionnement d'un composant quelconque de la protection, veuillez vérifier son état. Si l'état du composant est *ne fonctionne pas* ou *échec*, tentez de redémarrer Kaspersky Anti-Virus.

Si le redémarrage de l'application ne résout pas le problème, il est conseillé de rectifier les erreurs à l'aide du programme de restauration de l'application (cf. Chapitre 17, p. 232).

Si la procédure de restauration n'a rien changé, contactez le service d'Assistance technique de Kaspersky Lab. Il faudra peut-être que vous enregistriez le rapport de fonctionnement du composant afin de pouvoir fournir aux opérateurs du service d'assistance technique toutes les informations dont ils ont besoin.

Afin d'enregistrer le rapport de fonctionnement d'un composant particulier dans un fichier :

1. Sélectionnez le composant dans la section **Protection** de la fenêtre principale du logiciel et cliquez sur le lien Ouvrir le rapport (si le composant fonctionne à ce moment) ou sur le lien Ouvrir le rapport sur la dernière exécution (si le composant a été désactivé).
2. Dans la fenêtre du rapport, cliquez sur **Actions → Enregistrer sous** et dans la fenêtre qui s'ouvre, saisissez le nom du fichier où vous souhaitez enregistrer les résultats du fonctionnement du composant.

CHAPITRE 6. ADMINISTRATION COMPLEXE DE LA PROTECTION

Cette rubrique présente les informations sur la configuration des paramètres généraux de l'application utilisés dans le fonctionnement de tous les composants de la protection en temps réel et des tâches ainsi que sur la constitution de zones de protection : énumération des menaces contre lesquelles l'application interviendra et liste des objets de confiance exclus de l'analyse :

- Administration de la protection en temps réel de l'ordinateur (cf. point 6.1, p. 60);
- Utilisation de la technologie de réparation de l'infection active (cf. point 6.2, p. 64);
- Lancement des tâches sur un ordinateur portable (cf. point 6.3, p 65);
- Compatibilité entre Kaspersky Anti-Virus et les autres applications (cf. point 6.4, p. 65);
- Compatibilité entre Kaspersky Anti-Virus et l'autodéfense d'autres applications (cf. point 6.5, p. 66);
- Enumération des menaces (cf. point 6.2, p. 64) contre lesquelles l'application assurera une protection ;
- Liste des objets de la zone de confiance (cf. point 6.9, p. 72) qui seront exclus de la protection.

6.1. Désactivation/activation de la protection en temps réel de votre ordinateur

Par défaut, Kaspersky Anti-Virus est lancé au démarrage du système comme en témoigne le message *Kaspersky Anti-Virus 7.0* qui apparaît dans le coin supérieur droit de l'écran. La protection est garantie pendant toute la séance de travail. Tous les composants de la protection en temps réel sont activés (cf. point 2.2.1, p. 24).

Vous pouvez désactiver la protection offerte par Kaspersky Anti-Virus soit complètement, soit partiellement.

Attention !

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection en temps réel** 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 des composants du logiciel. La désactivation ou la suspension du fonctionnement des composants du logiciel 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 que tous les composants de la protection en temps réel qui vérifient les fichiers sur votre ordinateur, le courrier entrant et sortant, les scripts exécutés et le comportement des applications sont désactivés.

Pour suspendre le fonctionnement de la protection en temps réel :

1. Sélectionnez **Suspension de la protection** dans le menu contextuel (cf. point 4.2, p. 44)
2. Dans la fenêtre de désactivation (cf. ill. 5), 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 au démarrage de l'ordinateur soit activé (cf. point 15.11, p. 213).
   - A 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.

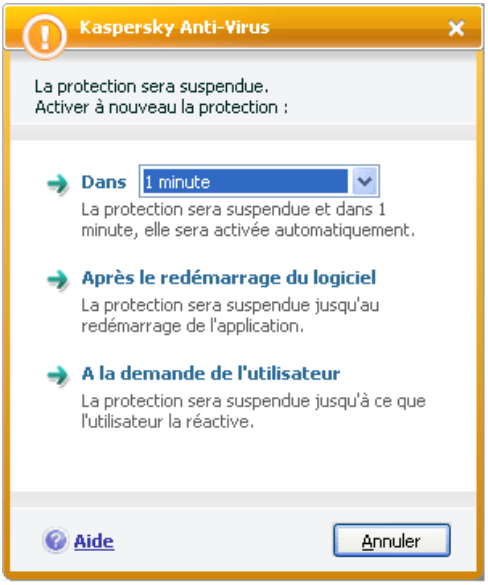


Illustration 5. Fenêtre de suspension de la protection de votre ordinateur

Cette action suspend le fonctionnement de tous les composants de la protection en temps réel. 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 inactive dans la barre des tâches est grise.

6.1.2. Désactivation complète de la protection de l'ordinateur

La désactivation complète signifie l'arrêt du fonctionnement des composants de la protection en temps réel. 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'utilisateur. L'activation automatique des composants de la protection 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 composants individuels ou composer une liste d'exclusions (cf. point 6.9, p. 72).

Pour désactiver complètement la protection en temps réel de l'ordinateur :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Protection**.
2. Désélectionnez la case **Activer la protection**.

Cette action entraînera l'arrêt du fonctionnement de tous les composants. 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 zone de notification de la barre des tâches de Microsoft Windows est en noir et blanc.

6.1.3. Suspension / désactivation de composants distincts de la protection

Il existe plusieurs moyens de désactiver un composant de la protection. 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 6.9, p. 72).

Pour suspendre un composant de la protection

Ouvrez la fenêtre principale de l'application, sélectionnez le composant dans la rubrique **Protection** et cliquez sur le lien Pause.

L'état du composant passe à en *pause*. La protection assurée par le composant sera suspendue jusqu'à ce que vous relanciez l'application ou que vous réactiviez le composant en cliquant sur le lien Rétablir le fonctionnement.

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

Pour arrêter un composant particulier de la protection :

Ouvrez la fenêtre principale de l'application, sélectionnez le composant dans la rubrique **Protection** et cliquez sur le lien Stop.

Dans ce cas, l'état du composant devient *inactif* et le nom du composant dans la liste de la rubrique **Protection** est désactivé (gris). La protection as-

surée par le composant qui était exécutée sera arrêtée jusqu'à ce que vous cliquiez sur le lien Activer.

Il est possible également d'arrêter n'importe quel composant de la protection en temps réel au départ de la fenêtre de configuration de l'application. Pour ce faire, ouvrez la fenêtre de configuration, sélectionnez le composant souhaité dans la section **Protection** et désélectionnez la case **Activer <nom du composant>**.

En cas de désactivation du composant, toutes les statistiques antérieures sont perdues et les données seront à nouveau consignées au lancement du composant.

Les différents composants de la protection en temps réel peuvent également être désactivés via la désactivation complète de la protection en temps réel de votre ordinateur (cf. point 6.1.2, p. 62).

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 de la protection**.

- Au départ de la fenêtre **principale** du logiciel.

  Sélectionnez la section **Protection** dans la partie gauche de la fenêtre principale puis cliquez sur le lien Lancement.

L'état de la protection redevient immédiatement *en exécution*. L'icône du logiciel dans la zone de notification de la barre des tâches de Microsoft Windows redevient active (en couleur).

6.2. Technologie de réparation de l'infection active

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. Lorsque Kaspersky Anti-Virus 7.0 découvre une menace active dans le système, il propose d'élargir la procédure de réparation afin de neutraliser la menace et de la supprimer.

L'ordinateur redémarrera à la fin de la procédure. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète. Si vous souhaitez utiliser la réparation étendue, sélectionnez la rubrique **Protection** et cochez la case ☑ **Utiliser la technologie de réparation de l'infection active** dans le bloc **Complémentaire** (cf. ill. 6).

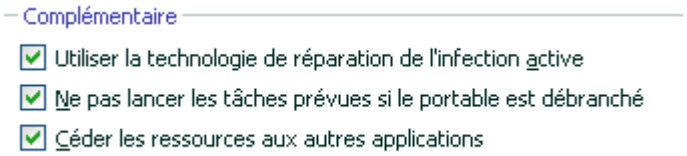


Illustration 6. Configuration des paramètres généraux

6.3. Utilisation de l'application sur un ordinateur portable

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter les tâches liées à la recherche de virus.

Etant donné que la recherche de virus et la mise à jour du logiciel sont assez gourmandes en ressources et durent un certain temps, nous vous conseillons de désactiver le lancement programmé de celles-ci. Cela vous permettra d'économiser la batterie. Au besoin, vous pourrez mettre à jour vous-même le programme (cf. point 5.6, p. 58) ou lancer l'analyse antivirus manuellement (cf. point 5.3, p. 55). Pour utiliser le service d'économie de la batterie, ouvrez la fenêtre de configuration de l'application, sélectionnez la rubrique **Protection** et cochez la case ☑ **Ne pas lancer les tâches prévues si le portable est débranché** dans le bloc **Complémentaire** (cf. ill. 6).

6.4. Performances de l'ordinateur pendant l'exécution de tâches

Afin de réduire la charge sur le processeur central et sur les sous-systèmes de disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches liées à la recherche de virus augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, le programme

arrête par défaut la recherche des virus et libère des ressources pour l'application de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Afin que la recherche de virus ne dépendent pas du travail de tels programmes, sélectionnez la rubrique **Protection** cochez la case et cochez la case **Céder les ressources aux autres applications** dans le bloc **Complémentaire** (cf. ill. 6).

N'oubliez pas que ce paramètre peut être défini individuellement pour chaque tâche de recherche de virus. Dans ce cas, la configuration d'un paramètre pour une tâche particulière a une plus grande priorité.

6.5. 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 craquage.

Pour résoudre ce problème, sélectionnez la rubrique Protection et cochez la case **Compatibilité avec les applications auto-protégées** dans le groupe **Compatibilité** (cf. ill. 6). Pour que la modification de ce paramètre entre en vigueur, il faut redémarrer le système d'exploitation.

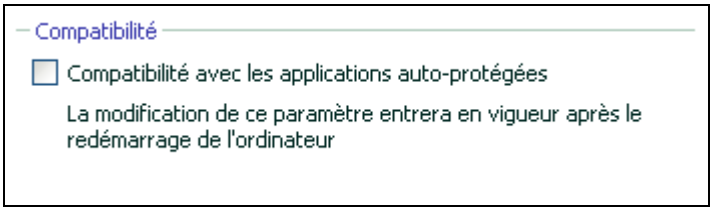


Illustration 7. Configuration des paramètres de compatibilité

Attention !

Si l'application est installée sur un ordinateur tournant sous Microsoft Windows Vista ou Microsoft Windows Vista x64, il n'est pas possible de résoudre le problème de compatibilité avec l'auto-défense des autres applications.

6.6. Lancement d'une tâche de recherche de virus ou de mise à jour avec les privilèges d'un utilisateur

Kaspersky Anti-Virus 7.0 offre la possibilité de lancer une tâche utilisateur 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 utilisateur qui jouit de tels privilèges.

S'agissant de la mise à jour du logiciel, elle peut être réalisée à partir 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 de recherche de virus au nom d'un autre utilisateur :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Analyse**.
2. Cliquez sur le bouton **Configuration** dans le groupe **Niveau de protection** et passez à l'onglet **Complémentaire** dans la fenêtre qui s'affiche.

Pour configurer le lancement de la mise à jour au nom d'un autre utilisateur,

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Mise à jour**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Paramètres de la mise à jour** et dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Complémentaire** (cf. ill. 8).

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.

N'oubliez pas que sans l'utilisation du lancement avec les privilèges, la mise à jour sera exécutée selon les privilèges du compte actuel. Si aucun utilisateur n'est enregistré à ce moment, que la mise à jour selon les privilèges d'un autre utilisateur n'est pas configurée et que la mise à jour est programmée, elle sera lancée selon les privilèges SYSTEM.

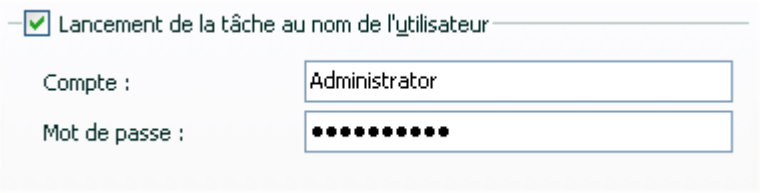


Illustration 8. Configuration du lancement des tâches au nom d'un autre utilisateur

6.7. Programmation du lancement de tâches et envoi de notifications

La configuration de la programmation est identique pour la recherche de virus, la mise à jour de l'application et l'envoi de notifications sur le fonctionnement de Kaspersky Anti-Virus.

L'exécution des tâches de recherche de virus créées lors de l'installation du logiciel est désactivée par défaut. La seule exception se situe au niveau de l'analyse des objets de démarrage qui est réalisée chaque fois que Kaspersky Anti-Virus est lancé. S'agissant de la mise à jour, elle est réalisée automatiquement par défaut au fil des diffusions des mises à jour sur les serveurs de Kaspersky Lab.

Si ce mode d'exécution de la tâche ne vous convient pas, il vous suffit de modifier les paramètres de programmation.

L'élément le plus important à définir, c'est l'intervalle d'exécution de l'événement (lancement de la tâche ou envoi de notification). Pour ce faire, sélectionnez l'option souhaitée dans le groupe **Fréquence** (cf. ill. 9). Il faudra ensuite définir les paramètres de l'intervalle dans le groupe **Configuration de la programmation**. Vous avez le choix entre les options suivantes :

- **Au moment défini**. Exécution de la tâche ou de l'envoi des notifications au jour et à l'heure indiquées.

Au lancement de l'application : la tâche est exécutée ou la notification est envoyée à chaque démarrage de Kaspersky Anti-Virus. Vous pouvez en plus, si vous le souhaitez, précisez le délai d'exécution de la tâche après le lancement de l'application.

Après chaque mise a jour : la tâche est lancée après chaque mise à jour des bases de l'application (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 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 : **Chaque X heure(s)** et définissez l'intervalle X. Pour une mise à jour toutes les heures, sélectionnez *Chaque 1 heure(s)*.

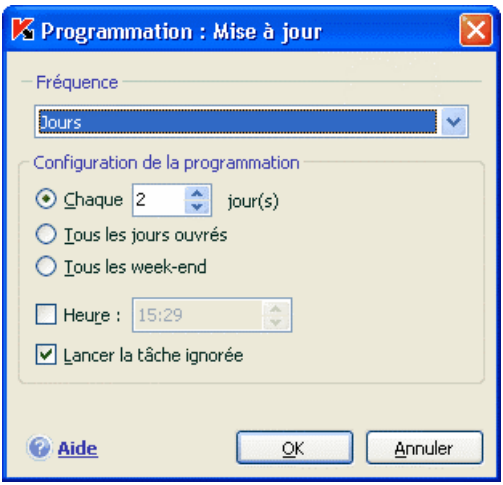


Illustration 9. Programmation de l'exécution de la tâche

Jour. Le lancement des tâches ou l'envoi de notifications est réalisé tous les quelques jours. Dans les paramètres de la programmation, définissez les valeurs de l'intervalle :

- Sélectionnez **Chaque X jours** et précisez l'intervalle *X* si vous souhaitez un intervalle de quelques jours.

- Sélectionnez **Tous les jours ouvrés** si vous souhaitez une exécution tous les jours du lundi au vendredi.
- Sélectionnez **Tous les week-end** si vous souhaitez une exécution uniquement les samedi et dimanche.

En plus de la fréquence, définissez l'heure à laquelle la tâche d'analyse sera lancée dans le champ **Heure**.

Semaines. Le lancement de la tâche ou l'envoi de notifications est réalisés certains jours de la semaine. Si vous choisissez cette fréquence, cochez les cases correspondantes aux jours de la semaine où le lancement doit être effectué dans les paramètres. Précisez l'heure dans le champ **Heure**.

Mois. La tâche ou l'envoi de notifications est réalisé une fois par mois à l'heure indiquée.

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

6.8. Types de programmes malveillants contrôlés

Kaspersky Anti-Virus vous protège contre divers types de programmes malveillants. Quelle que soit la configuration du programme, votre ordinateur sera toujours protégé contre les types de programmes malveillants les plus dangereux tels que les virus, les chevaux de Troie et les programmes d'attaque informatique. 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, ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Menaces et exclusions** (cf. ill. 10).

Les types de menaces (cf. point 1.3, p. 10) 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 recom-

mandations 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 bases de l'application 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. 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 6.9, p. 72).

Pour sélectionner le type de programmes malveillants à contrôler :

Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Menaces et exclusions**. La configuration s'opère dans le bloc **Catégorie de programmes malicieux** (cf. ill. 10).

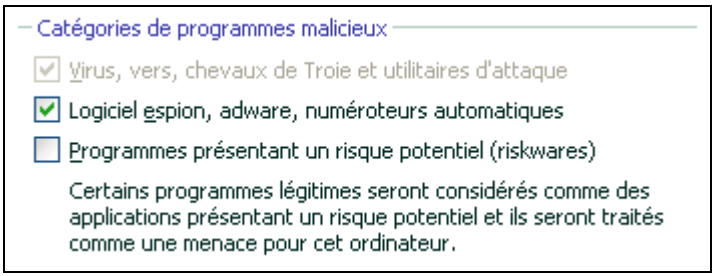


illustration 10. Sélection du type de menace à contrôler

6.9. Constitution de la zone de confiance

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

Cette zone de confiance peut être définie par l'utilisateur sur la base des particularités des objets qu'il manipule et des programmes installés sur l'ordinateur. La constitution de cette liste d'exclusions peut s'avérer utile si Kaspersky Anti-Virus bloque l'accès à un objet ou un programme quelconque alors que vous êtes convaincus 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 du type de menace selon la classification de l'Encyclopédie des virus (état attribué à l'objet par le programme suite à l'analyse).

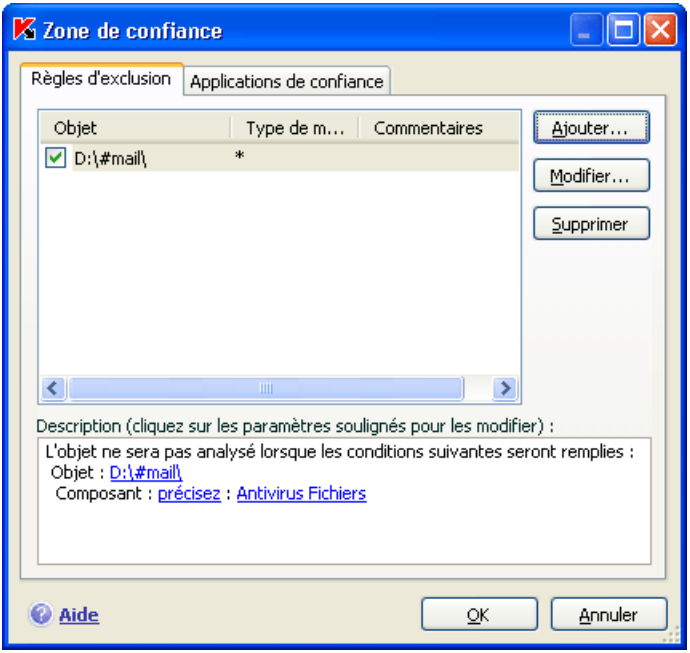


Illustration 11. Constitution de la zone de confiance

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 de l'application et passez à la section **Menaces et exclusions** (cf. ill. 10).
2. Cliquez sur **Zone de confiance** dans le bloc **Exclusions**.
3. Dans la boîte de dialogue (cf. ill. 11) qui apparaît, configurer les règles d'exclusion pour les objets et composez également une liste d'applications de confiance.

6.9.1. 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 en fonction du type de menace selon la classification de l'Encyclopédie des virus.

Le Type de menace 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 de la classification 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 le type de menace 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 par certains composants du programme (Antivirus Fichiers, Antivirus Courrier, Défense proactive, Antivirus Internet) 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** (cf. ill. 11).
2. Dans la fenêtre qui apparaît (cf. ill. 12), sélectionnez le type d'exclusion dans la section **Paramètres** :

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

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

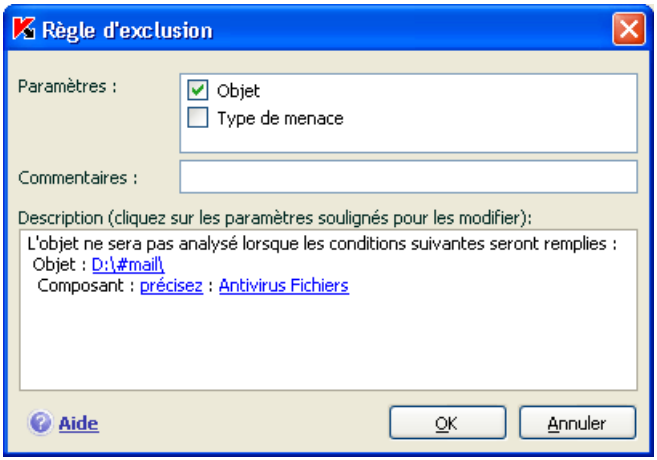


Illustration 12. Création d'une règle d'exclusion

Si vous cochez simultanément les deux cases, vous créerez une règle pour l'objet défini répondant au type de menace sélectionné. 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 le **Type de menace**, 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 **Type de menace**, 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 fichiers (cf. point A.2, p. 239). Afin que l'objet indiqué (fichier, masque de fichiers, répertoire) soit ignoré partout pendant l'analyse, cochez la case ☑ **Sous-répertoires compris**. Si vous avez défini le fichier **C:\Program Files\winword.exe** comme une exclusion et que vous avez coché la case d'analyse des sous-répertoire, le fichier **winword.exe** situé dans n'importe quel sous-répertoire de **C:\Program Files** sera ignoré.
   - Pour le **Type de menace** 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. 241).

     Pour certains objets exclus en fonction du type de menace, il est possible de définir dans le champ **Paramètres complémentaires** des conditions supplémentaires pour l'application de la règle. Dans la majorité des cas, ce champ est rempli automatiquement lors de l'ajout d'une règle d'exclusion au départ de la notification de la défense proactive.

     La saisie de paramètres complémentaires est requise pour les menaces suivantes :

     - *Invader* (intrusion dans les processus du programme). Pour cette menace, vous pouvez définir en guise de condition d'exclusion complémentaire le nom, le masque ou le chemin d'accès complet à l'objet victime de l'intrusion (par exemple, un fichier dll).

- *Launching Internet Browser* (lancement du navigateur selon les paramètres). Pour cette menace, vous pouvez définir en guise de condition d'exclusion complémentaire les paramètres de lancement du navigateur. Par exemple, vous avez interdit le lancement du navigateur selon les paramètres dans l'analyse de l'activité des applications de la Défense proactive. Vous souhaitez toutefois autoriser le lancement du navigateur pour le domaine *www.kaspersky.com* au départ d'un lien dans Microsoft Office Outlook. Pour ce faire, sélectionnez Microsoft Office Outlook en tant qu'**Objet** de l'exclusion et *Launching Internet Browser* en tant que **Type de menace**. Dans le champ **Paramètres complémentaires**, saisissez le masque du domaine autorisé.

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 précisez. 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 zone de confiance dans la fenêtre de notification (cf. ill. 13).

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**.

Illustration 13. Notification sur la découverte d'un objet dangereux

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. ill. 14).
3. Cette action entraîne l'ouverture de la fenêtre de configuration des exclusions. 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**.

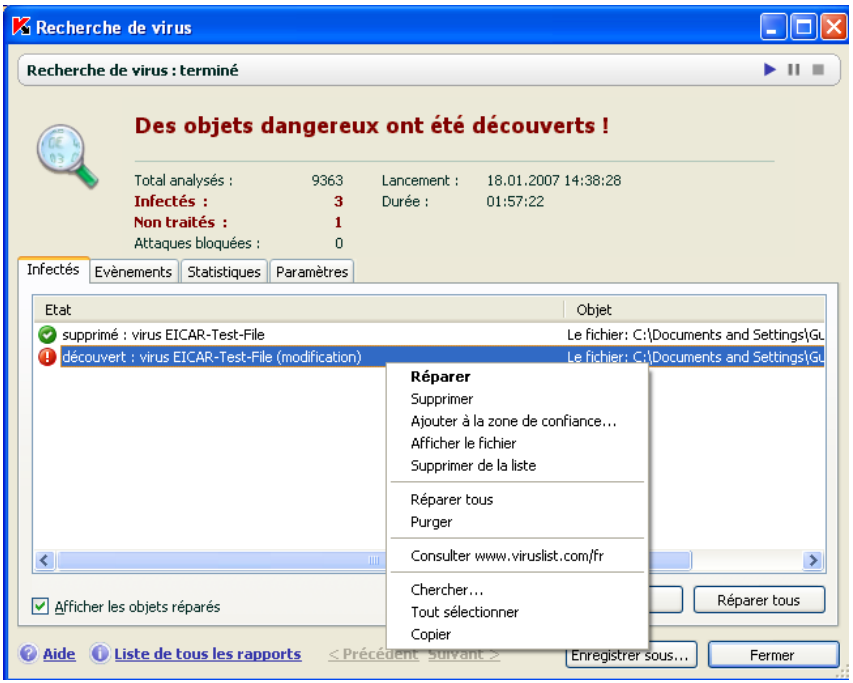


Illustration 14. Création d'une règle d'exclusion au départ du rapport

6.9.2. 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, les activités de réseau et les requêtes adressées à la base de registres système ne sera pas contrôlée.

Par exemple, vous estimez que le objets utilisés par le programme **Bloc-notes** de Microsoft Windows sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance 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 6.9.1, p. 73).

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 pro-

grammes 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, ce qui est particulièrement important lors de l'utilisation d'applications serveur.

Par défaut Kaspersky Anti-Virus analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère.

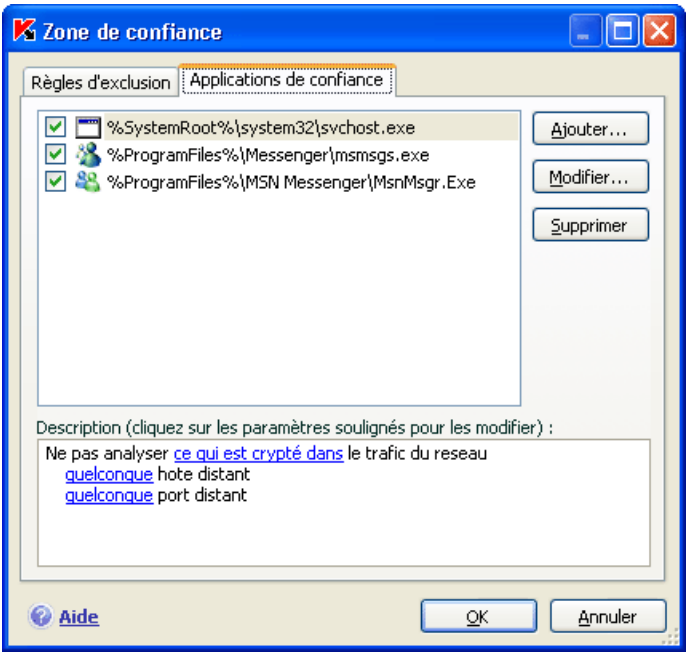


Illustration 15. Liste des applications de confiance

La constitution de la liste des applications de confiance s'opère sur l'onglet spécial **Applications de confiance** (cf. ill. 15). Après l'installation de Kaspersky Anti-Virus, la liste des applications de confiance contient par défaut les applications dont l'activité n'est pas analysées sur la base des recommandations des experts de Kaspersky Lab. Si vous estimez que les applications de la liste ne sont pas des applications de confiance, désélectionnez la case correspondante.

Vous pouvez modifier la liste à l'aide des boutons **Ajouter…**, **Modifier…** et **Supprimer…** situés à droite.

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 **Application de confiance**.
2. Dans la fenêtre **Application de confiance** (cf. ill. 16) 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.

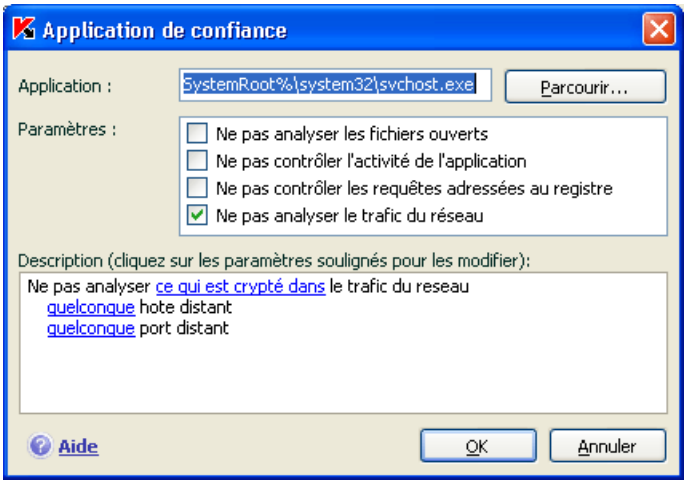


Illustration 16. Ajout d'une application à la liste des applications de confiance

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. Précisez ensuite les processus qui ne seront pas contrôlés 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.

- **Ne pas contrôler l'activité de l'application** : exclut de l'analyse dans le cadre de l'utilisation de la défense proactive n'importe quelle activité (y compris les activités suspectes) exécutée par l'application de confiance.
- **Ne pas contrôler les requêtes adressées au registre** : exclut de l'analyse les tentatives de requête adressée à la base de registres système émanant d'une application.
- **Ne pas analyser le trafic du réseau** : exclut de la recherche de virus et de messages non sollicités le trafic de réseau engendré par l'application de confiance. Vous pouvez exclure de l'analyse toute application de réseau ou uniquement le trafic encodé (à l'aide du protocole SSL). Pour ce faire, cliquez sur le lien tout qui prendra la valeur chiffré. De plus, vous pouvez limiter l'exclusion à un hôte distant/port en particulier. Pour définir ces restrictions, cliquez sur le lien quelconque qui prend alors la valeur précisez et précisez la valeur de l'hôte distant/du port.

CHAPITRE 7. PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS DE L'ORDINATEUR

Kaspersky Anti-Virus contient un composant spécial qui permet d'éviter l'infection du système de fichiers de votre ordinateur. Il s'agit de *l'Antivirus Fichiers*. 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 ouverts, enregistrés ou exécutés.

L'icône de Kaspersky Anti-Virus dans la zone de notification de la barre des tâches de Microsoft Windows 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 *bases de l'application*. Les bases contiennent la définition de tous les programmes malveillants et 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 un code malveillant est identifié dans le fichier, l'Antivirus Fichiers bloque le fichier et tente de le réparer. Si la réparation réussit, le fichier est accessible et si la réparation échoue, il est

supprimé. Pendant la réparation ou la suppression, une copie du fichier est placée dans la *sauvegarde*.

b. Si le fichier contient un code semblable à celui d'un programme malveillant mais qu'il est impossible de considérer le fichier à 100% comme un fichier malveillant, le fichier sera placé dans un référentiel spécial : *la quarantaine*. Il sera possible ensuite de tenter de le réparer à l'aide de bases actualisées.

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

Antivirus Fichiers protège les fichiers que vous utilisez selon un des niveaux suivants (cf. ill. 17):

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

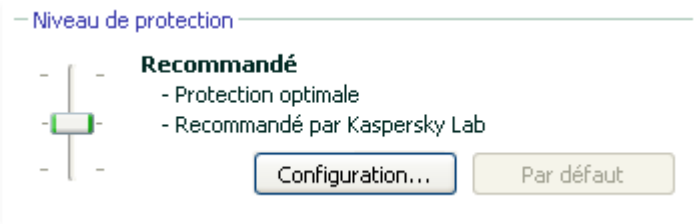


Illustration 17. Niveau de protection d'Antivirus Fichiers

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 **Autre**. Voici un exemple où la modification des paramètres du niveau proposé pourrait s'imposer.

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 :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Fichiers** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 17).

3. Dans la fenêtre qui s'ouvre, modifiez les paramètres de la protection des fichiers puis cliquez sur **OK**.

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. 85);
- Les paramètres qui définissent la zone protégée (cf. point 7.2.2, p. 88);
- Les paramètres qui définissent les actions à réaliser sur l'objet dangereux (cf. point 7.2.6, p. 95).;
- Les paramètres qui définissent l'utilisation des méthodes d'analyse heuristique (cf. point 7.2.4, p. 93);
- Les paramètres complémentaires de fonctionnement de l'Antivirus Fichiers (cf. point 7.2.3, page 90).

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. ill. 18). 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 t***xt*** 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. 237) 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.

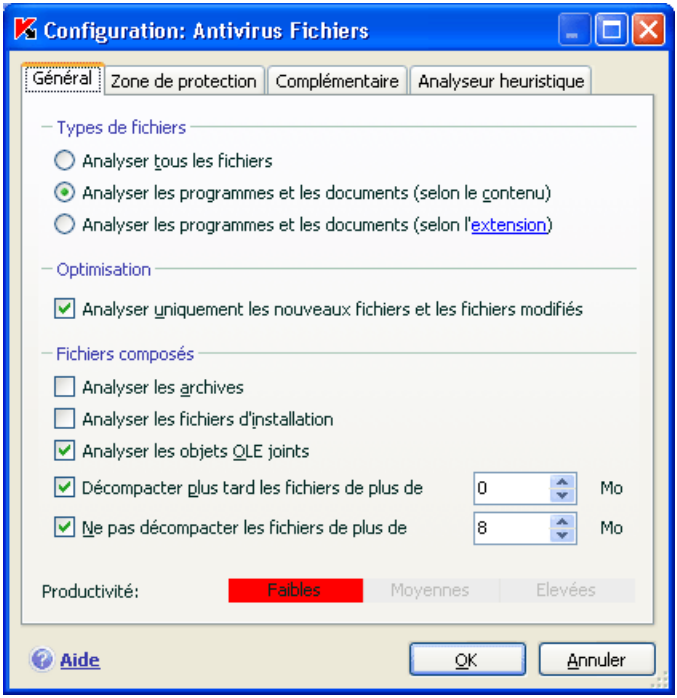


Illustration 18. Sélection du type de fichier soumis à l'analyse antivirus

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

- **Analyser les les archives/uniquement les nouveaux (-elles) archives** : analyse les archives au format ZIP, CAB, RAR, ARJ.
- **Analyser les/uniquement les nouveaux (-elles) fichiers d'installation** : recherche la présence d'éventuels virus dans les archives autoextractibles.
- **Analyser les/uniquement les nouveaux (-elles) 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 par l'utilisateur. 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. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
2. Cliquez sur **Configuration** dans le groupe **Niveau de protection** (cf. ill. 17).
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Zone de protection** (cf. ill. 19).

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**.

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

1. Indiquer uniquement les répertoires, disques ou fichiers qui doivent être protégés.
2. Constituer une liste des objets qui ne doivent pas être protégés.
3. 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**.

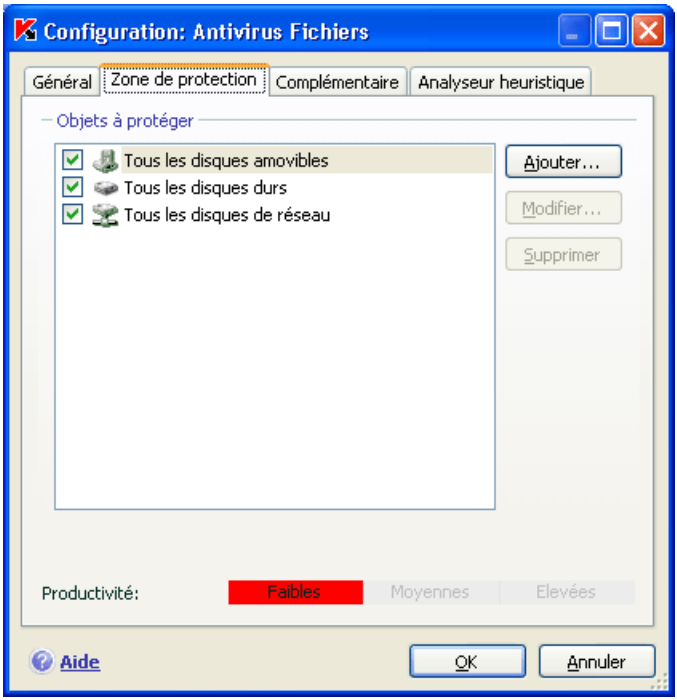


Illustration 19. Constitution de la zone protégée

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. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
2. Cliquez sur **Configuration** dans le groupe **Niveau de protection** (cf. ill. 17).
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Complémentaire** (cf. ill. 20).

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 Anti-Virus 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.

- **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.

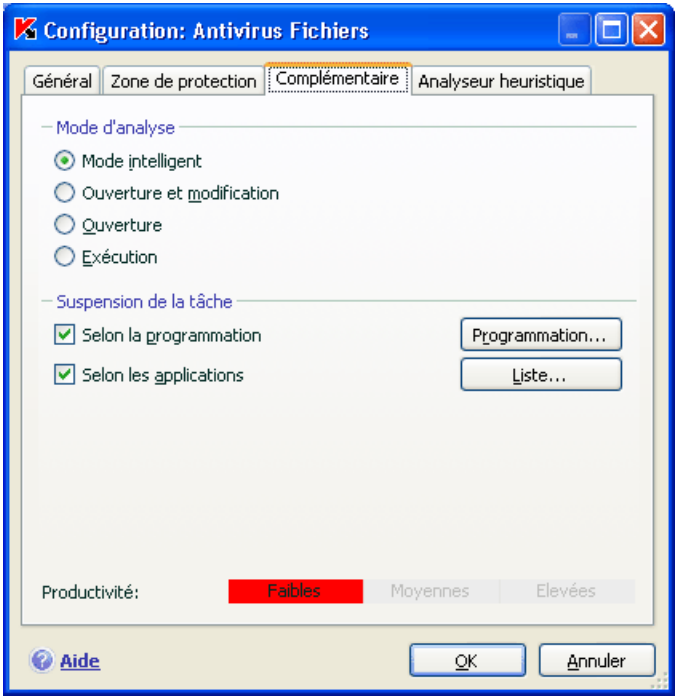


Illustration 20. Configuration des paramètres complémentaires de l'Antivirus Fichiers.

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 moments 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. ill. 20) qui s'ouvre après avoir cliqué sur le **Programmation**, définissez la plage d'arrêt du composant. Pour ce faire, saisissez la valeur au format hh:mm dans les champs correspondants.

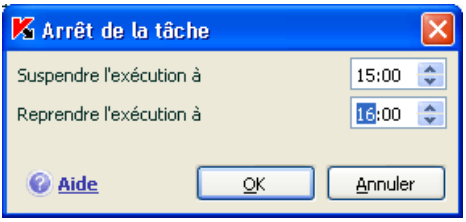


Illustration 21. Suspension du composant

Pour désactiver le composant en cas d'utilisation d'applications gourmande s en ressources, cochez la case **Selon les applications** (cf. ill. 22) et dans la fenêtre qui s'ouvre après avoir cliqué sur le bouton **Liste**, composez la liste des programmes.

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.

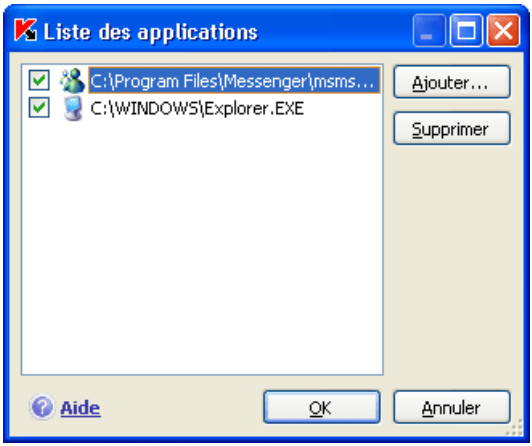


Illustration 22. Constitution de la liste des applications

7.2.4. Utilisation des méthodes d'analyse heuristique

Les méthodes d'analyse heuristique sont exploitées par plusieurs composants de la protection en temps réel, par exemple l'Antivirus Fichier, l'Antivirus Courrier et l'Antivirus Internet, ainsi que par la tâche de recherche de virus.

Comme vous le savez, l'analyse sur la base des signatures à l'aide de bases constituées antérieurement et contenant les définitions des menaces connues ainsi que les méthodes de réparation, indique clairement si l'objet analysé est malveillant et la catégorie à laquelle il appartient. La méthode heuristique, au contraire de la méthode qui repose sur les signatures, ne vise pas à trouver la signature d'un code malveillant mais bien les séquences d'opérations typiques qui permettent de tirer, avec un certain niveau de certitude, des conclusions sur la nature d'un fichier. L'avantage de la méthode heuristique tient au fait que son application ne requiert pas l'existence de bases. Ainsi, les nouvelles menaces peuvent être identifiées avant que leur activité ne soit remarquée par les spécialistes des virus.

Le module d'analyse heuristique simule l'exécution de l'objet dans un environnement virtuel sécurisé de Kaspersky Anti-Virus. Si le comportement de l'objet n'est pas suspect, il pourra être exécuté dans l'environnement de travail. Si des actions suspectes sont décelées à cette occasion, l'objet est considéré comme malveillant et son exécution sera interdite ou un message invitera l'utilisateur à choisir l'action à réaliser :

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

Pour utiliser la méthode heuristique, cochez la case  **Utiliser l'analyseur heuristique**. Vous pouvez, en plus, sélectionner le niveau d'analyse à l'aide du curseur : **superficielle**, **moyenne** ou **détaillée**. Le niveau de détail de l'analyse garantit l'équilibre entre la minutie de la recherche des virus, c.-à-d. la qualité, et la charge imposée aux ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse est élevé, plus les ressources du système seront sollicitée et plus longtemps elle prendra.

Attention !

Les nouvelles menaces, découvertes grâce à l'analyseur heuristique, sont étudiées par les spécialistes de Kaspersky Lab et les outils de réparation sont proposés dans les bases actualisées toutes les heures.

Par conséquent, si vous procédez régulièrement à la mise à jour des bases de l'application et que vous maintenez la protection de l'ordinateur au niveau optimal, il n'est pas nécessaire de recourir à la méthode d'analyse heuristique en permanence.

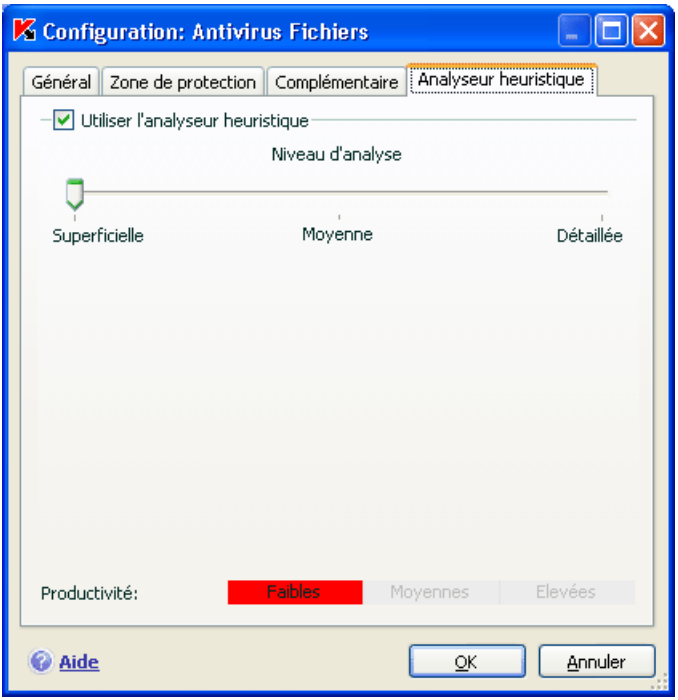


Illustration 23. Utilisation des méthodes d'analyse heuristique

L'onglet **Analyseur heuristique** (cf. ill. 23) vous permet d'activer/désactiver l'utilisation des méthodes heuristiques d'identification des nouvelles menaces dans le cadre de l'utilisation d'Antivirus Fichiers. Pour ce faire, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

2. Cliquez sur **Configuration** dans le groupe **Niveau de protection** (cf. ill. 17).
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Analyseur heuristique**.

7.2.5. 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. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection** (cf. ill. 17).

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**.

7.2.6. 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 1.2, p. 10).
- *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 :

Ouvrez la fenêtre de configuration de l'application et sélectionnez **Antivirus Fichiers** dans la rubrique **Protection**. Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 24).

Illustration 24. Actions que peut exécuter Antivirus Fichiers sur un objet dangereux

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
Confirmer l'action	Antivirus Fichiers affiche un message d'avertissement qui reprend les informations relatives à l'objet malveillant source de l'infection (potentielle) et propose l'une des actions suivantes. Les actions varient en fonction de l'état de l'objet.
Bloquer l'accès	Antivirus Fichiers bloque l'accès à l'objet. Les informations sont consignées dans le rapport (cf. point 15.3, p. 182). Vous pouvez plus tard tenter de réparer cet objet.
Bloquer l'accès **Réparer**	Antivirus Fichiers bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à nouveau disponible. Si la réparation échoue, l'objet reçoit le statut potentiellement infecté et il est placé en quarantaine (cf. point 15.1, p. 175). Les informations relatives à cette situation sont consignées dans le rapport. Il est possible de tenter de réparer cet objet ultérieurement.

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
Bloquer l'accès **Réparer** **Supprimer si la réparation est impossible**	Antivirus Fichiers bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à nouveau disponible. Si la réparation de l'objet échoue, il sera supprimé. Une copie de sauvegarde sera conservée dans le dossier de sauvegarde (cf. point 15.2, p. 179).
Bloquer l'accès **Supprimer**	L'antivirus de fichiers bloque l'accès à l'objet et le supprime.

Quel que soit le statut de l'objet (infecté ou potentiellement infecté), Kaspersky Anti-Virus crée une copie de sauvegarde avant de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

7.3. Réparation différée des objets

Si vous avez sélectionné **Bloquer l'action** en tant qu'action réalisée sur les objets malveillants, ces objets ne seront pas réparés et ils ne seront pas accessibles.

Si vous avez sélectionné

Bloquer l'accès

Réparer

alors, tous les objets qui n'ont pas été réparés seront bloqués.

Pour pouvoir à nouveau accéder aux objets bloqués, vous devrez les réparer. Pour ce faire :

1. Sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection** de la fenêtre principale de l'application et cliquez sur le lien Ouvrir le rapport.
2. Sélectionnez les objets qui vous intéressent sur l'onglet **Détectés** 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. PROTECTION ANTIVIRUS DU COURRIER

Kaspersky Anti-Virus contient un composant spécial qui protège le courrier entrant et sortant. Il s'agit de *l'antivirus de messagerie électronique*. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire système de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI[1] et NNTP ainsi que via les connexions sécurisées (SSL) ou via les protocoles POP3 et IMAP.

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

La protection du courrier est réalisée par défaut selon l'algorithme suivant :

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par l'antivirus de messagerie électronique.
2. Le message est décomposé selon ses parties constitutives, à savoir : l'en-tête du message, le corps du message et la pièce jointe.
3. Le corps et la pièce jointe (y compris les objets OLE) sont soumis à la recherche d'éventuels objets dangereux. L'identification des objets malveillants est réalisée à l'aide des *bases* utilisées par le logiciel et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.
4. Les comportements suivants sont envisageables à l'issue de l'analyse :
    - Si le corps du message ou la pièce jointe contient un code malveillant, l'antivirus de messagerie électronique bloque le message, place une copie de l'objet infecté dans le *dossier de sauvegarde* et tente de réparer l'objet. Si la réparation réussit, l'utilisateur peut accéder au message. Dans le cas contraire, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial

[1] L'analyse du courrier sur le protocole MAPI est réalisé à l'aide d'un plug-in spécial pour Microsoft Office Outlook et The Bat !

est inclus dans l'objet du message. Ce texte indique que le message a été traité par Kaspersky Anti-Virus.

- Si le corps du message ou la pièce jointe contient un code semblable à un code malveillant, sans garantie, la partie suspecte du message est placée dans un dossier spécial : la *quarantaine*.
- Si aucun code malveillant n'a été découvert dans le message, le destinataire pourra y accéder immédiatement.

Un plug-in spécial (cf. point 8.2.2, p. 104) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Outlook.

Si vous utilisez The Bat!, Kaspersky Anti-Virus peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. point 8.2.3, p. 105) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de Kaspersky Anti-Virus.

S'agissant des autres clients de messageries (dont Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), l'antivirus de messagerie analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

Sous Thunderbird, les messages transmis via le protocole IMAP ne sont pas soumis à l'analyse antivirus en cas d'utilisation de règles de tri des messages.

8.1. Sélection du niveau de sécurité du courrier

Kaspersky Anti-Virus assure la protection du courrier selon un des 3 niveaux suivants (cf. ill. 25):

Protection maximale : le contrôle du courrier entrant et sortant est total. Le logiciel analyse en détail les pièces jointes, indépendamment du temps d'analyse, y compris les archives.

Recommandé : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets que ceux du niveau **Protection maximale**, à l'exclusion des pièces jointes et des messages dont l'analyse dure plus de trois minutes.

Vitesse maximale : la configuration de ce niveau de protection vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de messages analysés est réduit. Ce niveau assure uniquement l'analyse du courrier entrant, mais pas des archives et des objets (messages) joints dont l'analyse dure plus de trois minu-

tes. L'utilisation de ce niveau est recommandée uniquement si d'autres moyens de protection du courrier sont installés sur votre ordinateur.

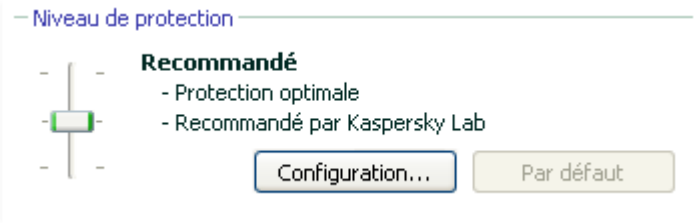


Illustration 25. Sélection du niveau de protection du courrier

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

Vous pouvez augmenter ou réduire le niveau de protection du courrier 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 d'objets de messages électroniques soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si pour une raison quelconque 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 **Autre**. Voici un exemple où la modification des paramètres du niveau proposé pourrait s'imposer.

Exemple:

votre ordinateur est en dehors du réseau local et se connecte à Internet via un modem. Vous utilisez Microsoft Outlook Express pour envoyer et recevoir vos messages ainsi qu'un service de messagerie en ligne gratuit. Pour diverses raisons, votre courrier contient souvent des archives en pièce jointe. Comment protéger au maximum votre ordinateur contre une infection via le courrier électronique ?

Conseil pour la sélection du niveau :

l'analyse de la situation permet de conclure que le risque d'infection via le courrier électronique est très élevé (absence de protection centralisée du courrier et des moyens d'accès à Internet).

Dans ce cas, il est conseillé d'utiliser le niveau **Protection maximale** qui sera modifié de la manière suivante : il est conseillé de réduire la durée d'analyse des objets en pièce jointe, par exemple 1 à 2 minutes. La majorité des archives jointes sera analysée et la vitesse de traitement du courrier ne sera pas sensiblement ralentie.

Pour modifier les paramètres du niveau de protection actuel :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Courrier** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 25).
3. Dans la fenêtre qui s'ouvre, modifiez les paramètres de la protection du courrier puis cliquez sur **OK**.

8.2. Configuration de la protection du courrier

Les règles d'analyse du courrier sont définies à l'aide de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent le flux de messagerie protégé (cf. point 8.2.1, p. 102);
- Les paramètres qui définissent l'utilisation des méthodes d'analyse heuristique (cf. point 8.2.4, p. 107);
- Les paramètres qui définissent l'analyse des messages dans Microsoft Office Outlook (cf. point 8.2.2, p. 104) et The Bat! (cf. point 8.2.3, p. 105);
- Les paramètres qui définissent les actions à réaliser sur les objets dangereux des messages (cf. point 8.2.6, p. 109).

Tous ces types de paramètres sont abordés en détails ci-après.

8.2.1. Sélection du flux de messagerie protégé

L'antivirus de messagerie vous permet de choisir quel flux de messages électroniques sera soumis à la recherche d'éventuels objets dangereux.

Par défaut, le composant assure la protection du courrier selon les paramètres du niveau **Recommandé**. Cela signifie que le courrier entrant et le courrier sortant sont analysés. Au tout début de l'utilisation, il est conseillé d'analyser le courrier sortant car il est possible que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

Si vous êtes certains que les messages que vous envoyez ne contiennent pas d'objets dangereux, vous pouvez désactiver la protection du courrier sortant. Pour ce faire :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Courrier** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 25).
3. Dans la fenêtre choisissez l'option **Uniquement le courrier entrant** dans le bloc **Zone de protection**.

En plus de la sélection du flux de messagerie, vous pouvez également préciser s'il faut contrôler les archives en pièce jointe et définir la durée maximale d'analyse d'un objet. Ces paramètres sont définis dans le bloc **Optimisation**.

Si votre ordinateur n'est protégé par aucun moyen du réseau local et si l'accès à Internet s'opère sans serveur proxy ou pare-feu, il est conseillé de ne pas désactiver l'analyse des archives en pièce jointe ou de saisir une durée maximale pour l'analyse des objets.

Si vous travaillez dans un environnement protégé, vous pouvez modifier la limite de la durée d'analyse des objets afin d'accroître la vitesse.

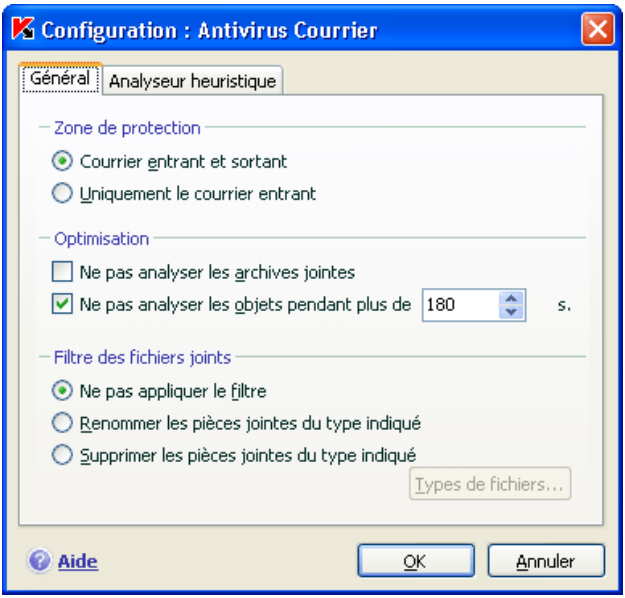


Illustration 26. Configuration de la protection du trafic de messagerie

Dans le bloc **Filtre des fichiers joints**, vous pouvez configurer les conditions de filtrage des objets joints aux messages électroniques :

- **Ne pas appliquer le filtre** : ne procède pas au filtrage complémentaire des pièces jointes.
- **Renommer les pièces jointes du type indiqué** : filtre les pièces jointes d'un certain format et remplace le dernier caractère du nom du fichier par un trait de soulignement. Vous pouvez sélectionner le type de fichier dans la fenêtre qui s'ouvre à l'aide du bouton **Types de fichiers**.
- **Supprimer les pièces jointes du type indiqué** : filtre et supprime les fichiers en pièce jointe d'un certain type. Vous pouvez sélectionner le type de fichier dans la fenêtre qui s'ouvre à l'aide du bouton **Types de fichiers...**.

Pour obtenir de plus amples informations sur les types de fichier qui peuvent être filtrés, consultez la rubrique A.1 à la page 237.

L'utilisation d'un filtre offre une protection supplémentaire car les programmes malveillants se propagent via courrier électronique sous la forme de pièces jointes. Le changement de nom ou la suppression de la pièce jointe permet de protéger votre ordinateur contre l'exécution automatique d'une pièce jointe à la réception du message.

8.2.2. Configuration de l'analyse dans Microsoft Office Outlook

Si vous utilisez Microsoft Office Outlook, vous pouvez configurer davantage la recherche d'éventuels virus dans votre courrier.

Lors de l'installation de Kaspersky Anti-Virus, un plug-in spécial est intégré à Microsoft Office Outlook. Il vous permet de passer rapidement à la configuration des paramètres de l'antivirus de messagerie et de définir à quel moment la recherche d'éventuels objets dangereux sera lancée.

Le plug-in prend la forme de l'onglet **Antivirus Courrier** dans le menu **Services** → **Paramètres** (cf. ill. 27).

Sélectionnez un mode d'analyse du courrier :

- **Analyser à la réception** : analyse chaque message dès son arrivée dans votre boîte aux lettres.
- **Analyser à la lecture** : analyse le message lorsque vous l'ouvrez pour le lire.
- **Analyser à l'envoi** :analyse tous les messages que vous envoyez, au moment de l'envoi.

Attention !

Si Microsoft Office Outlook se connecte au serveur de messagerie via le protocole IMAP, il est conseillé de ne pas utiliser le mode **Analyser à la réception.** Ce mode implique la copie du message sur l'ordinateur local au moment de l'arrivée sur le serveur, ce qui supprimera l'avantage du protocole IMAP, à savoir l'économie de trafic et la gestion des lettres non sollicitées sur le serveur sans les copier sur l'ordinateur de l'utilisateur.

L'action qui sera exécutée sur l'objet dangereux du message est définie dans les paramètres de l'antivirus de messagerie électronique. Pour passer à la configuration de ces paramètres, cliquez sur ici.

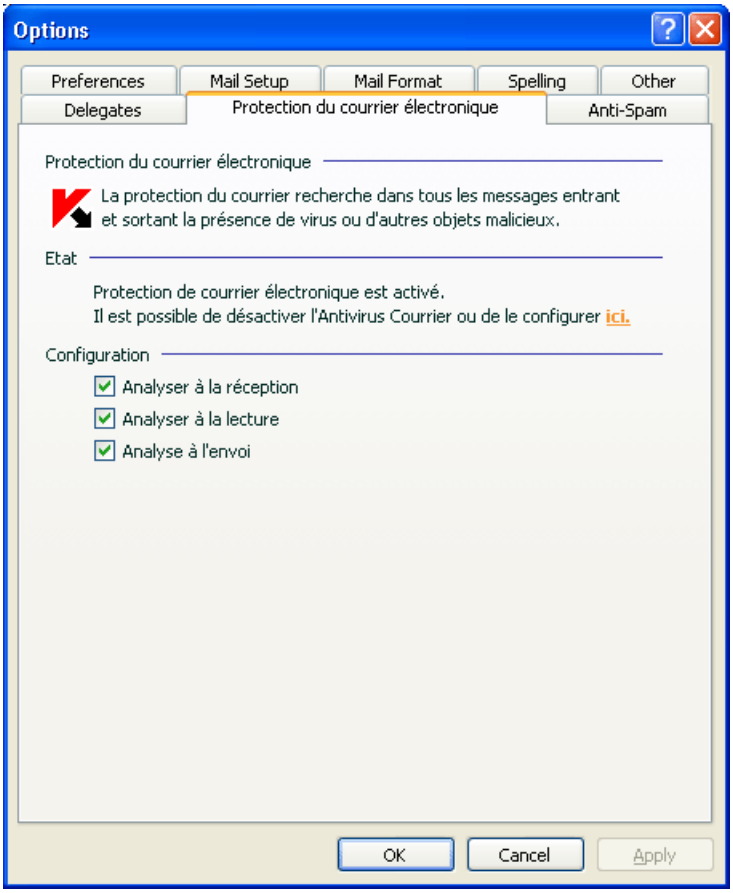


Illustration 27. Configuration détaillée de la protection du courrier dans Microsoft Office Outlook

8.2.3. Configuration de l'analyse du courrier dans The Bat!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Attention !

Les paramètres de l'antivirus de messagerie qui définissent l'analyse ou non du courrier entrant et sortant ainsi que les actions à réaliser sur les objets dangereux de messages et les exclusions sont ignorées. Les seuls élément pris en considération par The Bat!, sont l'analyse des pièces jointes et la restriction sur la durée de l'analyse d'un objet du message (cf. point 8.2.1, p. 102).

Pour passer à la configuration de la protection du courrier indésirable dans The Bat! :

1. Sélectionnez l'élément **Configuration** dans le menu **Propriétés** du client de messagerie.
2. Sélectionnez le nœud **Protection contre les virus** dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable (cf. ill. 28) sont appliqués à tous les modules antivirus de l'ordinateur compatibles avec The Bat!

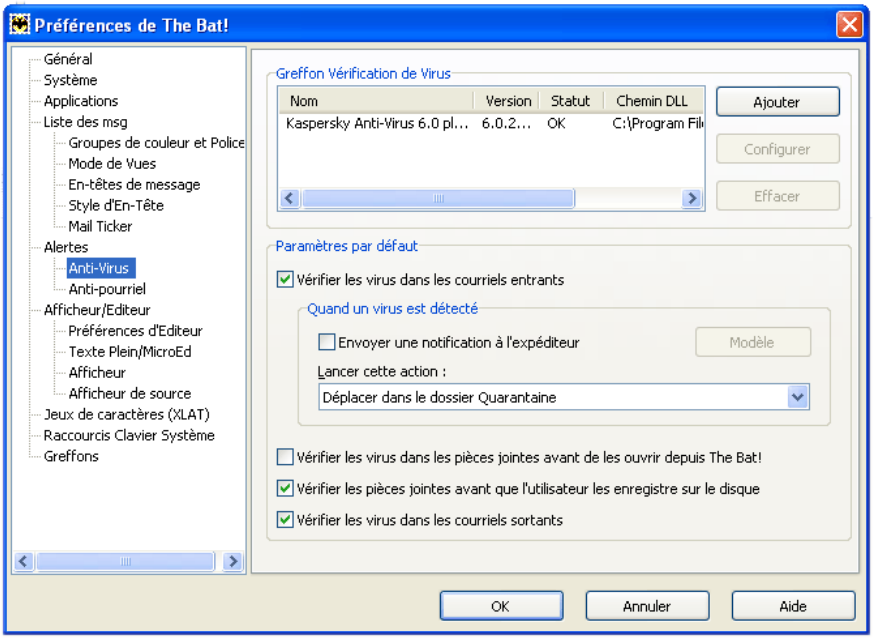


Illustration 28. Configuration du courrier dans The Bat!

Vous devez définir :

- Le flux de messagerie qui sera soumis à l'analyse antivirus (courrier entrant, sortant);
- Le moment auquel aura lieu l'analyse antivirus des objets du message (à l'ouverture du message, avant l'enregistrement sur le disque);
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :

  Tenter de réparer les parties infectées : tente de réparer l'objet infecté du message; si la réparation est impossible, l'objet reste dans le message. Kaspersky Anti-Virus vous avertira obligatoirement si l'objet du message électronique est infecté. Même si vous choisissez **Supprimer** dans la fenêtre de notification de l'antivirus de messagerie électronique, l'objet restera dans le message car l'action à réaliser sur le message, sélectionnée dans The Bat! prévaut sur l'action de l'antivirus de messagerie électronique.

  Supprimer les parties infectées : supprime l'objet dangereux du message, qu'il soit infecté ou soupçonné d'être infecté.

  Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Attention !

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés dans The Bat! par un titre spécial.

8.2.4. Utilisation des méthodes d'analyse heuristique

Les méthodes d'analyse heuristique sont exploitées par plusieurs composants de la protection en temps réel ainsi que par la tâche de recherche de virus (pour de plus amples informations, consultez le point 7.2.4 à la page 93).

Vous pouvez activer/désactiver l'utilisation des méthodes heuristiques d'identification des nouvelles menaces dans le cadre de l'utilisation d'Antivirus Courrier. Pour ce faire, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Courrier** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 25).

3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Analyseur heuristique** (cf. ill. 29).

Pour utiliser les méthodes heuristiques, cochez la case **Utiliser l'analyseur heuristique**. De plus, vous pouvez sélectionner le niveau de détail de l'analyse. Pour ce faire, mettez le curseur sur une des trois positions : **superficielle, moyenne** ou **détaillée**.

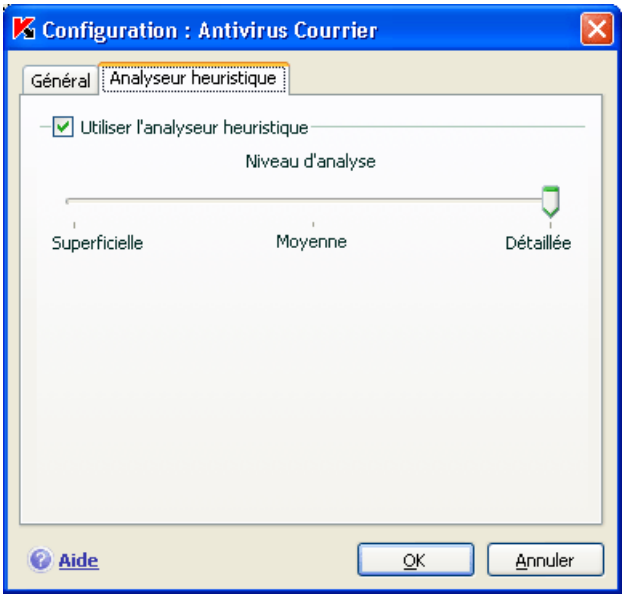


Illustration 29. Utilisation des méthodes d'analyse heuristique

8.2.5. Restauration des paramètres de protection du courrier par défaut

Lorsque vous configurez Antivirus Courrier, vous avez toujours la possibilité de revenir aux paramètres recommandés par les experts de Kaspersky Lab et regroupés sous le niveau **Recommandé**.

Pour restaurer les paramètres de protection du courrier par défaut :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Courrier** dans la section **Protection**.
2. Cliquez sur **Par défaut** dans la section **Niveau de protection** (cf. ill. 25).

8.2.6. Sélection des actions à réaliser sur les objets dangereux des messages

Si l'analyse antivirus d'un message électronique indique que le message ou l'un de ses objets (corps ou pièce jointe) est infecté ou soupçonné d'être infecté, la suite des opérations de l'antivirus de messagerie dépendra du statut 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*), pour de plus amples renseignements, consultez le point 1.2 à la page 10);
- *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, Antivirus Courrier affiche un message par défaut en cas de découverte d'un objet dangereux et potentiellement infecté et propose un choix d'actions.

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

Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 30).

Illustration 30. Sélection de l'action à réaliser sur l'objet dangereux du message

Examinons en détails les différentes options en matière de traitement des objets dangereux des messages électroniques.

Action choisie	Résultat de l'action
Confirmer l'action	Antivirus Courrier affiche un message d'avertissement qui reprend les informations relatives à l'objet malveillant source de l'infection (potentielle) et propose l'une des actions suivantes.
Bloquer l'accès	Antivirus Courrier bloque l'accès à l'objet. Les informations relatives à cette situation sont consignées dans le rapport (cf. point 15.3, p. 182). Vous pouvez plus tard tenter de réparer cet objet.
Bloquer l'accès **Réparer**	Antivirus Courrier bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à nouveau disponible. Si la réparation est impossible, l'objet est placé en quarantaine (cf. point 15.1, p. 175). Les informations relatives à cette situation sont consignées dans le rapport. Il est possible de tenter de réparer cet objet ultérieurement.
Bloquer l'accès **Réparer** **Supprimer si la réparation est impossible**[2]	Antivirus Courrier bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à nouveau disponible. Si la réparation de l'objet échoue, il sera supprimé. Une copie de l'objet est conservée dans le dossier de sauvegarde. L'objet dont l'état est potentiellement infecté sera placé en quarantaine.
Bloquer l'accès **Supprimer**	Si Antivirus Courrier découvre un objet infecté ou potentiellement infecté, il le supprime sans avertir au préalable l'utilisateur.

Avant la réparation ou la suppression d'un objet, Kaspersky Anti-Virus crée une copie de sauvegarde avant de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde (cf. point 15.2, p. 179) au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

[2] Si vous utilisez The Bat! en tant que client de messagerie, les objets dangereux des messages seront soit réparés, soit supprimé avec cette action de l'antivirus de messagerie électronique (en fonction de l'action sélectionnée dans The Bat!).

CHAPITRE 9. PROTECTION INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur à un risque d'infection par des programmes dangereux. Ceux-ci peuvent s'introduire dans votre ordinateur pendant que vous lisez certains articles en ligne.

Pour garantir la sécurité de vos données lorsque vous utilisez Internet, Kaspersky Anti-Virus propose un composant spécial : Antivirus Internet. Il protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

Attention !

La protection Internet prévoit le contrôle du trafic http qui transite uniquement via les ports indiqués dans la liste des ports contrôlés (cf. point 15.4, p. 190). La liste des ports le plus souvent utilisés pour le transfert du courrier et du trafic HTTP est livrée avec le logiciel. Si vous utilisez des ports absents de cette liste, vous devrez les ajouter afin de protéger le trafic qui transite via ces derniers.

Si vous travaillez dans un domaine non protégé, il est conseillé d'utiliser l'antivirus Internet en guise de protection. Si votre ordinateur fonctionne dans un réseau protégé par un pare-feu ou un filtre de trafic HTTP, l'antivirus Internet vous offrira une protection supplémentaire.

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

Examinons les détails du fonctionnement de ce composant.

l'antivirus Internet est composé de deux modules qui garantissent :

- La *protection du trafic HTTP* : analyse de tous les objets qui arrivent sur l'ordinateur via le protocole HTTP.
- *Analyse des scripts* : analyse de tous scripts traités dans Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancés lors de l'utilisation de l'ordinateur, y compris d'Internet.

  S'agissant de Microsoft Internet Explorer, il existe un plug-in spécial qui s'intègre au programme lors de l'installation de Kaspersky Anti-Virus. Le bouton  qui apparaît dans la barre d'outils du navigateur confirme l'installation du plug-in. En cliquant sur cette icône, vous ouvrez un

panneau qui reprend les statistiques d'Anti-Virus sur le nombre de scripts bloqués et analysés.

La protection du trafic HTTP s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP est intercepté et analysé par l'antivirus Internet pour découvrir la présence de code malveillant. L'identification des objets malveillants est réalisée à l'aide des *bases* utilisées par Kaspersky Anti-Virus et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :

   Si la page Web ou l'objet auquel l'utilisateur souhaite accéder contient un code malveillant, l'accès sera bloqué. Dans ce cas, un message s'affiche et signale que la page ou l'objet sollicité est infecté.

   Si le fichier ou la page Web ne contient aucun code malveillant, l'utilisateur peut y accéder tout de suite.

L'analyse des scripts est réalisée selon l'algorithme suivant :

1. Chaque script lancé sur une page Web est intercepté par l'antivirus Internet et soumis à une analyse antivirus.
2. Si le script contient un code malveillant, l'antivirus Internet le bloc et avertit l'utilisateur à l'aide d'une infobulle.
3. Si le script ne contient aucun code malicieux, il est exécuté.

Attention!

Pour intercepter le trafic http et les scripts et y rechercher d'éventuels virus, il faut qu'Antivirus Internet soit lancé avant l'instauration de la connexion avec le site Internet. Dans le cas contraire, le trafic ne sera pas analysé.

9.1. Sélection du niveau de sécurité Internet

Kaspersky Anti-Virus assure la protection de votre utilisation d'Internet selon un des 3 niveaux suivants (cf. ill. 31):

Protection maximale : le contrôle des scripts et des objets reçus via le protocole HTTP est total. Le logiciel analyse en détail tous les objets à l'aide des signatures complètes. Ce niveau de protection est recommandé dans les environnements agressifs lorsque aucun autre moyen de protection du trafic HTTP n'est utilisé.

Recommandé : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets que ceux du niveau **Protection maximale**, si ce n'est que la durée de mise en cache des fragments de fichier est restreinte, ce qui permet d'accélérer l'analyse et le transfert des objets à l'utilisateur.

Vitesse maximale : la configuration de ce niveau de protection vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume d'objets analysés est réduit vu l'utilisation d'un ensemble restreint bases de l'application. L'utilisation de ce niveau est recommandée uniquement si d'autres moyens de protection du trafic Internet sont installés sur votre ordinateur.

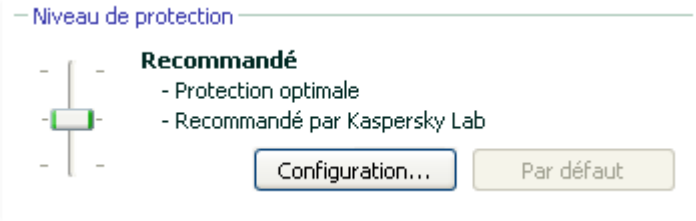


Illustration 31. Sélection du niveau de protection d'Internet

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

Vous pouvez augmenter ou réduire le niveau de protection du courrier 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 d'objets soumis à la recherche de code malveillant sera réduit, plus la vitesse de l'analyse sera élevée

Si pour une raison quelconque 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 **Autre**. Voici un exemple où la modification des paramètres du niveau proposé pourrait s'imposer:

Exemple:

Votre ordinateur se connecte à Internet via modem. Il ne fait pas partie du réseau local et la protection antivirus du trafic HTTP entrant est absente.

Dans le cadre de vos activités professionnelles, vous téléchargez souvent de gros fichiers. L'analyse de tels fichiers prend en général un certain temps.

Comment protéger au maximum votre ordinateur contre une infection via le trafic HTP ou les scripts ?

Conseil pour la sélection du niveau :

l'analyse de la situation permet de conclure que votre ordinateur fonctionne dans un niveau agressif et que le risque d'infection via le trafic HTTP est très élevé (absence de protection centralisée du trafic Internet et des moyens d'accès à Internet).

Dans ce cas, il est conseillé d'utiliser le niveau **Vitesse maximale** qui sera modifié de la manière suivante : il est conseillé de limiter dans le temps la mise en cache des fragments de fichiers lors de l'analyse.

Pour modifier les paramètres du niveau de protection proposé par défaut :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Internet** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 31).
3. Dans la fenêtre qui s'ouvre, modifiez les paramètres de la protection du courrier puis cliquez sur **OK**.

9.2. Configuration de la protection Internet

La protection Internet analyse tous les objets téléchargés sur votre ordinateur via le protocole HTTP et assure le contrôle de tous les scripts WSH (JavaScript, Visual Basic Script, etc).

Vous pouvez configurer différents paramètres de l'antivirus Internet afin d'accélérer la vitesse de fonctionnement du composant, notamment :

- Définir les paramètres généraux d'analyse (cf. point 9.2.1, p. 115);
- Composer la liste des adresses dont le contenu est fiable (cf. point 9.2.2, p 116);

- Activer/désactiver l'utilisation des méthodes d'analyse heuristique (cf. point 9.2.3, p. 117).

Vous pouvez également sélectionner les actions que l'antivirus Internet exécutera sur les objets du trafic HTTP.

Tous ces types de paramètres sont abordés en détails ci-après.

9.2.1. Paramètres généraux d'analyse

Afin d'accroître le taux de détection des codes malveillants, Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. Dans cette méthode, l'analyse est réalisée uniquement une fois que l'objet entier a été reçu. Ensuite, l'objet est soumis à une recherche de virus et, en fonction des résultats de celle-ci, il est soit transféré au destinataire ou bloqué.

Sachez toutefois que la mise en cache augmente la durée de traitement de l'objet et du transfert à l'utilisateur. Elle peut également provoquer des problèmes au niveau de la copie et du traitement de gros objets en raison de l'écoulement du délai de connexion du client HTTP.

Pour résoudre ce problème, nous vous proposons de limiter dans le temps la mise en cache des fragments des objets. Une fois cette attente écoulée, chaque partie du fichier reçue sera transmise à l'utilisateur sans vérification et l'objet sera analysé complètement une fois qu'il sera copié. Ceci permet de réduire la durée du transfert de l'objet à l'utilisateur et de résoudre le problème des déconnexions sans nuire à la sécurité lors de la connexion à Internet.

Par défaut, la limitation dans le temps de la mise en cache des fragments est de 1 seconde. L'augmentation de cette valeur ou la levée de la restriction dans le temps augmente le niveau de l'analyse antivirus virus mais entraîne un certain ralentissement au niveau de l'accès à l'objet.

Pour établir une restriction dans le temps pour la mise en cache des fragments ou pour lever cette restriction :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Internet** dans la section **Protection**.
2. Cliquez sur **Configuration** dans la fenêtre de configuration de l'antivirus Internet (cf. ill. 31).
3. Sélectionnez la valeur adéquate dans le bloc **Paramètres d'analyse** de la fenêtre qui s'affiche (cf. ill. 32).

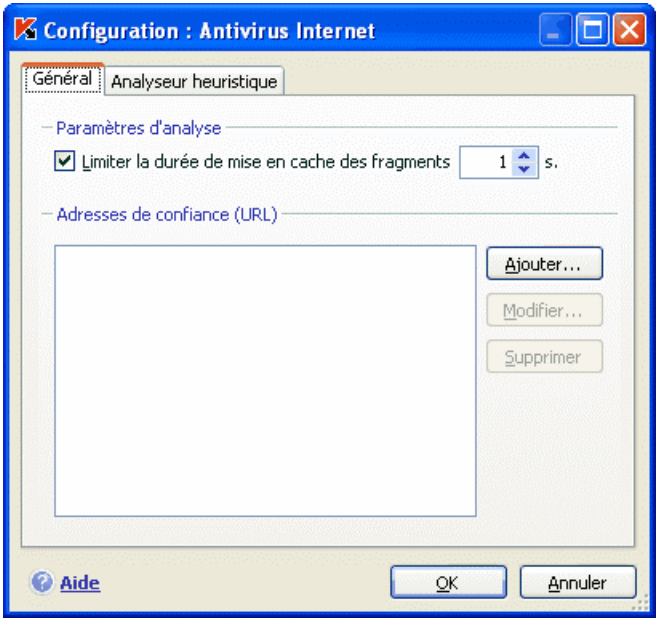


Illustration 32. Configuration du niveau de protection Internet

9.2.2. Constitution de la liste des adresses de confiance

Vous pouvez créer une liste d'adresses de confiance pour lesquelles vous n'avez absolument aucun doute au niveau du contenu. Les informations issues de ces adresses ne seront pas soumises à la recherche d'objets dangereux. Cela peut être utile lorsque l'antivirus Internet gêne le chargement d'un fichier quelconque en bloquant le téléchargement.

Pour constituer la liste des adresses de confiance :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Internet** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 31).
3. Composez, dans la fenêtre qui s'ouvre (cf. ill. 32), la liste des serveurs de confiance dans la zone **Adresses de confiance (URL)**. Utilisez pour ce faire les boutons situés à droite.

Lors de la saisie d'une adresse de confiance, vous pouvez choisir un masque à l'aide des caractères spéciaux suivants :

***** : n'importe quelle séquence de caractères.

Exemple : le masque ***abc*** signifie que toute adresse contenant la séquence **abc** ne sera pas analysée, par exemple www.virus.com/download_virus/page_0-9abcdef.html.

? : n'importe quel caractère.

Exemple : le masque **Patch_123?.com** signifie que l'adresse contenant cette séquence de caractères suivie de n'importe quel caractère après le "3" ne sera pas analysée, par exemple **Patch_1234.com**. Toutefois, l'adresse **patch_12345.com** sera quant à elle analysée.

Au cas où les caractères ***** et **?** feraient partie d'une URL authentique ajoutée à la liste, il est indispensable d'ajouter également le caractère **** qui annule le caractère *****, **?**ou **** qui le suit

Exemple : il faut absolument ajouter à la liste des adresses de confiance l'URL suivante : www.virus.com/download_virus/virus.dll?virus_name=

Afin que Kaspersky Anti-Virus n'interprète pas **?** comme un symbole d'exclusion, il faut le faire précéder du caractère ****. Ainsi, notre URL ajoutée à la liste des adresses de confiance deviendra : www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Utilisation des méthodes d'analyse heuristique

Les méthodes d'analyse heuristique sont exploitées par plusieurs composants de la protection en temps réel ainsi que par la tâche de recherche de virus (pour de plus amples informations, consultez le point 7.2.4 à la page 93).

Vous pouvez activer/désactiver l'utilisation des méthodes heuristiques d'identification des nouvelles menaces dans le cadre de l'utilisation d'Antivirus Internet. Pour ce faire, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Internet** dans la section **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection**.
3. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Analyseur heuristique** (cf. ill. 29).

Pour utiliser les méthodes heuristiques, cochez la case **Utiliser l'analyseur heuristique**. De plus, vous pouvez sélectionner le niveau de détail de l'analyse.

Pour ce faire, mettez le curseur sur une des trois positions : **superficielle, moyenne** ou **détaillée**.

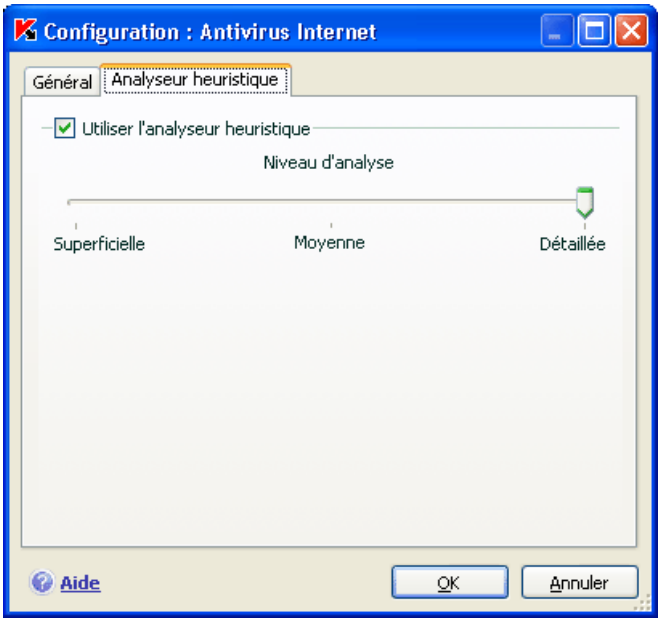


Illustration 33. Utilisation des méthodes d'analyse heuristique

9.2.4. Restauration des paramètres de protection Internet par défaut

Lorsque vous configurez Antivirus Internet, vous avez toujours la possibilité de revenir aux paramètres recommandés par les experts de Kaspersky Lab et regroupés sous le niveau **Recommandé**.

Pour restaurer les paramètres de protection Internet par défaut :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Antivirus Internet** dans la section **Protection**.
2. Cliquez sur **Par défaut** dans la section **Niveau de protection** (cf. ill. 31).

9.2.5. Sélection des actions à réaliser sur les objets dangereux

Si l'analyse d'un objet du trafic HTTP détermine la présence d'un code malveillant, la suite des opérations dépendra de l'action que vous aurez spécifiée.

Pour configurer la réaction de l'antivirus Internet suite à la découvert d'un objet dangereux :

Ouvrez la fenêtre de configuration de l'application et sélectionnez **Antivirus Internet** dans la rubrique **Protection**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 34).

Par défaut, l'antivirus Internet affiche un message par défaut en cas de découverte d'un objet dangereux et suspect et propose un choix d'actions.

Illustration 34. Sélection de l'action à réaliser sur le script dangereux

Examinons en détails les différentes options en matière de traitement des objets dangereux présents dans le trafic HTTP.

Action choisie	**Résultat en cas de découverte d'un objet dangereux dans le trafic http.**
Confirmer l'action	L'antivirus Internet affiche un message d'avertissement qui reprend les informations relatives au code malveillant source de l'infection et propose l'une des actions suivantes.
Bloquer	L'antivirus Internet bloque l'accès à l'objet et affiche un message signalant le blocage. Ces informations sont également reprises dans le rapport (cf. point 15.3, p. 182).
Autoriser	L'antivirus Internet autorise l'accès à l'objet dangereux. Les informations sont consignées dans le rapport.

S'agissant des actions sur les scripts dangereux, l'antivirus Internet bloque toujours leur exécution et affiche à l'écran une infobulle qui informe l'utilisateur sur l'action exécutée. Vous ne pouvez pas modifier l'action exécutée sur un script dangereux, si ce n'est désactiver le fonctionnement du module d'analyse des scripts.

CHAPITRE 10. DEFENSE PROACTIVE DE L'ORDINATEUR

Attention !

Cette version ne contient pas le composant: **Contrôle de l'intégrité des applications** pour les ordinateurs tournant sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64.

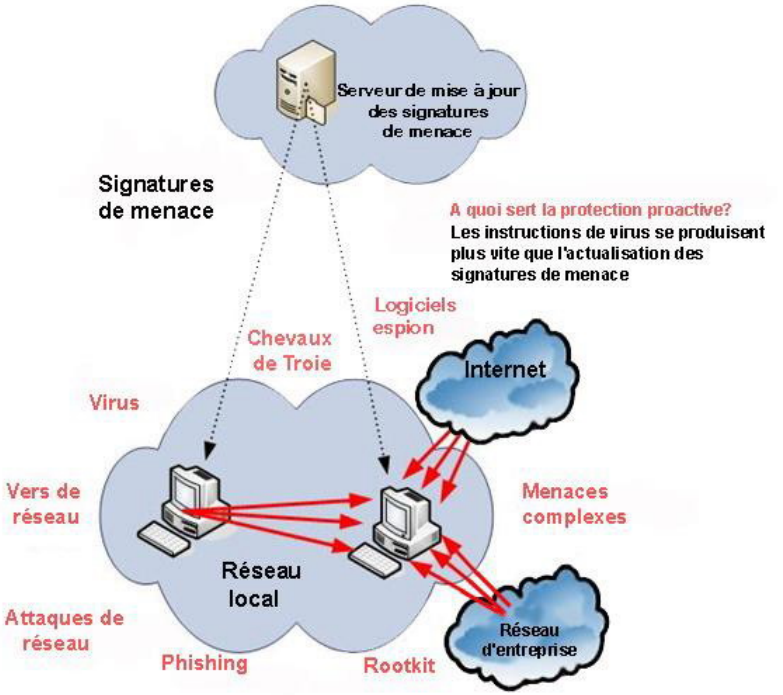
Kaspersky Anti-Virus offre non seulement une protection contre les menaces connues, mais également contre les menaces récentes qui ne sont pas encore reprises dans les bases de l'application. Cet aspect de la protection est pris en charge par un composant particulier : la *défense proactive*.

La nécessité d'une défense proactive a vu le jour dès le moment où la vitesse de propagation des programmes malveillants a dépassé la vitesse de mise à jour des protections antivirus capables de neutraliser ces menaces. Les technologies réactives de protection contre les virus requièrent au minimum une infection par la nouvelle menace, le temps nécessaire à l'analyse du code malveillant, à son ajout dans les bases de l'application et à la mise à jour de celles-ci sur l'ordinateur de l'utilisateur. Tout cela laisse suffisamment de temps à la nouvelle menace pour causer des dégâts irréparables.

Les technologies préventives sur lesquelles reposent la défense proactive de Kaspersky Anti-Virus évitent ces pertes de temps et permettent de neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. Comment est-ce possible ? A la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de l'application, les technologies préventives identifient les nouvelles menaces sur votre ordinateur en suivant les séquences d'actions exécutées par un programme quelconque. Le logiciel est livré avec un ensemble de critères qui permettent de définir la dangerosité de l'activité de l'un ou l'autre programme. Si, à la suite de l'analyse, la séquence d'actions d'un programme quelconque suscite des doutes, Kaspersky Anti-Virus applique l'action définie par la règle associée à ce genre d'activité.

L'activité dangereuse est définie par l'ensemble des actions du programme. Par exemple, en cas de découverte d'actions telles que la copie de certains programmes sur les ressources du réseau, dans le répertoire de démarrage automatique, dans la base de registres système, puis le transfert de cette copie, on peut affirmer sans crainte qu'il s'agit certainement d'un ver. Parmi les actions dangereuses, citons :

- Modifications du système de fichiers ;
- Intégration de modules dans d'autres processus ;
- Processus cachés dans le système ;
- Modification de certaines clés de la base de registres système de Microsoft Windows.



Toutes les opérations dangereuses sont surveillées et bloquées par la défense proactive. La défense proactive fonctionne selon une série de règles reprises dans le programme et rédigées par l'utilisateur. Une *règle* est en ensemble de critères qui définit l'ensemble des actions suspectes et la réaction du logiciel face à une telle activité.

Des règles distinctes sont prévues pour l'activité de l'application et contrôlent les modifications de la base de registres système et les programmes lancés sur l'ordinateur. Vous pouvez modifier la liste des règles et en ajouter de nouvelles voire supprimer ou modifier certaines. Les règles peuvent interdire ou autoriser.

Voici l'algorithme de fonctionnement de la défense proactive :

1. Directement après le démarrage de l'ordinateur, la défense proactive analyse les aspects suivants :

   - *Actions de chaque application exécutée sur l'ordinateur*. L'historique des actions exécutées et leur séquences sont enregistrées et comparées aux séquences caractéristiques des activités dangereuses (la base des types d'activités dangereuses est intégrée à Kaspersky Anti-Virus et elle est actualisée en même temps que les bases de l'application).

   - *Intégrité des modules logiciels* des applications installées sur l'ordinateur, ce qui permet d'éviter la substitution de modules, l'insertion de code malveillant.

   - *Chaque tentative de modification de la base de registres système* (suppression ou ajout de clé à la base de registres système, saisie de valeurs pour les clés dans un format incorrect empêchant toute consultation ou modification, etc.),

2. L'analyse s'opère selon les règles d'autorisation et d'interdiction de la défense proactive.

3. Les comportements suivants sont possibles en fonction des résultats de l'analyse :

   - Si l'activité répond aux conditions prévues par la règle d'autorisation de la défense proactive ou si elle n'est concernée par aucune règle d'interdiction, elle ne sera pas bloquée.

   - Si l'activité est décrite dans une règle d'interdiction, la suite de l'action du composant est régie par les instructions reprises dans la règle. En règle générale, une telle action est bloquée. Il est possible qu'une notification apparaisse à l'écran. Celle-ci reprend l'application, le type d'activité et l'historique des actions exécutées. Vous devrez décider vous-même d'autoriser ou non une telle action. Vous pouvez créer une règle pour une telle activité et annuler les actions exécutées dans le système.

     Si aucune action n'est prise lors de l'affichage de la notification de la défense proactive, l'application appliquera après un certain temps l'action par défaut recommandée pour ce type de menace. L'action par défaut peut varier selon la menace.

La défense proactive s'exécute dans le respect stricte de paramètres (cf. ill. 35) qui définissent si :

- *L'activité des applications est contrôlée sur votre ordinateur.*

  Ce mode de fonctionnement est réglementé par la case **Activer l'analyse de l'activité**. Le mode est activé par défaut, ce qui garantit une analyse rigoureuse de l'activité de n'importe quel programme lancé sur l'ordinateur. Il existe une sélection d'activités dangereuses. Pour chacune d'entres elles, vous pouvez configurer l'ordre de traitement des applications (cf. point 10.1, p. 125) avec une telle activité. Il est possible également de créer des exclusions, ce qui permet d'annuler le contrôle de l'activité pour certaines applications.

- *Le contrôle de l'intégrité de l'application est activé.*

  Cette fonction est responsable de l'intégrité des modules des applications installées sur l'ordinateur et est réglementé par la case **Activer le contrôle de l'intégrité**. L'intégrité est surveillée via le contrôle de la composition des modules du programme et de la somme de contrôle du modèle du programme en question. Vous pouvez créer des règles pour le contrôle (cf. point 10.2, p. 129) de l'intégrité des modules d'une application quelconque en ajoutant son nom à la liste des applications contrôlées.

  Ce composant de la défense proactive n'est pas disponible dans les versions installées sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64.

- *Le contrôle des modifications de la base de registres système est assuré.*

  La case **Activer la surveillance du Registre** est cochée, ce qui signifie que Kaspersky Anti-Virus analyse toutes les tentatives de modifications des clés contrôlées dans la base de registres système de Microsoft Windows.

  Vous pouvez créer vos propres règles (cf. point 10.3.2, p. 137) de contrôle en fonction de la clé de registre.

Vous pouvez configurer les exclusions (cf. point 6.9.1, p. 73) pour les modules de la défense proactive et composer des listes d'applications de confiance (cf. point 6.9.2, p. 78).

Tous ces paramètres sont abordés en détails ci-après.

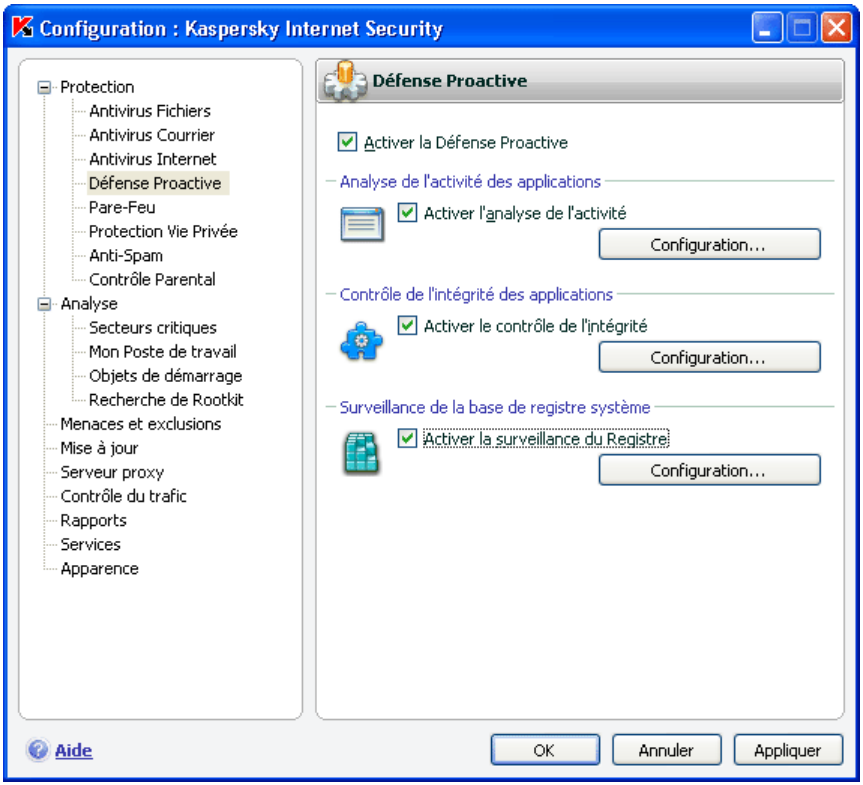


Illustration 35. Paramètres de la défense proactive

10.1. Règles de contrôle de l'activité

N'oubliez pas que la configuration du contrôle de l'activité dans l'application installée sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64 est différente de la configuration pour les applications installées sous d'autres systèmes d'exploitation.

Les informations relatives à la configuration du contrôle de l'activité pour les systèmes d'exploitation cités sont reprises à la fin de cette rubrique.

Kaspersky Anti-Virus surveille l'activité des applications sur votre ordinateur. L'application contient un ensemble de description d'événements qui peuvent être considérés comme dangereux. Une règle est créée pour chacun des événements. Si l'activité d'une application est considérée comme dangereuse, la dé-

fense proactive suivra à la lettre les instructions reprises dans la règle prévue pour ce type d'activité.

Cochez la case **Activer l'analyse de l'activité** pour lancer le contrôle de l'activité des applications.

Voici quelques exemples d'événements pouvant survenir dans le système qui seront considérés comme suspects :

- *Activité dangereuse (analyse du comportement)* : Kaspersky Anti-Virus analyse l'activité des applications installées sur l'ordinateur et sur la bas de la liste de règles composées par les experts de Kaspersky Lab, identifie les actions dangereuses ou suspectes. Il peut s'agir par exemple de l'installation cachée de programme, de la copie automatique.

- *Lancement du navigateur avec les paramètres :* l'analyse de ce type d'activité permet de déceler les tentatives de lancement caché du navigateur avec des paramètres. Une telle activité est caractéristique pour le lancement d'un navigateur Internet depuis une application quelconque avec paramètres définis de la ligne de commande : par exemple, lors de l'utilisation d'un lien vers un site Internet quelconque repris dans un message présent dans votre boîte aux lettres.

- *Implantation dans un autre processus* : ajout dans le processus d'un programme d'un code exécutable ou création d'un flux complémentaire. Cette activité est très répandue parmi les chevaux de Troie.

- *Découverte de Rootkit*. Les rootkits ou outils de dissimulation d'activité permettent de dissimuler la présence de programmes malveillants et de leurs processus dans le système. Kaspersky Anti-Virus recherche la présence de processus dissimulés dans le système d'exploitation.

- *Intrusion d'intercepteurs de fenêtre.* Cette activité se manifeste lors de la tentative de lecture de mots de passe ou d'autres informations confidentielles dans les boîtes de dialogue du système d'exploitation. Kaspersky Anti-Virus est à l'affût de cette activité en cas de tentative d'interception des données échangées entre le système d'exploitation et la boîte de dialogue.

- *Valeurs suspectes dans le registre*. La base de registres système est une base de données qui contient les paramètres système et utilisateur définissant le fonctionnement de Microsoft Windows et de tout service installé sur l'ordinateur. Les programmes malveillants qui tentent de dissimuler leur présence dans le système écrivent des valeurs incorrectes dans la base de registres. Kaspersky Anti-Virus recherche la présence de valeurs douteuses dans la base de registres système.

- *Activité suspecte dans le système*. L'application analyse les actions du système d'exploitation Microsoft Windows.

- *Découverte d'intercepteurs de frappes*. Cette activité se manifeste lorsqu'un programme malveillant intercepte les données saisies à l'aide du clavier.

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Anti-Virus et il est impossible de la modifier. Vous pouvez :

- refuser de contrôler une activité quelconque en désélectionnant la case ☑ qui se trouve en regard de son nom.
- modifier la règle qui définit le fonctionnement de la défense proactive lors de la découverte d'activités dangereuses.
- composer une liste d'exclusions (cf. point 6.9, p. 72) reprenant les applications que vous n'estimez pas dangereuses.

Pour passer à la configuration du contrôle de l'activité :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Défense proactive** dans la rubrique **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Analyse de l'activité des applications** (cf. ill. 35).

Les activités dangereuses contrôlées par la défense proactive sont reprises dans la fenêtre **Configuration: analyse de l'activité** (cf. ill. 36).

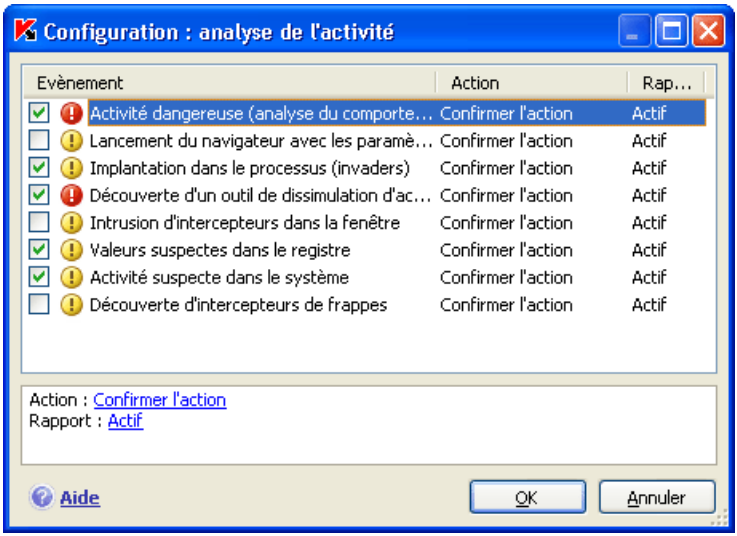


Illustration 36. Configuration du contrôle de l'activité des applications sous

Pour modifier une règle de contrôle de l'activité dangereuse, sélectionnez-la dans la liste de l'onglet **Evénement** et définissez dans la partie inférieure de la fenêtre les paramètres de la règle :

- Définissez la réaction de la défense proactive suite à la découverte d'une activité dangereuse.

  Vous pouvez sélectionner une des actions suivantes en guise de réaction : Autoriser, Confirmer l'action et Terminer le processus. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée. De plus, à la fin de l'exécution du processus, vous pouvez placer l'application suspecte en quarantaine. Pour ce faire, cliquez sur Actif/Inactif en regard du paramètre correspondant. Pour identifier les processus cachés dans le système, vous pouvez également définir un intervalle pour le lancement de l'analyse.

- Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, cliquez sur Actif/Inactif.

Afin de ne pas contrôler une activité dangereuse quelconque, désélectionnez la case ☑ qui se trouve en regard de son nom dans la liste des applications dangereuses.

Particularités de la configuration du contrôle de l'activité des applications dans Kaspersky Anti-Virus Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64 :

Si l'ordinateur tourne sous un des systèmes d'exploitation cités ci-dessus, alors seul un type d'événement est contrôlé dans le système, à savoir l'*activité dangereuse (analyse du comportement)*. Afin que Kaspersky Anti-Virus contrôle également les modifications des comptes utilisateurs en plus, cochez la case ☑ **Contrôler les comptes systèmes** (cf. Illustration 37). Cette possibilité est désactivée par défaut.

Les comptes utilisateur réglementent l'accès au système et définissent l'utilisateur et son environnement de travail, ce qui permet d'éviter d'endommager le système d'exploitation ou les données des autres utilisateurs. Les processus système sont les processus qui ont été lancé par le compte système.

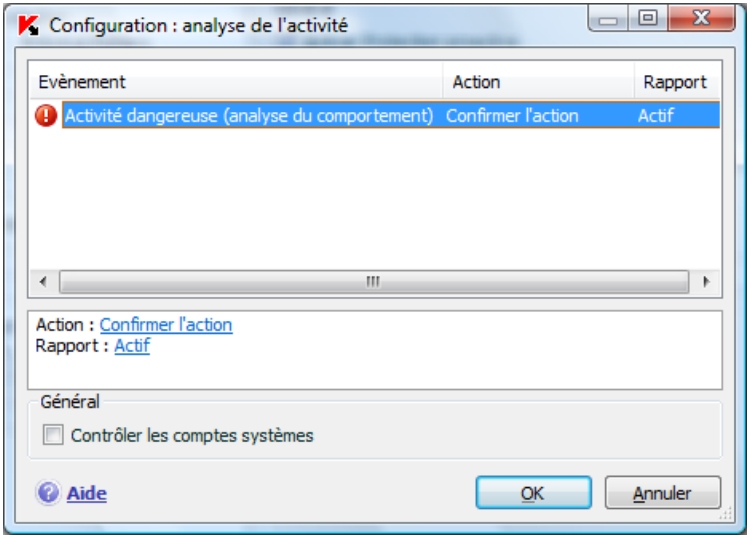


Illustration 37. Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64.

10.2. Contrôle de l'intégrité de l'application

Ce composant de la défense proactive ne fonctionne pas sur les ordinateurs tournant sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64.

Il existe de nombreux programmes critiques pour le système qui peuvent être utilisés par les codes malveillants pour se diffuser, par exemple les navigateurs Internet, les clients de messagerie, etc. En règle générale, il s'agit d'application système, de processus utilisés pour se connecter à Internet ou lors de l'utilisation du courrier ou d'autres documents. C'est pour cette raison que ces applications sont considérées comme *critiques* d'un point de vue du contrôle de leur activité.

La défense proactive contrôle les applications critiques, analyse leur activité, l'intégrité des modules et le lancement d'autres processus par ces applications. Kaspersky Anti-Virus est livré avec une liste d'applications critiques et chacune d'entre elles possède sa propre règle pour l'activité de l'application. Vous pouvez ajouter à cette liste d'autres applications que vous jugez critiques de même que supprimer ou modifier les règles pour les applications reprises dans la liste.

A côté de la liste des applications critiques, il existe également un ensemble de modules de confiance pouvant être chargés dans toutes les applications contrôlées. Il s'agit par exemple des modules qui possèdent la signature de Microsoft Corporation. Il est fort probable que les applications qui contiennent de tels modules ne soient pas malveillantes. Pour cette raison, il n'est pas nécessaire de soumettre leurs actions à un contrôle strict. Les experts de Kaspersky Lab ont composé une liste de ces modules afin de réduire la charge de votre ordinateur lors du fonctionnement de la défense proactive.

Les composants qui possèdent la signature Microsoft Corporation sont repris par défaut automatiquement dans la liste des applications de confiance. Le cas échéant, vous pouvez ajouter ou supprimer des éléments de cette liste.

Le contrôle des processus dans le système est activé en cochant la case **Activer le contrôle de l'intégrité**. La case est n'est pas sélectionnée par défaut. En cas de contrôle de l'intégrité, chaque application ou module lancé est analysé afin de voir s'il se trouve dans la liste des applications critiques ou des applications de confiance. Si l'application appartient à la liste des applications critiques, son activité sera soumise à un contrôle de la part de la défense proactive conformément à la règle définie.

Pour passer à la configuration du monitorage des processus :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Défense proactive** dans la rubrique **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Contrôle de l'intégrité des applications** (cf. ill. 35).

Examinons plus en détail le fonctionnement avec les processus critiques et les processus de confiance.

10.2.1. Configuration des règles de contrôle des applications critiques

Les *applications critiques* sont les fichiers exécutables des programmes dont il est primordial de contrôler l'activité dans la mesure où ces programmes sont utilisés par des objets malveillants pour se diffuser.

Une liste d'applications critiques, composée par les experts de Kaspersky Lab et livrée avec le logiciel, est reprise sur l'onglet **Applications contrôlées** (cf. ill. 38). Une règle encadrant l'activité de l'application est créée pour chacune de ces applications. Vous pouvez créer vos propres règles ou modifier les règles existantes.

La défense proactive analyse les opérations suivantes dans les applications critiques : lancement, modification de la composition des modules de l'application

et lancement de l'application en tant que processus fils. Pour chacune des opérations citées, vous pouvez sélectionner la réaction de la défense proactive (autoriser ou non l'opération) et préciser s'il est nécessaire de consigner l'activité dans le rapport de fonctionnement du composant. Par défaut, le lancement, la modification et le lancement de processus fils pour pratiquement toutes les applications critiques sont autorisés.

Afin d'ajouter une application à la liste des applications critiques et de créer une règle:

1. Cliquez sur le bouton **Ajouter** dans l'onglet **Applications contrôlées**. Cette action entraîne l'ouverture d'un menu contextuel. Le point **Parcourir** ouvre la boîte de dialogue traditionnelle pour la sélection des fichiers. Vous pouvez également cliquer sur le point **Applications** afin d'afficher la liste des applications ouvertes à ce moment et de sélectionner celle que vous voulez. L'application prendra la première place dans la liste. Une règle d'autorisation sera créée par défaut. Lors du premier lancement de l'application, une liste des modules utilisés au lancement est créée. Ce sont ces modules qui seront autorisés.
2. Sélectionnez la règle dans la liste et définissez-en les paramètres dans la partie inférieure de l'onglet :
   - Définissez la réaction de la défense proactive en cas de tentative de lancement, de modification de la composition ou de lancement d'une application critique en tant que processus fils.

     Vous pouvez sélectionner une des actions suivantes en guise de réaction : Autoriser, Confirmer l'action et Interdire. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée.
   - Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, utilisez le lien consigner dans le rapport / ne pas consigner dans le rapport.

Pour désactiver le contrôle de l'activité d'une application critique quelconque, il suffit de désélectionner la case ☑ qui se trouve en regard de son nom.

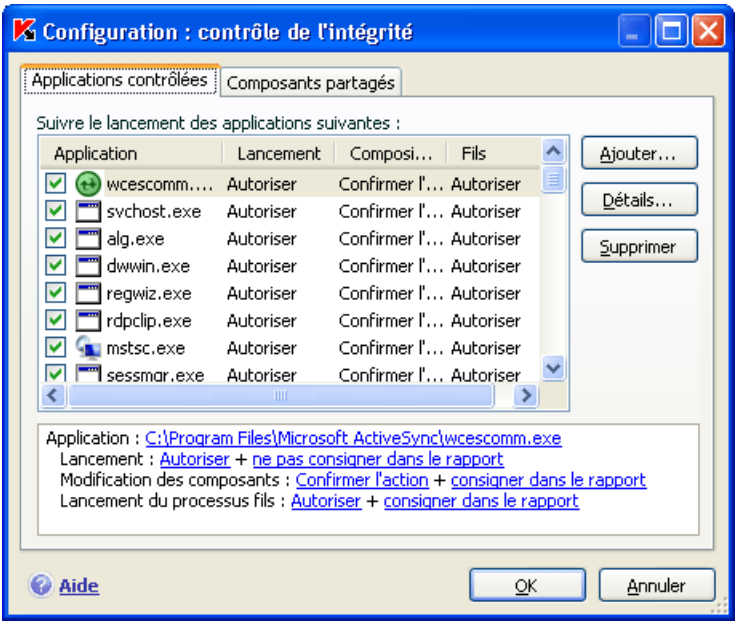


Illustration 38. Configuration du contrôle de l'intégrité de l'application

Pour consulter la liste des modules de l'application sélectionnée, cliquez sur **Détails**. La fenêtre **Configuration: module de l'application** reprend la liste des modules utilisés lors du lancement de l'application contrôlée. Vous pouvez modifier cette liste à l'aide des boutons **Ajouter** et **Supprimer** situés dans la partie droite de la fenêtre.

Vous pouvez également autoriser ou interdire le chargement d'un module quelconque par une application contrôlée. Une règle d'autorisation est créée par défaut pour chaque module. Pour modifier l'action, sélectionnez le module dans la liste puis cliquer sur le bouton **Modifier**. Définissez l'action requise dans la fenêtre qui s'ouvre.

N'oubliez pas qu'au moment du premier lancement de l'application contrôlée après l'installation de Kaspersky Anti-Virus, un apprentissage se déroule jusqu'au moment où vous quittez l'application. La liste des modules utilisés par l'application est constituée au cours de cet apprentissage. Les règles de contrôle de l'intégrité seront appliquées aux lancements suivants de l'application.

10.2.2. Création de la liste des composants partagés

Kaspersky Anti-Virus prévoit une liste de composants partagés qui peuvent être chargés dans toutes les applications contrôlées. Cette liste est reprise sur l'onglet **Composants partagés** (cf. ill. 39). La liste contient les modules utilisés par Kaspersky Anti-Virus, les composants qui possèdent la signature de Microsoft Corporation et les composants ajoutés par l'utilisateur.

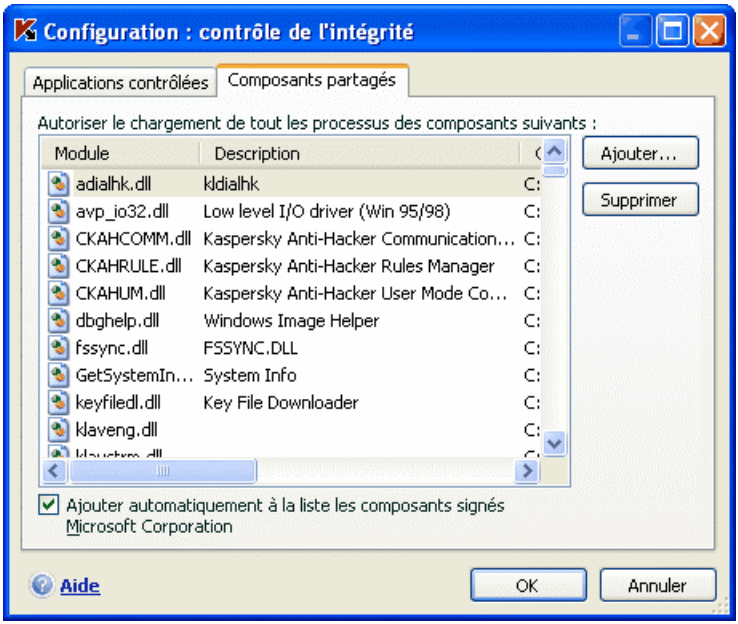


Illustration 39. Configuration de la liste des modules de confiance

Vous pouvez installer différents programmes sur votre ordinateur et si vous souhaitez que les modules accompagnés de la signature de Microsoft Corporation soient ajoutés automatiquement à la liste des modules de confiance, cochez la case ☑ **Ajouter automatiquement à la liste les composants signés Microsoft Corporation**. Dans ce cas, si l'application contrôlée tente de charger un module possédant la signature de Microsoft Corporation, le chargement de ce module sera accepté automatiquement et le module sera placé dans la liste des composants partagés.

Pour ajouter des modules de confiance, cliquez sur **Ajouter** et sélectionnez les modules souhaités dans la boîte de dialogue traditionnelle de sélection des fichiers.

10.3. Contrôle des modifications de la base de registres système

La modification de la base de registres système du système d'exploitation de votre ordinateur est un des buts poursuivis par de nombreux programmes malveillants. Il peut s'agir de jokewares inoffensifs ou d'autres programmes plus dangereux qui représentent une véritable menace pour votre ordinateur.

Ainsi, un programme malveillant pourrait s'inscrire dans la clé de registre responsable du lancement automatique des applications. Directement après le démarrage du système d'exploitation de l'ordinateur, le programme malveillant sera ouvert automatiquement.

La défense proactive contrôle les modifications des objets de la base de registres système. Pour enclencher ce module, cochez la case **Activer la surveillance du Registre**.

Pour passer à la configuration du contrôle de la base de registres système :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le composant **Défense proactive** dans la rubrique **Protection**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Surveillance de la base de registre système** (cf. ill. 35).

La liste des règles qui régissent la manipulation des objets du registre a déjà été dressée par les experts de Kaspersky Lab et elle est reprise dans le fichier d'installation. Les opérations sur les objets du registre sont réparties en groupes logiques tels que *System security*, *Internet Security*, etc. Chacun de ces groupes contient les objets de la base de registres système et les règles de manipulation de celles-ci. Cette liste est actualisée en même temps que la mise à jour du logiciel.

La liste complète des règles est prise sur l'onglet **Configuration : surveillance du Registre** (cf. ill. 40).

Chaque groupe possède une priorité d'exécution que vous pouvez augmenter ou diminuer à l'aide des boutons **Monter** et **Descendre**. Plus le groupe est haut dans la liste, plus sa priorité est importante. Si un même objet est repris dans plusieurs groupes, la première règle qui sera appliquée à l'objet sera la règle du groupe dont la priorité est la plus élevée.

Utilisez l'une des méthodes suivantes pour annuler l'utilisation d'un groupe de règles quelconque :

- Désélectionnez la case ☑ en regard du nom du groupe. Dans ce cas, le groupe de règles demeure dans la liste, mais il n'est plus utilisé.
- Supprimez le groupe de règles de la liste. Il est déconseillé de supprimer les groupes composés par les experts de Kaspersky Lab car ils contiennent les listes des objets de la base de registres système qui sont le plus souvent utilisés par les programmes malveillants.

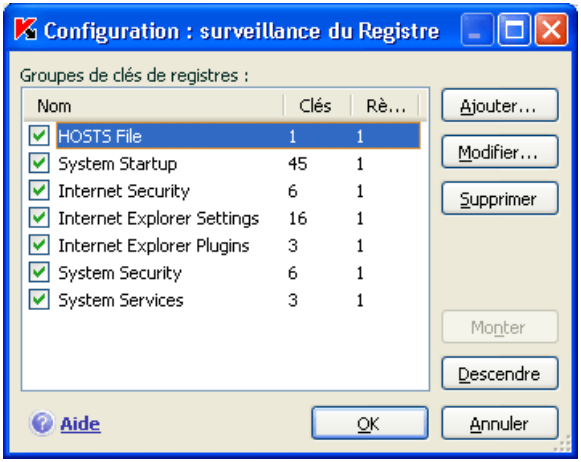


Illustration 40. Groupe de clés de la base de registres système contrôlées

Vous pouvez créer vos propres groupes d'objets contrôlés. Pour ce faire, cliquez sur **Ajouter** dans la fenêtre du groupe d'objets.

Exécutez les actions suivantes dans la fenêtre ouverte :

1. Saisissez le nom du nouveau groupe d'objets de la base de registres système dans le champ **Nom**.
2. Constituez la liste des objets (cf. point 10.3.1, p. 136) de la base de registres système qui feront partie du groupe contrôlé dans l'onglet **Clés**. Il peut s'agir d'un seul objet ou de plusieurs.
3. Sur l'onglet **Règles**, créez une règle (cf. point 10.3.2, p. 137) pour les objets du registre. Vous pouvez créer plusieurs règles de traitement et définir leur priorité.

10.3.1. Sélection des objets de registre pour la création de règles

Le groupe d'objets créé doit reprendre au moins un objet de la base de registres système. La liste des objets pour la règle est rédigée sur l'onglet **Clés**.

Afin d'ajouter un objet de la base de registres système :

1. Cliquez sur **Ajouter** dans la boîte de dialogue **Modification du groupe** (cf. ill. 41).
2. Dans la boîte de dialogue qui s'ouvre, sélectionnez l 'objet ou le groupe d'objets de la base de registres système pour laquelle vous voulez créer une règle de contrôle.

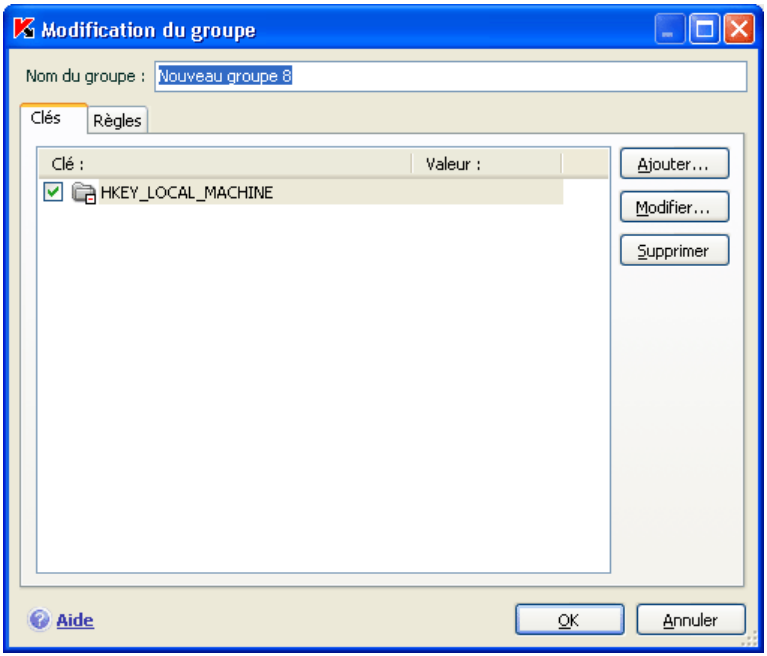


Illustration 41. Ajout d'une clé à contrôler

3. Indiquez dans le champ **Valeur** la valeur de l'objet ou le masque du groupe d'objets auquel vous souhaitez appliquer la règle.

4. Cochez la case **Clés intégrées comprises** afin que la règle s'applique à toutes les clés intégrées de la clé de la base de registres système sélectionnée pour l'objet.

L'utilisation simultanée d'un masque avec les caractères * ou ? et de l'option **Clés intégrées comprises** s'impose uniquement si ces caractères figurent dans le nom de la clé.

Si un groupe d'objets dans le registre a été sélectionné à l'aide d'un masque et qu'une règle concrète a été définie, celle-ci sera appliquée à la valeur indiquée pour n'importe quelle clé du groupe sélectionné.

10.3.2. Création d'une règle de contrôle des clés du registre

La règle de contrôle des clés de la base de registres système est basée sur la définition de :

- l'application à laquelle la règle sera appliquée si elle adresse une requête la base de registres système;
- des réactions du programme en cas de tentative de la part de l'application d'exécuter une opération quelconque avec les objets de la base de registres système.

Ainsi, afin de créer une règle pour les objets de la base de registres système sélectionnées :

1. Cliquez sur **Créer** dans l'onglet **Règles**. La règle générale sera ajoutée en tête de liste (cf. ill. 42).
2. Sélectionnez la règle dans la liste et définissez-en les paramètres dans la partie inférieure de l'onglet :
   - Précisez l'application.

     Par défaut, une règle est créée pour chaque application. Afin que la règle soit appliquée à un programme concret, cliquez avec le bouton gauche de la souris sur le lien Toute. Il devient Sélectionnée. Cliquez ensuite sur le lien Indiquez l'application. Cette action entraîne l'ouverture d'un menu contextuel. Le point **Parcourir** ouvre la boîte de dialogue traditionnelle pour la sélection des fichiers. Vous pouvez également cliquez sur le point **Applications** afin d'afficher la liste des applications ouvertes à ce moment et de sélectionner celle que vous voulez.

- Définissez la réaction de la défense proactive lorsque l'application sélectionnée tente de lire, de modifier ou de supprimer les objets de la base de registres système.

  Vous pouvez sélectionner une des actions suivantes en guise de réaction : Autoriser, Confirmer l'action et Interdire. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée.

- Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, utilisez le lien consigner dans le rapport / ne pas consigner dans le rapport.

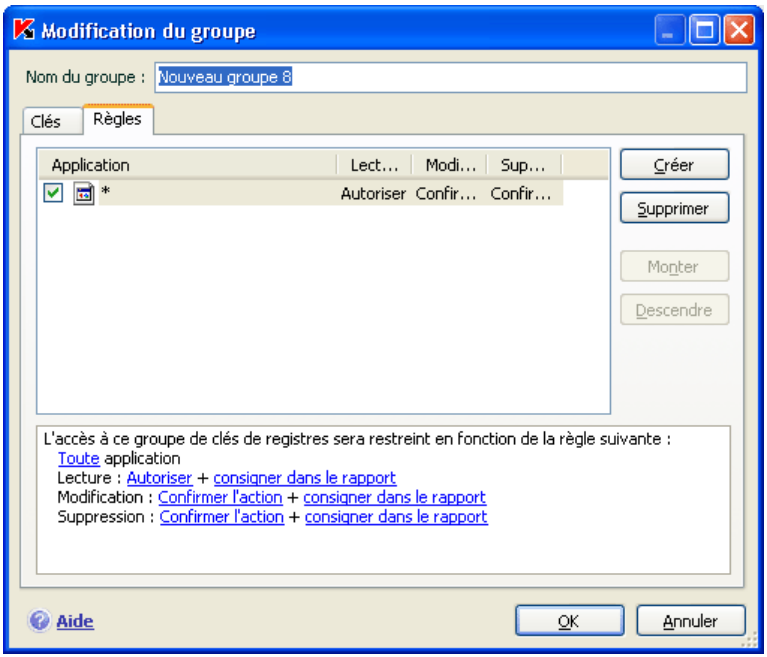


Illustration 42. Création d'une règle de contrôle des clés de la base de registre système

Vous pouvez créer quelques règles et définir la priorité de leur application à l'aide des boutons **Monter** et **Descendre**. Plus la règle est placée en haut de la liste, plus sa priorité est élevée.

Il est possible également de créer une règle d'autorisation pour l'objet de la base de registres système au départ de la notification sur la tentative d'exécution d'une opération sur l'objet. Pour ce faire, cliquez sur Créer une règle d'autorisation et dans la boîte de dialogue qui s'ouvre, précisez l'objet de la base de registres système auquel la règle s'appliquera.

CHAPITRE 11. RECHERCHE DE VIRUS SUR L'ORDINATEUR

L'un des principaux composants de la protection antivirus de l'ordinateur est la recherche de virus dans les secteurs indiqués par l'utilisateur. Kaspersky Anti-Virus 7.0 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 les autres composants de la protection en temps réel.

Kaspersky Anti-Virus 7.0 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.

Rootkit

Recherche la présence éventuelle de Rootkit qui dissimulent les programmes malveillants dans le système d'exploitation. Ces utilitaires s'insèrent dans le système en dissimulant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité.

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres (cf. point 11.4, p. 143) et même programmer le lancement de la tâche (cf. point 6.7, p. 68).

Il est possible également de créer des tâches personnalisées (cf. point 11.3, p. 142) de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des boîtes aux lettres de messagerie une fois par semaine ou une tâche pour la recherche de la présence éventuelle de virus dans le répertoire **Mes documents**.

De plus, vous pouvez rechercher la présence éventuelle de virus dans n'importe quel objet (exemple : un des disques durs sur lequel se trouve les programmes et les jeux, les bases de messagerie ramenées du travail, les archives reçues par courrier électronique, etc.) 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 traditionnelles (ex. : dans la fenêtre de l'**Assistant** ou au départ du **Bureau**, etc.).

La section **Analyse** 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.

Vous pouvez créer un disque de démarrage (cf. point 15.4, p. 190) qui permet de rétablir le système d'exploitation après une attaque de virus qui aurait endommager les fichiers du système et qui empêcherait le démarrage initial. Pour ce faire, cliquez sur le lien Créer un CD de Secours Bootable.

11.1. 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 6.7, p. 68).

Afin de lancer la tâche de recherche de virus manuellement :

Sélectionnez le nom de la tâche dans la section **Analyse** de la fenêtre principale puis cliquez sur le lien Lancer l'analyse.

Les tâches en cours d'exécution sont reprises dans le menu contextuel qui s'ouvre lorsque vous cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows.

Pour suspendre la tâche de recherche de virus :

Sélectionnez le nom de la tâche dans la section **Analyse** de la fenêtre principale puis cliquez sur le lien Pause. L'analyse sera suspendue jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon l'horaire. Pour lancer l'analyse manuelle, cliquez sur le lien Rafraîchir.

Pour suspendre l'exécution de la tâche :

Sélectionnez le nom de la tâche dans la section **Analyse** de la fenêtre principale puis cliquez sur le lien Stop. 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.

11.2. 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 **Analyse** dans la fenêtre principale du programme. La liste des objets sera reprise dans la partie droite de la fenêtre (cf. ill. 43).

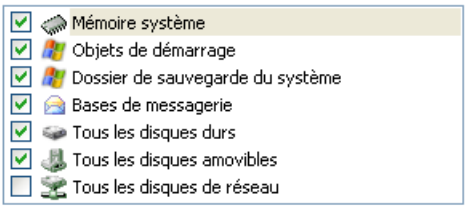


Illustration 43. Liste des objets à analyser

Les listes 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, de nouvelles zones d'analyse ont été ajoutées telles que les boîtes aux lettres de messagerie de l'utilisateur, la mémoire système, les objets de démarrage, le dossier de sauvegarde du système d'exploitation et les objets du dossier de sauvegarde de Kaspersky Anti-Virus.

De plus, lors de l'ajout d'un répertoire contenant des objets intégrés, vous pouvez modifier le niveau de suivi. Pour ce faire, utilisez le point correspondant du menu contextuel. Pour ce faire, sélectionnez l'objet dans la liste des objets à

analyser, ouvrez le menu contextuel et cliquez sur l'option **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 le lien Lancer l'analyse.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc. (cf. ill. 44). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

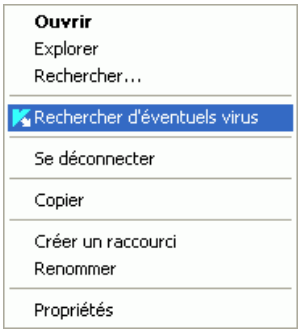


Illustration 44. Analyse d'un objet au départ du menu contextuel de Microsoft Windows

11.3. 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 **Analyse** de la fenêtre principale du logiciel, sélectionnez la tâche dont les paramètres vous conviennent le mieux.
2. Ouvrez le menu contextuel et sélectionnez **Enregistrer sous** ou cliquez sur le lien Nouvelle tâche d'analyse.

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 **Analyse** de la fenêtre principale du logiciel.

Attention !

Le nombre de tâches que peut créer l'utilisateur 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 11.2, p. 141), indiquer les paramètres d'exécution de la tâche (cf. point 11.4, p. 143) et, le cas échéant, programmer (cf. point 6.7, p. 68)le lancement automatique.

Afin de renommer une tâche créée :

sélectionnez la tâche dans la section **Analyse** de la fenêtre principale puis, cliquez sur le lien 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 **Analyse** sera modifié.

Pour supprimer une tâche créée :

sélectionnez la tâche dans la section **Analyse** de la fenêtre principale du logiciel puis, cliquez sur le lien 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 **Analyse**.

Attention !

Vous pouvez uniquement renommer les tâches que vous avez créées.

11.4. 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, sélectionnez le nom de la tâche dans la rubrique **Analyse** puis, cliquez sur Configuration.

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 11.4.1, p. 144);
- passer à la configuration détaillée du niveau :
    - indiquer les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 11.4.2, p. 145);
    - configurer le lancement des tâches au nom d'un autre compte utilisateur (cf. point 0, p. 66);
    - définir les paramètres complémentaires de l'analyse (cf. point 11.4.3, p. 149)
    - activer la recherche de Rootkit (cf. point 11.4.4, p. 151) et utiliser les méthodes d'analyse heuristique (cf. point 11.4.5, p. 152);
- restaurer les paramètres d'analyse utilisés par défaut (cf. point 11.4.6, p. 153);
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou potentiellement infecté (cf. point 11.4.7, p. 153);
- programmer le lancement automatique de la tâche (cf. point 6.7, p. 68).

De plus, vous pouvez définir des paramètres uniques de lancement pour toutes les tâches (cf. point 11.4.8, p. 155).

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

11.4.1. Sélection du niveau de protection

Chaque tâche liée à la recherche de virus analyse les objets selon un des trois niveaux suivants (cf. ill. 45):

Protection maximale 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 **Protection maximale**, à l'exception des fichiers au format de courrier électronique.

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

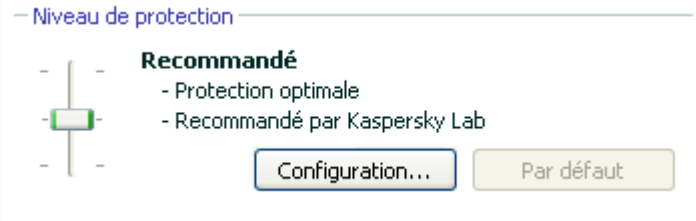


Illustration 45. Sélection du niveau de protection pour la recherche de virus

Par défaut, l'analyse des fichiers 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 de protection devient **Autre**.

Pour modifier les paramètres du niveau de protection actuel :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche d'analyse dans la rubrique **Analyse**.
2. Cliquez sur le bouton **Configuration** dans le groupe **Niveau de protection** (cf. ill. 45).
3. Dans la fenêtre qui s'ouvre, modifiez les paramètres de protection des fichiers puis cliquez sur **OK**.

11.4.2. 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. ill. 46). 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.

  > Informations.
  >
  > Il existe divers formats de fichiers pour laquelle la probabilité d'une infection par un code malveillant suivie de son activation est très faible. Les fichiers texte en sont un exemple.
  >
  > Et il existe d'autres formats qui contiennent ou peuvent contenir un code exécutable. C'est le cas par exemple des fichiers au format *exe*, *dll* ou *doc*. Le risque d'infection par un code malveillant et d'activation est très élevé pour ces fichiers.

  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.

- **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 le lien extension, vous pourrez découvrir à liste des extensions des fichiers qui seront soumis à l'analyse dans ce cas (cf. point A.1, p. 237).

> 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 renommé 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)**, 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.

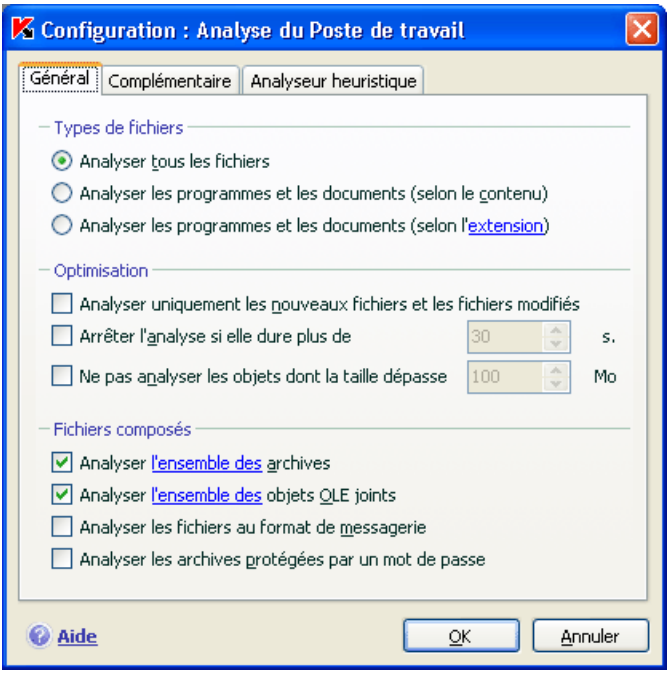


Illustration 46. Configuration des paramètres de l'analyse

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

- **Arrêter l'analyse si elle 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 les objets dont la taille dépasse … 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 après le lancement du traitement des objets découverts pendant l'analyse. 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. Lorsque la case est sélectionnée, Kaspersky Anti-Virus décompose le fichier au format de messagerie et recherche la présence éventuelle de virus dans chacun des composants du message (corps du message, pièce jointe). Si la case n'est pas sélectionnée, le fichier au format de messagerie est traité comme un fichier simple.

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.

11.4.3. 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. ill. 47):

- **Utiliser 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 bases de l'application, de la date de l'analyse précédente et des modifications des paramètres d'analyse.

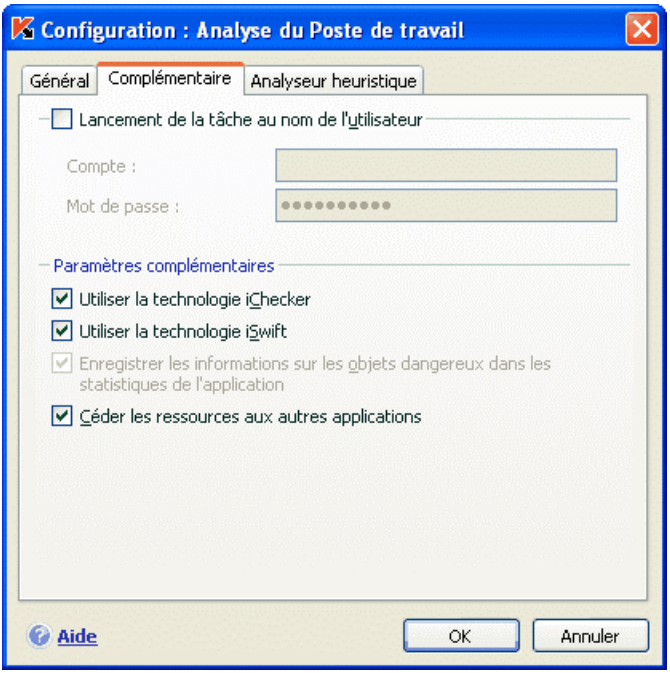


Illustration 47. Configuration complémentaire de l'analyse

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 de l'application, l'archive sera analysée

à nouveau.
La technologie iChecker™ a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et 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).

Utiliser la technologie iSwift : Cette technologie est une 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.

Consigner les informations relatives aux objets dangereux dans les statistiques de l'application : enregistre les informations relatives à la découverte d'objets dangereux dans les statistiques générales de l'application et affiche la liste des menaces dangereuses dans l'onglet **Infectés** de la fenêtre du rapport (cf. point 15.3.2, p. 185). Si la case n'est pas sélectionnée, les informations relatives aux objets dangereux ne seront pas reprises dans le rapport et, par conséquent, il sera impossible de traiter ces objets.

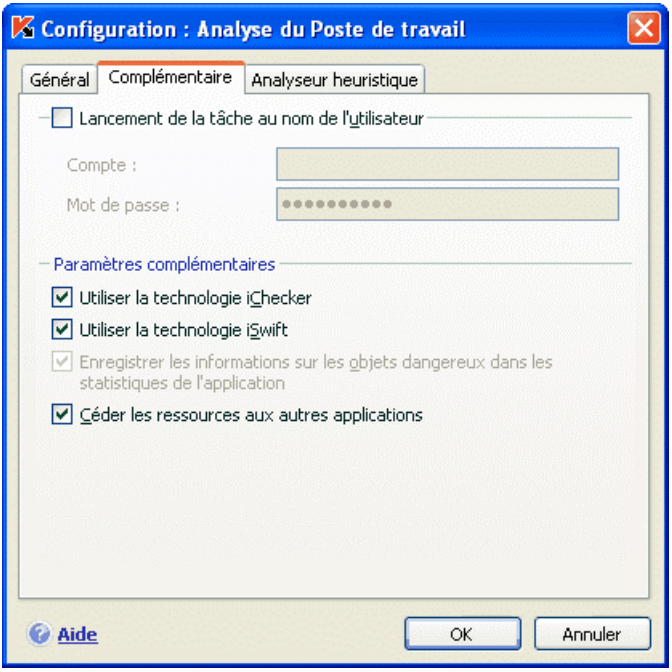


Illustration 48. Configuration complémentaire de l'analyse

Céder les ressources aux autres applications : suspend l'exécution de la tâche de recherche de virus si les ressources du processeurs sont utilisées par d'autres applications.

11.4.4. Recherche de Rootkit

Un outil de dissimulation d'activité est un utilitaire qui permet de dissimuler la présence de programmes malveillants dans le système d'exploitation. Ces utilitaires s'insèrent dans le système en dissimulant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité.

La recherche de Rootkit peut être exécutée par n'importe quelle tâche de recherche de virus (pour autant que cette possibilité ait été activée dans les paramètres de la tâche en question), toutefois les experts de Kaspersky Lab ont élaboré et configuré de manière optimale une tâche distincte de recherche des programmes malveillants de ce type.

Pour activer la recherche de Rootkit, cochez la case **Activer la recherche** dans le groupe **Recherche de Rootkit**. Lorsque la recherche est activée, vous pouvez définir le niveau de découverte de ces outils en cochant la case **Analyse la recherche étendue**. Dans ce cas, le système procédera à une recherche minutieuse des programmes de ce type par le biais de l'analyse d'une grande quantité d'objets de différents types. Les cases sont désélectionnées par défaut car l'activation de ce mode requiert des ressources considérables pour le système d'exploitation.

Pour configurer la recherche de Rootkit :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans le groupe **Analyse**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection** (cf. ill. 45) et dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Analyseur heuristique** (cf. ill. 49).

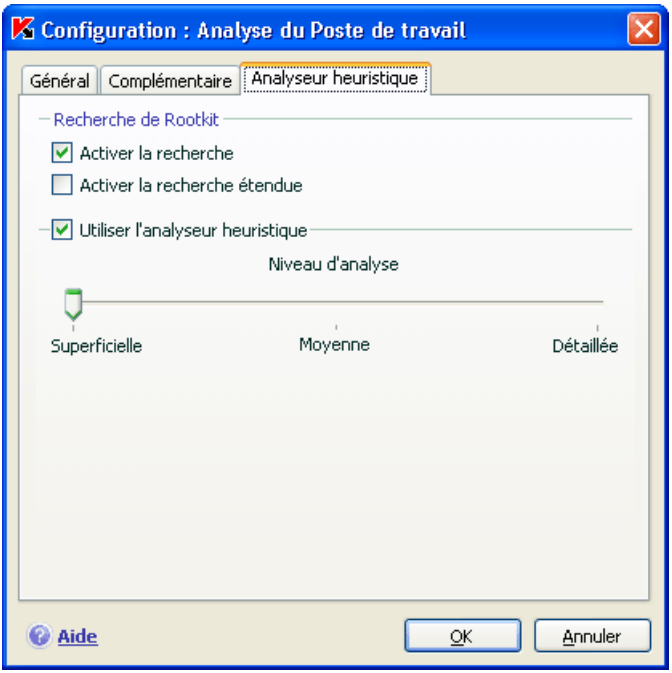


Illustration 49. Configuration des paramètres de recherche de virus et d'utilisation des méthodes d'heuristique

11.4.5. Utilisation des méthodes d'analyse heuristique

Les méthodes d'analyse heuristique sont utilisées par plusieurs composants de la protection en temps réel ainsi que dans les tâches de recherche des virus (pour de plus amples informations, consultez le point 7.2.4 à la page. 93).

Vous pouvez activer/désactiver l'utilisation des méthodes heuristiques d'identification des nouvelles menaces sur l'onglet **Analyseur heuristique** (cf. ill. 49) dans le cadre du fonctionnement de la recherche de virus. Pour ce faire, exécutez les actions suivantes :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Analyse**.
2. Cliquez sur le bouton **Configuration** dans le bloc **Niveau de protection**. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Analyseur heuristique**.

Pour utiliser les méthodes heuristiques, cochez la case **Utiliser l'analyseur heuristique**. Vous pouvez également sélectionner le niveau de détail de l'analyse. Pour ce faire, déplacez le curseur sur une des trois positions : **Superficielle**, **Moyenne** ou **Détaillée**.

11.4.6. 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. Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Analyse**.
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection** (cf. ill. 45).

11.4.7. 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 potentiellement infectés sont placés en quarantaine.

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

Ouvrez la fenêtre de configuration de l'application et sélectionnez le nom de la tâche dans la rubrique **Analyse**. Toutes les actions possibles sont reprises dans le groupe correspondant (cf. ill. 50).

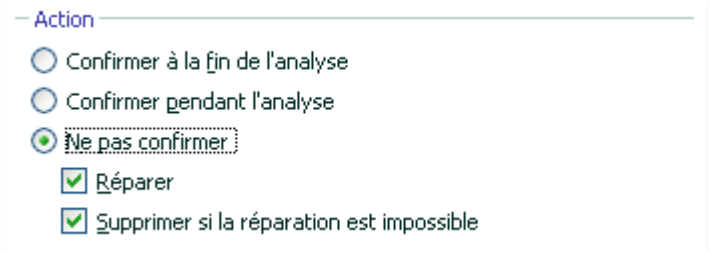


Illustration 50. Sélection de l'action à réaliser sur l'objet dangereux

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. Une fenêtre contenant les statistiques avec la liste des objets découverts apparaîtra à la fin de l'analyse et vous pourrez choisir le traitement à réaliser.
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 avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la tentative échoue, l'objet reçoit le statut *potentiellement infecté* et est placé en quarantaine (cf. point 15.1, p. 175). Les informations relatives à cette situation sont consignées dans le rapport (cf. point 15.3, p. 182). Il est possible de tenter de réparer cet objet ultérieurement.
Ne pas confirmer **Réparer** **Supprimer si la réparation est impossible**	Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la réparation de l'objet échoue, il sera supprimé.
Ne pas confirmer **Réparer** **Supprimer**	Le programme supprimera automatiquement l'objet.

Quel que soit le statut de l'objet (infecté ou potentiellement infecté), Kaspersky Anti-Virus crée une copie de sauvegarde avant de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde (cf. point 15.2, p. 179)au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

11.4.8. 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. Ouvrez la fenêtre de configuration et sélectionnez la section **Analyse**.
2. Définissez les paramètres de l'analyse : sélectionnez le niveau de protection (cf. point 11.4.1, p. 144), réalisez la configuration

complémentaire du niveau et indiquez l'action qui sera réalisée sur les objets (cf. point 11.4.7, p. 153).

3. Afin d'appliquer les paramètres définis à toutes les tâches, cliquez sur **Appliquer** dans le bloc **Paramètres des autres tâches**. Confirmez les paramètres uniques dans la boîte de dialogue de confirmation.

CHAPITRE 12. ESSAI DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

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.

12.1. 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 l'identifie en tant que **virus** et exécute l'action définie 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 de l'application 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 bases 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 a 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.

12.2. Vérification de l'Antivirus Fichiers

Afin de vérifier le fonctionnement de l'Antivirus Fichiers :

1. 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 ☑ **Consigner les événements non critiques** dans la section **Journaux** de la fenêtre de configuration des rapports (cf. point 15.3.1, p. 184).
2. Créez un répertoire sur le disque, copiez-y le fichier d'essai téléchargé depuis le site officiel de l'organisation (cf. point 12.1, p. 157) ainsi que les modifications du virus d'essai.

Antivirus Fichiers intercepte la requête adressée au fichier, il l'analyse et signale la découverte d'un objet dangereux :

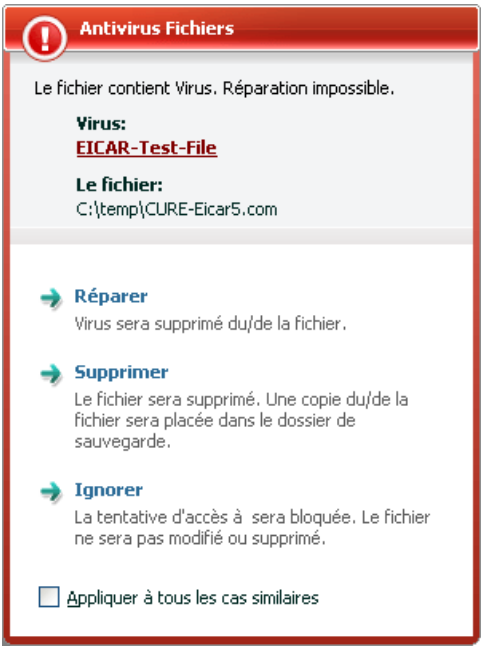


Illustration 51. Découverte d'un objet dangereux

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.

12.3. 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 12.1, p. 157) ainsi que les versions modifiées du virus d'essai.
2. Créez une nouvelle tâche de recherche de virus (cf. point 11.3, p. 142) et en guise d'objet à analyser, sélectionnez le dossier contenant la sélection de virus d'essais (cf. point 12.1, p. 157).

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 **Consigner les événements non critiques** dans la section **Rapports** de la fenêtre de configuration de l'application (cf. point 15.3.1, p. 184).
4. Exécutez la tâche (cf. point 11.1, p. 140) 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 :

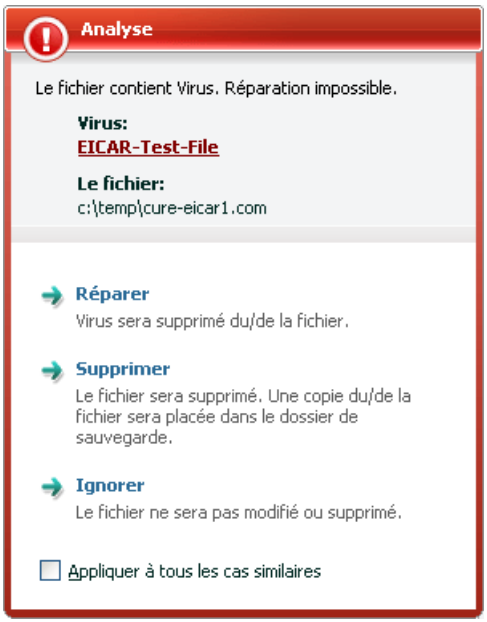


Illustration 52. Découverte d'un objet dangereux

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 13. MISE A JOUR DU LOGICIEL

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

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

- **Bases Antivirus et pilotes de réseau**

  La protection de vos données est réalisée à l'aide des bases de données contenant les signatures de menace. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces bases sont enrichies toutes les heures des définitions des nouvelles menaces et des moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

  Outre la mise à jour des bases Antivirus, le système actualise également les pilotes de réseaux qui permettent aux composants de la protection d'intercepter le trafic de réseau.

  Les versions antérieures des logiciels antivirus de Kaspersky Lab prenaient en charge l'utilisation de différentes bases : 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 adéquates. Nos logiciels utilisent désormais des bases qui offrent une protection non seulement contre divers types de programmes malveillants et d'objets présentant un risque potentiel.

- **Modules logiciels**

  En plus des bases de l'application, 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.

Pour garantir la réussite des mises à jour depuis les serveurs, votre ordinateur doit absolument être connecté à Internet. Si la connexion à Internet s'opère via un serveur proxy, il faudra configurer les paramètres de connexion (cf. point 15.7, p. 198).

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 495 797 87 00, au +7 (495) 645-79-39 ou +7 (495) 956-00-00 pour obtenir l'adresse d'un partenaire de Kaspersky Lab qui pourra vous donner les mises à jour sur disquette ou sur CD/DVD-ROM dans un fichier 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, l'application 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 bases installées sur votre ordinateur sont comparés à ceux de la source des mises à jour. Si les bases et les composants installés sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les bases et les modules diffèrent, la partie manquante de la mise à jour sera installée. La copie des bases et des modules complets n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

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

La possibilité d'annuler (cf. point 13.2, p. 164) une mise à jour est indispensable, par exemple si les bases que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

Parallèlement à la mise à jour, vous pouvez copier les mises à jour obtenues dans une source locale (cf. point 13.3.3, p. 170). Ce service permet d'actualiser les bases antivirus et les modules utilisés par les applications de la version 7.0 sur les ordinateurs du réseau en réduisant le trafic Internet.

13.1. 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 13.3.1, p. 165).

Vous pouvez lancer la mise à jour du logiciel depuis :

- le menu contextuel (cf. point 4.2, p. 44);
- la fenêtre principale du logiciel (cf. point 4.3, p. 46).

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 zone de notification de la barre des tâches de Microsoft Windows.
2. Sélectionnez le point **Mise à jour**.

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

1. Ouvrez la fenêtre principale de l'application et sélectionnez le composant **Mise à jour**.
2. Cliquez sur le lien Mettre à jour.

Le processus de mise à jour du logiciel sera illustré dans une fenêtre spéciale. Pour obtenir de plus amples informations sur le processus de mise à jour, cliquez sur le lien Détail. Cette action entraîne un rapport détaillé sur la mise à jour. Vous pouvez fermer la fenêtre du rapport. Pour ce faire, cliquez sur le bouton **Fermer**. La mise à jour se poursuivra.

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 13.3.3, p. 170).

13.2. 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 bases et des modules de l'application avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau la version antérieure des bases après une mise à jour ratée.

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

1. Ouvrez la fenêtre principale de l'application et sélectionnez le composant **Mise à jour**.
2. Cliquez sur le lien Revenir à la mise à jour précédente.

13.3. 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 13.3.1, p. 165);
- le mode de lancement de la mise à jour du logiciel et les objets actualisés (cf. point 13.3.2, p. 168);
- la fréquence de lancement des mises à jour lorsque le lancement automatique est programmé (cf. point 6.7, p. 68);
- le nom du compte utilisateur sous lequel la mise à jour sera réalisée (cf. point 0, p.66);
- la nécessité de copier les mises à jour reçues dans un répertoire local (cf. 13.3.3, p. 170);
- les actions à réaliser après la mise à jour du logiciel (cf. point 13.3.4, p. 171).

Tous ces paramètres sont abordés en détails ci-après.

13.3.1. Sélection de la source des mises à jour

La source des mises à jour est une ressource quelconque qui contient les mises à jour des signatures des menaces et des modules logiciels de Kaspersky Anti-Virus. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Les *serveurs des mises à jour de Kaspersky Lab* constituent la source principale de mise à jour. Il s'agit de sites Internet spéciaux prévus pour la diffusion des bases et des modules logiciels pour tous les produits de Kaspersky Lab.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 495 797 87 00, au +7 (495) 645-79-39 ou au +7 (495) 956-00-00 pour obtenir l'adresse

d'un partenaire de Kaspersky Lab qui pourra vous donner les mises à jour sur disquette ou sur CD/DVD-ROM dans un fichier 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 HTTP ou dans un répertoire local ou de réseau.

La sélection de la source de mises à jour s'opère dans l'onglet **Source de mises à jour** (cf. ill. 53).

Par défaut, la liste contient uniquement 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 des mises 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://user:password@server.

Attention !

Si en guise de source de la mise à jour vous avez sélectionné une ressource située hors de l'intranet, vous devrez être connecté à Internet pour télécharger 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 des mises à jour** ou saisissez son chemin d'accès complet dans le champ **Source**.

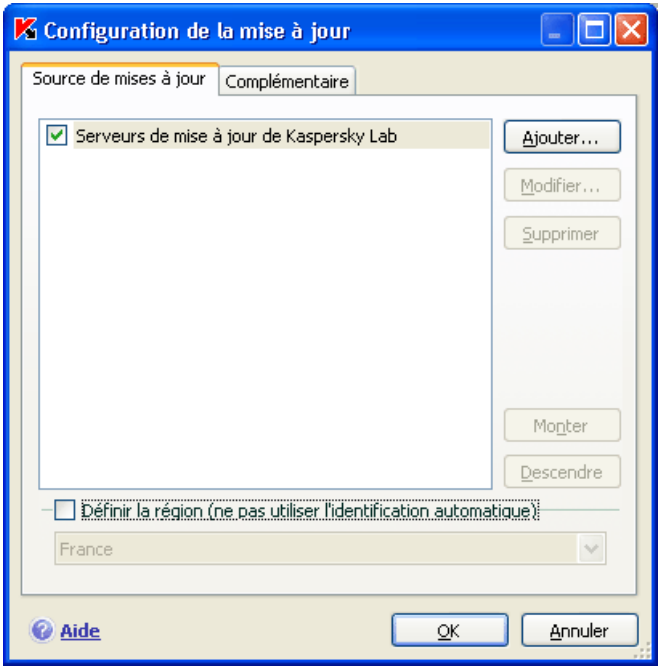


Illustration 53. Sélection de la source des mises à jour

Kaspersky Anti-Virus ajoute la nouvelle source de mises 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 mises 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 sont les seules 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.

13.3.2. 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 objet de la mise à jour (cf. ill. 54) désignent les objets qui seront actualisés :

- Les bases de l'application ;
- Les pilotes de réseau qui assure l'interception du trafic de réseau par les composants de la protection ;
- Les modules de l'application ;

Les bases de l'application et les pilotes de réseau sont actualisés à chaque fois tandis que les modules de l'application sont actualisées uniquement lorsque le mode correspondant est activé.

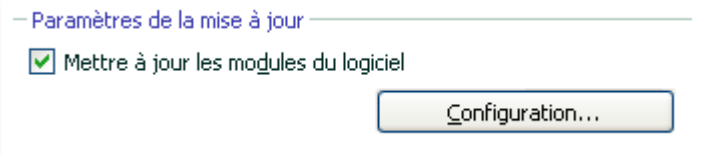


Illustration 54. Sélection des objets de la mise à jour

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

Ouvrez la fenêtre de configuration de l'application, sélectionnez le composant **Mise à jour** et cochez la case ☑ **Mettre à jour les modules du logiciel**.

Si à ce moment la source ne contient pas la mise à jour des modules de l'application, celle-ci recevra les mises à jour indispensables et les appliquera après le redémarrage de l'ordinateur. Les mises à jour récupérées des modules ne seront pas installées avant le redémarrage.

Si la mise à jour suivante de l'application a lieu avant le redémarrage de l'ordinateur et l'installation des mises à jour des modules récupérées antérieurement, seule la mise à jour des bases de l'application sera réalisée.

Le mode de mise à jour du logiciel (cf. ill. 55) désigne la manière dont la mise à jour sera lancée. Choisissez l'un des modes suivants dans le groupe **Mode d'exécution** :

Automatique. Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source (cf. point 13.3.1, p. 165). Lorsque Kaspersky Anti-Virus découvre de nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode de mise à jour est activé par défaut.

Si 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 bases et des modules de l'application, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

Illustration 55. Sélection du mode de lancement de la mise à jour

Tous les 1 jour(s). 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 chaque à jour. 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 6.7 à la page 68).

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.

13.3.3. Copie des mises à jour

Si les ordinateurs sont regroupés au sein d'un réseau local, il n'est pas nécessaire de télécharger les mises à jour et de les installer sur chaque ordinateur car cela augmenterait le trafic de réseau. Vous pouvez utiliser le service des copies des mises à jour qui contribue à la réduction du trafic dans la mesure où la mise à jour est organisée de la manière suivante :

1. Un des ordinateurs du réseau obtient les mises à jour pour l'application 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.

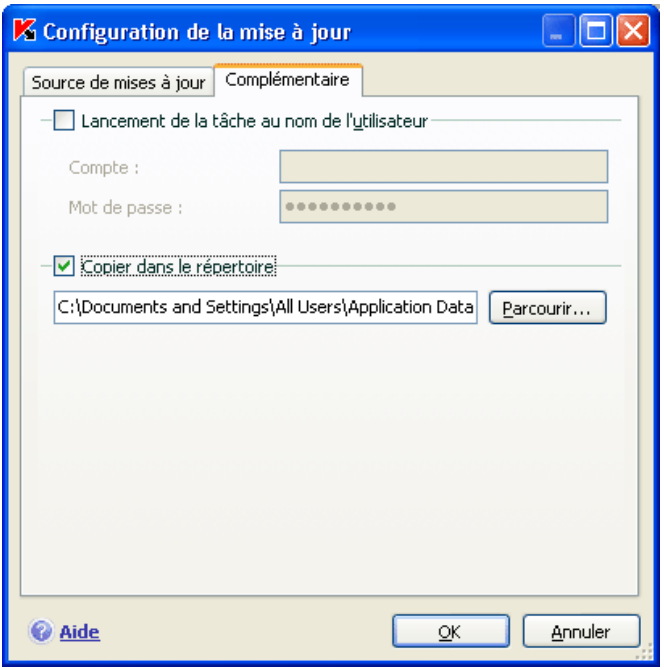


Illustration 56. Configuration du service de copie des mises à jour

Pour activer la copie des mises à jour, cochez la case **Copier dans le répertoire** de l'onglet **Complémentaire** (cf. ill. 56) 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.

N'oubliez pas que Kaspersky Anti-Virus 7.0 reçoit des serveurs de Kaspersky Lab uniquement les paquets indispensables à sa propre mises à jour.

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.

13.3.4. Actions exécutées après la mise à jour du logiciel

Chaque mise à jour des bases de l'application 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 15.1, p. 175). Il se peut que la version actualisée des bases de Kaspersky Anti-Virus puisse reconnaître et neutraliser le danger.

Par défaut, le logiciel analyse les objets en quarantaine après chaque mise à jour. 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 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 11, p. 139). Il est conseillé de configurer le lancement automatique de cette tâche après chaque mise à jour des bases (cf. point 6.7, p. 68).

CHAPITRE 14. ADMINISTRATION DES LICENCES

Kaspersky Anti-Virus fonctionne grâce à une *licence* que vous pourrez trouver sous la forme d'un code d'activation ou d'une clé fichier. Cette licence est octroyée sur la base de l'achat de l'application et vous donne le droit d'utiliser celui-ci dès le jour de l'acquisition et de l'activation de la licence.

Sans la 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 bases de l'application. Vous pourrez toujours analyser votre ordinateur à l'aide de la recherche de virus et utiliser les composants de la protection, mais uniquement à l'aide des bases 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 votre ordinateur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la validité de la licence de l'application. Kaspersky Anti-Virus vous préviendra en temps opportuns de la proximité de la fin de validité de la licence. Le message de circonstance sera affiché à chaque lancement de l'application.

Les informations relatives à la licence installées sont reprises dans la rubrique **Activation** (cf. ill. 57) de la fenêtre principale de l'application. Le bloc **Numéro(s) de série** indique le numéro de licence, son type (commerciale, évaluation, test bêta), le nombre maximum d'ordinateurs sur lesquels cette licence peut être utilisée, la fin de validité de la licence et le nombre de jour restant avant cette date. Pour consulter les informations complémentaires, cliquez sur le lien Consulter les détails relatifs aux licences.

Pour lire les termes du contrat de licence pour l'utilisation de l'application, cliquez sur le lien Lire le contrat de licence. Pour supprimer une licence de la liste, cliquez sur Supprimer la licence.

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

1. Achetez une nouvelle licence. Pour ce faire, cliquez sur le lien Acheter une nouvelle licence (si l'application n'a pas été activée) ou sur Renou-

veler la licence. Dans la page Web qui s'ouvre, vous pourrez saisir toutes les informations relatives à l'achat de la licence via la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la société.

En cas d'achat via la boutique en ligne, vous recevrez, après confirmation du paiement, le code d'activation de l'application dans un message envoyé à l'adresse indiquée dans le bon de commande.

2. Installez la licence. Pour ce faire, cliquez sur le lien Installer la licence dans la rubrique **Activation** de la fenêtre principale de Kaspersky Anti-Virus ou utilisez la commande **Activation** du menu contextuel de l'application. Cette action entraînera l'ouverture de l'Assistant d'activation (cf. point 3.2.2, p. 36).

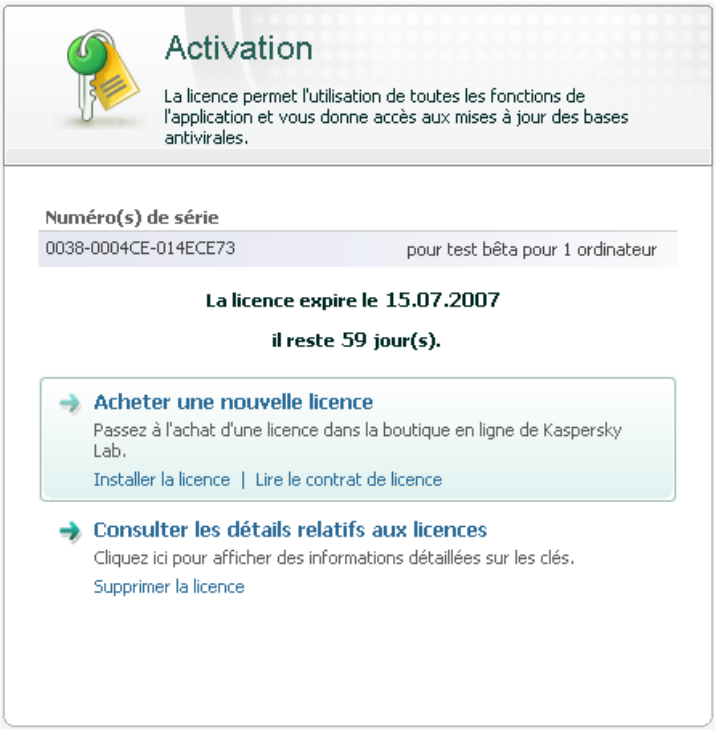


Illustration 57. Administration des licences

CHAPITRE 15. 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 15.2, p. 179). 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 bases de l'application actuelles (cf. point 15.1, p. 175).

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 15.10, p. 211). 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, banque de solutions.
- 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 15.9.1, p. 203). 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 protègent les propres fichiers du logiciel contre les modifications réalisées par des personnes mal intentionnées, interdisent l'administration externe du logiciel par des services et introduisent des restrictions sur l'exécution de certaines actions à l'aide de Kaspersky Anti-Virus (cf. point 15.9.2, p. 206). Par exemple, une modification du niveau de protection peut fortement influencer la sécurité des données sauvegardées sur votre ordinateur.

- Le service d'administration des configurations de l'application permet d'enregistrer les paramètres de fonctionnement de l'application pour les transférer vers d'autres ordinateurs (cf. point 15.9.3, p. 210), ainsi que de rétablir les paramètres par défaut (cf. point 15.9.4, p. 210).

Le logiciel propose également des rapports complets (cf. point 15.3, p. 182) sur le fonctionnement de tous les composants de la protection et l'exécution de toutes les tâches liées à la recherche de virus et aux mises à jour.

La constitution de la liste des ports contrôlés permet de régler le contrôle des données qui transitent via les ports issues de certains composants de protection de Kaspersky Anti-Virus (cf. point 15.4, p. 190). La configuration des paramètres du serveur proxy (cf. point 15.7, p. 198) garantit l'accès de l'application à Internet, ce qui est important pour le fonctionnement de certains composants de la protection en temps réel et pour la mise à jour.

La création d'un disque de secours permet de rétablir le fonctionnement de l'ordinateur (cf. point 15.4, p. 190). Cela est particulièrement utile lorsqu'il n'est plus possible de lancer le système d'exploitation de l'ordinateur après l'infection du code malveillant.

Vous pouvez également modifier l'aspect extérieur de Kaspersky Anti-Virus et configurer les paramètre de l'interface actuelle (cf. point 15.6, p. 196).

Examinons en détails ces différents services.

15.1. 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 bases de l'application contiennent les menaces qui ont été étudiées par les experts de Kaspersky Lab. Si le programme malveillant a été modifié et que ces modifications ne figurent pas encore dans les bases, Kaspersky Anti-Virus considère l'objet comme étant infecté par une modification d'un programme malveillant et le classe comme objet poten-

tiellement infecté. Il indique obligatoirement à quelle menace cette infection ressemble.

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

  Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Anti-Virus 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, l'antivirus de courrier électronique ou lors de la recherche de virus ou par la défense proactive.

Vous pouvez vous-même placer un objet en quarantaine en cliquant sur le lien 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.

15.1.1. Manipulation des objets en quarantaine

Le nombre total d'objets placés en quarantaine est repris dans les **Rapports** de la fenêtre principale. 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 lien 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 sur le lien Quarantaine.

Vous pouvez réaliser les opérations suivantes dans l'onglet quarantaine (cf. ill. 58) :

- 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*.

> En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se produira uniquement si l'analyse a eu lieu un certain temps (au moins trois jours) après la mise du fichier en quarantaine.

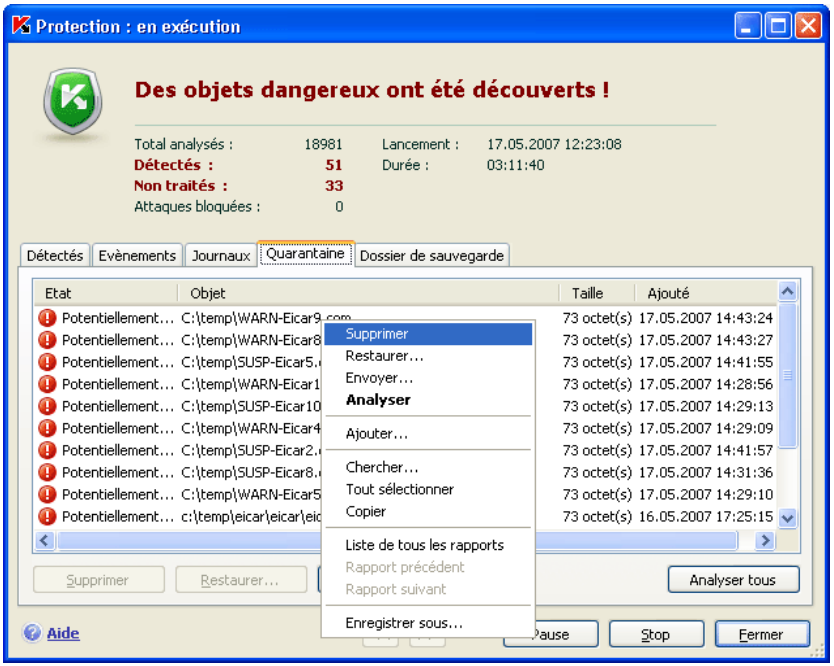


Illustration 58. Liste des objets en quarantaine

- Analyser et réparer à l'aide de la version actuelle des bases de l'application tous les objets potentiellement infectés qui se trouvent en quarantaine. 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.

- Restaurer les fichiers dans un répertoire choisi par l'utilisateur ou dans le répertoire d'origine où ils se trouvaient avant d'être mis en quarantaine (par défaut). 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**.

15.1.2. 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 bases de l'application (pour de plus amples informations, consultez le point 13.3.4 à la page 171)

  Attention !

  Le logiciel ne peut analyser les objets en quarantaine directement après la mise à jour des bases 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 de configuration de l'application et sélectionnez la rubrique **Rapports**.
2. Définissez dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. ill. 59) le délai de conservation au terme duquel les objets seront automatiquement supprimés.

Illustration 59. Configuration de la conservation des objets en quarantaine

15.2. 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.

15.2.1. Manipulation des copies de sauvegarde

Le nombre total de copies de sauvegarde placées dans le dossier est repris dans les **Rapports** de la fenêtre principale de l'application. 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 lien Purger. N'oubliez pas que cette action entraîne la suppression des objets du dossier de quarantaine et des fichiers de rapport.

Pour manipuler les copies des objets dangereux :

Cliquez sur le lien Dossier de sauvegarde.

La partie centrale de l'onglet (cf. ill. 60) reprend la liste des copies de sauvegarde. Les informations suivantes sont fournies pour chaque copie : nom complet de l'objet avec chemin d'accès à son emplacement d'origine, l'état de l'objet attribué suite à l'analyse et sa taille.

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 bases de l'application 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 les copies les plus anciennes du répertoire (cf. point 15.2.2, p. 181).

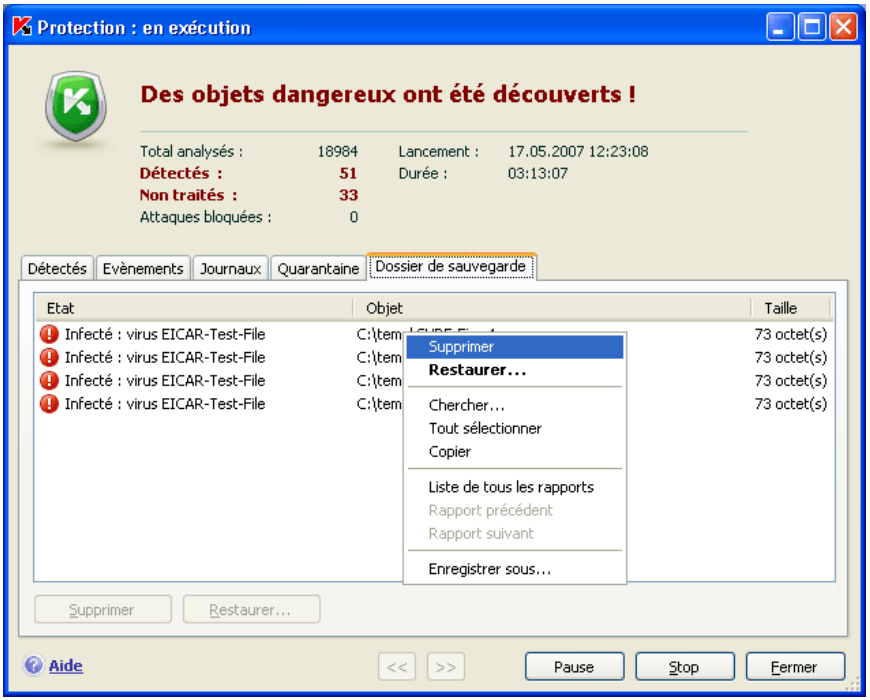


Illustration 60. Copies de sauvegarde des objets supprimés ou réparés

15.2.2. 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 30 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 de configuration de l'application et sélectionnez la rubrique **Rapports**.
2. Définissez le délai de conservation des copies de sauvegarde dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. ill. 59) dans la partie droite de la fenêtre.

15.3. Utilisation des rapports

Le fonctionnement de chaque composant 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 la rubrique **Rapports** de la fenêtre principale du logiciel. Ces informations sont reprises dans le bloc **Rapports**.

Pour consulter les rapports :

Cliquez sur le lien Rapports.

La fenêtre s'ouvre sur l'onglet **Rapports** (cf. ill. 61). Vous y verrez les derniers rapports sur tous les composants et les tâches de recherche de virus et de mise à jour lancées au cours de cette session de Kaspersky Anti-Virus. Le résultat du fonctionnement est affiché en regard de chaque composant ou tâche. Exemple, *en exécution, en pause* ou *inactif.* Si vous souhaitez consulter l'historique complet des rapports pour la session en cours, cochez la case **Afficher l'historique**.

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

sélectionnez le nom du composant 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 du composant 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. En fonction du composant ou de la tâche, la composition des onglets peut varier:

- L'onglet **Détectés** contient la liste des objets dangereux découverts par le composant ou la tâche de recherche de virus exécutée.
- **Evénements** illustre les événements survenus pendant l'exécution de la tâche ou le fonctionnement du composant
- L'onglet **Statistiques** reprend les statistiques détaillées de tous les objets analysés.
- L'onglet **Paramètres** reprend les paramètres qui définissent le fonctionnement du composant de protection, de la recherche de virus ou de la mise à jour des bases de l'application.

- L'onglet **Registres** apparait uniquement dans le rapport de la défense proactive. Ils fournissent des informations et sur toutes les tentatives de modification de la base de registres système du système d'exploitation.

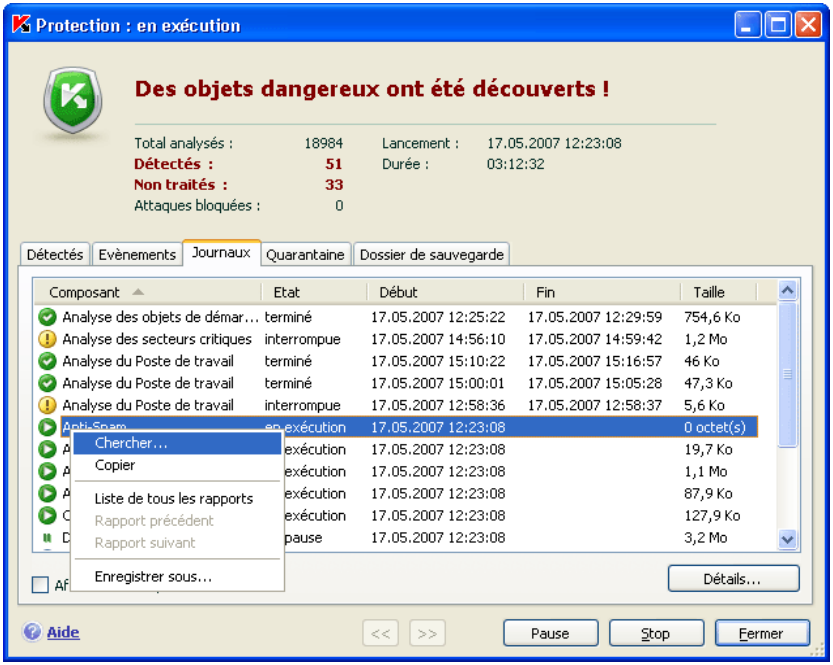


Illustration 61. Rapports sur le fonctionnement des composants du programme

Tout le rapport peut être exporté 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 d'un composant 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 **Actions→Enregistrer sous** et indiquez où vous souhaitez enregistrer le fichier.

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

Tous les onglets de rapport à l'exception des **Paramètres** et **Statistiques** contiennent 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 bases de l'application actualisées ou le supprimer. Vous pouvez appliquer cette action à un seul objet de la liste ou à une sélection d'objets.

Supprimer : supprime l'objet dangereux de l'ordinateur.

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 bases de l'application.

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 : 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 des boutons **Réparer** (pour un objet ou un groupe d'objets sélectionnés) ou **Réparer tous** (pour tous les objets de la liste). Lors du traitement de chaque objet, un message apparaît et vous invite à décider des actions à réaliser.

Si vous cochez dans cette fenêtre la case **Appliquer à tous les cas similaires**, alors l'action sélectionnée sera appliquée à tous les objets du même état avant le début du traitement.

15.3.1. Configuration des paramètres du rapport

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

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Rapports**.
2. Dans le bloc **Rapports** (cf. ill. 62), 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 30 jours. Les rapports sont supprimés à l'issue des 30 jours. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.

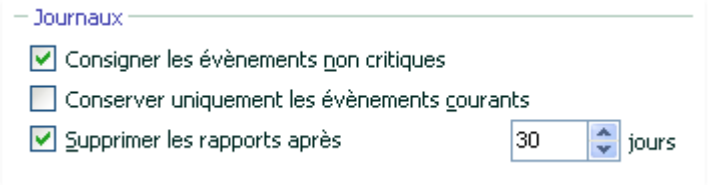


Illustration 62. Configuration des paramètres de constitution des rapports

15.3.2. Onglet Détectés

Cet onglet (cf. ill. 63) 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**.

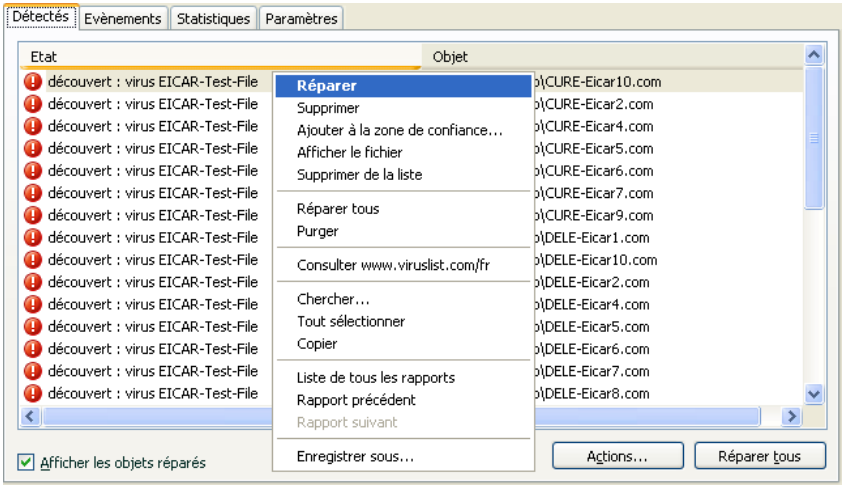


Illustration 63. Liste des objets dangereux découverts

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.

15.3.3. Onglet Evénements

Cet onglet (cf. ill. 64) reprend la liste de tous les événements importants survenus pendant le fonctionnement du composant de protection, lors de l'exécution d'une tâche liée à la recherche de virus ou de la mise à jour, pour autant que ce comportement ne soit pas annulé par une règle de contrôle de l'activité (cf. point 10.1, p. 125).

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.

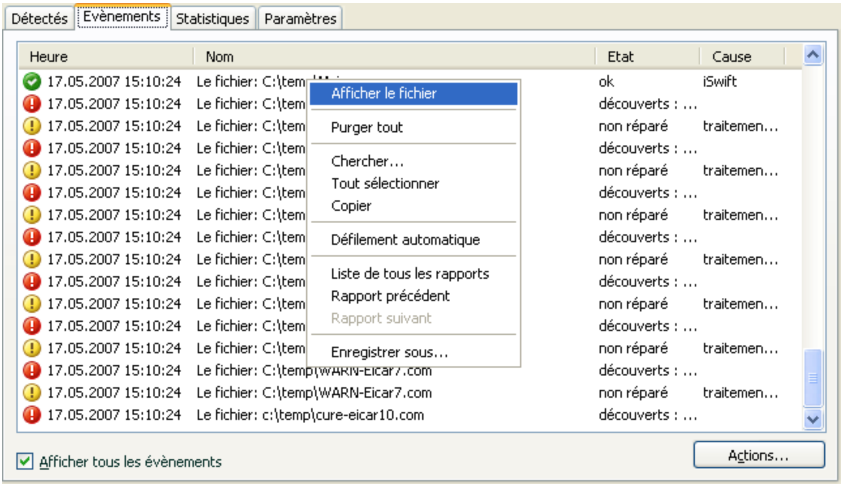


Illustration 64. Evénements survenus pendant

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.

15.3.4. Onglet Statistiques

Cet onglet reprend les statistiques détaillées du fonctionnement du logiciel ou de l'exécution des tâches liées à la recherche de virus (cf. ill. 65). Vous pouvez voir:

- Le nombre d'objets soumis à l'analyse antivirus pendant la session actuelle du composant 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.

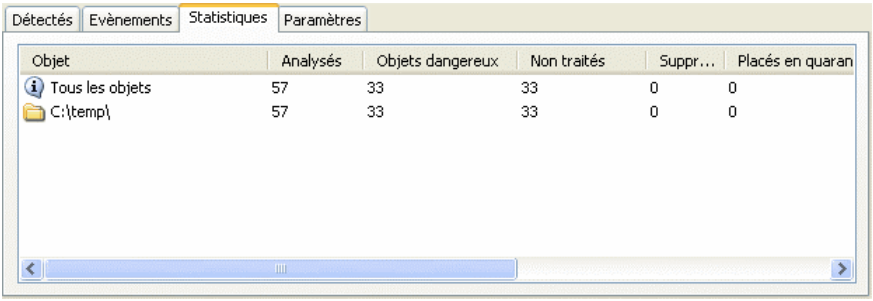


Illustration 65. Statistique du composant

15.3.5. Onglet Paramètres

Cet onglet (cf. ill. 66) présente tous les paramètres qui définissent le fonctionnement du composant de la protection 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 le composant 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.

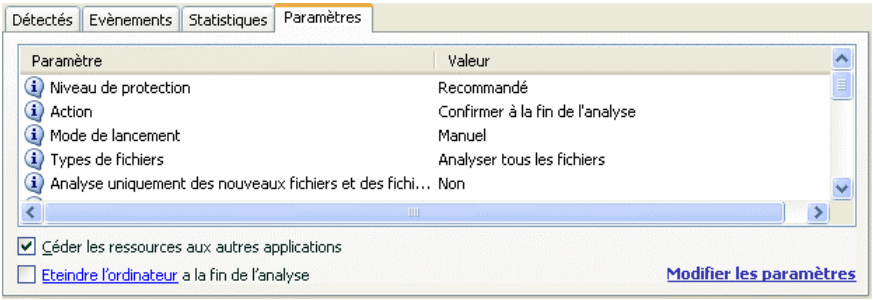


Illustration 66. Paramètres de fonctionnement du composant

- 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.

  Cette option est utile si vous lancez la recherche de virus à la fin de votre journée de travail et que vous ne voulez pas attendre la fin de l'analyse.

  Cependant, l'utilisation de ce paramètre requiert le préparatif suivant : le cas échéant, il faut, avant de lancer l'analyse, désactiver la requête du mot de passe lors de l'analyse des objets et sélectionner le mode de traitement automatique des objets dangereux. Le mode de fonctionnement interactif est désactivé suite à ces actions. Le programme n'affichera aucune requête susceptibles d'interrompre l'analyse.

15.3.6. Onglet *Registre*

Les opérations sur les clés de la base de registres système au moment du lancement du programme sont consignées dans l'onglet **Registre** (cf. ill. 67), si l'enregistrement n'est pas contraire à la règle (cf. point 10.3.2, p. 137).

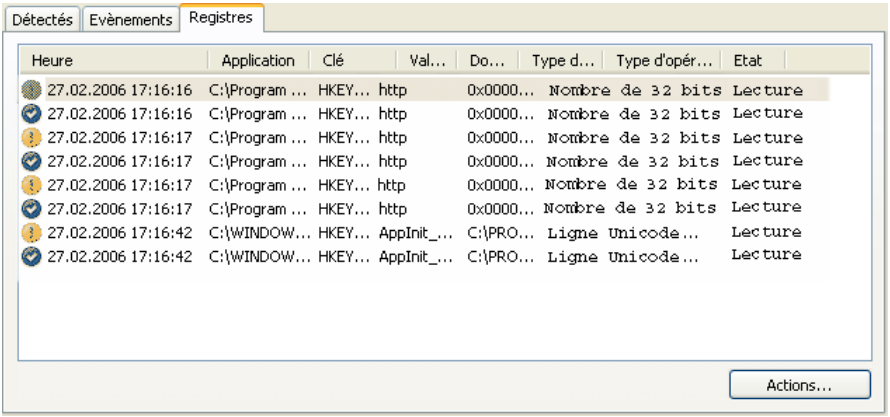


Illustration 67. Lecture et modification de clés de la base de registre

L'onglet reprend le nom complet de la clé, sa valeur, le type de données ainsi que des renseignements sur l'opération exécutée : tentative d'exécution d'une action quelconque, heure de l'autorisation, etc.

15.4. Disque de secours

Kaspersky Anti-Virus propose la création d'un disque de secours.

Le disque de démarrage doit permettre la restauration des fonctions du système après une attaque de virus qui aurait endommagé le système de fichiers du système d'exploitation et qui rendrait impossible le chargement initial. Le disque comprend :

- Les fichiers systèmes de Microsoft Windows XP Service Pack 2;
- Un ensemble d'utilitaire pour le diagnostic du système d'exploitation;
- Les fichiers du logiciel Kaspersky Anti-Virus;
- Les fichiers contenant les bases de l'application.

Afin de créer le disque de secours:

1. Ouvrez la fenêtre principale de l'application et sélectionnez **Analyse**.
2. Cliquez sur le lien Créer un CD/DVD de Secours Bootable afin de lancer la création du disque.

Le disque de secours ne peut fonctionner que sur l'ordinateur sur lequel il a été créé. L'utilisation de ce disque sur d'autres ordinateurs peut entraîner des conséquences imprévisibles car il contient des paramètres propres à un ordinateur particulier (par exemple, les informations relatives aux secteurs de démarrage).

La création d'un disque de secours est possible uniquement pour les versions installées sous Microsoft Windows XP et Microsoft Windows Vista. Pour les autres versions, y compris Microsoft Windows XP Professional x64 Edition et Microsoft Windows Vista x64 la création d'un tel disque n'est pas prise en charge.

15.4.1. Création d'un CD de Secours Bootable

Attention ! Afin de pouvoir créer ce disque de démarrage, vous devrez utiliser le disque d'installation de Microsoft Windows XP Service Pack 2.

La création d'un disque de secours s'opère à l'aide du programme PE Builder.

Afin de créer un disque à l'aide de PE Builder, il faut tout d'abord l'installer sur l'ordinateur.

La création du disque de secours s'opère à l'aide d'un assistant spécial qui contient une succession de fenêtre (étape) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Pour terminer le travail de l'assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Etape 1. Préparatifs pour l'enregistrement

Pour créer le disque de secours, indiquez le chemin d'accès aux répertoires suivants :

- Répertoire d'installation de PE Builder.
- Répertoire de sauvegarde des fichiers du disque de démarrage avant la création du cédérom.

  Si ce n'est pas la première fois que vous créez un disque, ce répertoire contient déjà l'ensemble des fichiers préparés la dernière fois. Afin d'utiliser les fichiers enregistrés préalablement, cochez la case adéquate.

N'oubliez pas que la version antérieure des fichiers du disque de démarrage contient les anciennes bases de l'application. Afin de garantir la meilleure recherche de virus et la restauration du système, il est conseillé d'actualiser les bases et de créer une nouvelle version du disque de démarrage.

- Cédérom d'installation de Microsoft Windows XP Service Pack 2.

Cliquez sur **Suivant** une fois que vous aurez saisi le chemin d'accès aux différents répertoires. Cette action entraînera le lancement de PE Builder et la création des fichiers du disque de démarrage. Attendez la fin du processus. Cela peut durer quelques minutes.

Etape 2. Création d'un fichier ISO

Une fois que PE Builder aura terminé de créer les fichiers du disque de démarrage, la fenêtre **Création d'un fichier ISO** s'ouvrira.

Le fichier ISO est une image du futur disque sous la forme d'une archive. Les fichiers au format ISO sont correctement interprétés par la majorité des programmes d'enregistrement de cédérom (par exemple, Nero).

S'il ne s'agit pas du premier disque de secours que vous créez, vous pouvez utiliser le fichier ISO de la version précédente. Pour ce faire, sélectionnez **Fichier ISO existant**.

Etape 3. Enregistrement du disque

Cette fenêtre de l'Assistant vous permet de choisir quand enregistrer les fichiers du disque de démarrage sur le cédérom/dvd-rom : maintenant ou plus tard.

Si vous avez sélectionné l'enregistrement immédiat du disque, indiquez s'il faut nettoyer le contenu du lecteur de cédérom/dvd-rom avant de procéder à l'enregistrement. Pour ce faire, cochez la case correspondante. Cette possibilité est accessible uniquement si le graveur de cédérom/dvd-rom est compatible avec les cédéroms/dvd-rom réinscriptibles.

En cliquant sur **Suivant**, vous lancez le processus d'enregistrement du cédérom de démarrage. Attendez la fin du processus. Cela peut durer quelques minutes.

Etape 4. Fin de la création du disque de démarrage

Cette fenêtre de l'assistant vous informe de la réussite de la création du disque de secours.

15.4.2. Utilisation du disque de démarrage

En mode de réparation, Kaspersky Anti-Virus fonctionnera uniquement si la fenêtre principale est ouverte. Le programme sera déchargé dès que la fenêtre principale sera fermée.

Le programme Bart PE, installé par défaut, ne prend pas en charge les fichiers chm et le navigateur Internet. Cela signifie que l'aide de Kaspersky Anti-Virus et les conseils dans l'interface du logiciel ne sont pas accessibles en mode de restauration.

Lorsqu'il n'est plus possible de démarrer le système d'exploitation suite à une attaque de virus, agissez comme suit :

1. Créez un disque de secours à l'aide de Kaspersky Anti-Virus sur l'ordinateur sain.
2. Introduisez le disque de démarrage dans le lecteur de l'ordinateur infecté et redémarrez. Cette action entraîne le lancement du système d'exploitation Microsoft Windows XP SP2 avec l'interface du logiciel Bart PE.
   Le logiciel Bart PE prend en charge le fonctionnement dans un réseau local. Lors du lancement du programme, l'écran affiche une requête d'activation de la prise en charge de l'utilisation au sein de réseau local. Acceptez-la si vous avez l'intention d'actualiser les bases de l'application depuis un répertoire local avant d'analyser l'ordinateur. Si la mise à jour n'est pas nécessaire, annulez l'activation de la prise en charge du réseau.
3. Pour lancer Kaspersky Anti-Virus, exécutez la commande **Démarrer→Programmes→Kaspersky Anti-Virus 7.0→Start**.

   Cette action entraîne l'ouverture de la fenêtre principale de Kaspersky Anti-Virus. En mode de restauration, seules la recherche de virus et la mise à jour des signatures des menaces au départ du réseau local (si vous avez activé la prise en charge du réseau dans Bart PE) sont accessibles.
4. Lancez l'analyse antivirus de l'ordinateur.

N'oubliez pas que l'analyse par défaut utilise les bases de l'application qui étaient d'actualité lors de la création du disque de démarrage. Pour cette raison, il est conseillé d'actualiser les bases avant de lancer l'analyse.

Pensez également au fait que les bases de l'application actualisées seront utilisées par l'application uniquement lors de la session d'utilisation du disque de secours avant de redémarrer l'ordinateur.

Attention !

Si la vérification de l'ordinateur permet d'identifier des objets infectés ou potentiellement infectés et que ceux-ci ont été traités avec mise en quarantaine ou dans le dossier de sauvegarde, il est conseillé de terminer le traitement dans cette session d'utilisation du disque de secours.

Dans le cas contraire, ces objets seront perdus après le redémarrage de l'ordinateur.

15.5. Constitution de la liste des ports contrôlés

Les composants tels que l'antivirus de courrier électronique et l'antivirus Internet contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains ports ouverts de l'ordinateur. Ainsi, l'antivirus de courrier électronique analyse les données transmises via le protocole SMTP tandis que l'antivirus Internet analyse les paquets HTTP.

La lise des ports qui sont normalement utilisés pour le courrier et le trafic http sont repris dans le logiciel. Vous pouvez ajouter de nouveaux ports ou désactiver le contrôle exercé sur certains ports, ce qui suspend la recherche d'éventuels objets dangereux dans le trafic qui transite via ces ports.

Pour modifier la liste des ports soumis à un contrôle :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Contrôle du trafic**.
2. Cliquez sur le bouton **Configuration des ports**.
3. Modifiez la liste des ports soumis à un contrôle dans la fenêtre **Configuration des ports** (cf. ill. 68).

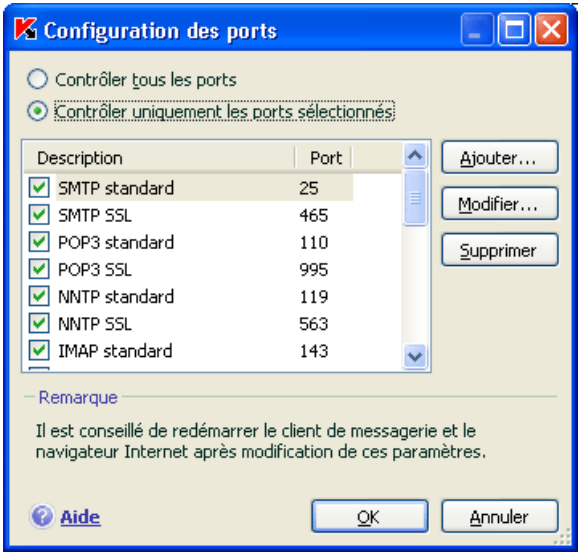


Illustration 68. Liste des ports contrôlés

Cette fenêtre reprend la liste des ports contrôlés par Kaspersky Anti-Virus. Afin d'analyser les flux de données qui transitent via tous les ports ouverts du réseau, sélectionnez l'option **Contrôler tous les ports**. Si vous souhaitez modifier la liste des ports contrôlés manuellement, sélectionnez l'option **Contrôler uniquement les ports sélectionnés**.

Pour ajouter un nouveau port à la liste :

1. Cliquez sur **Ajouter** dans la fenêtre de configuration des ports.
2. Saisissez le numéro du port et sa description dans les champs correspondant de la fenêtre **Nouveau port**.

Par exemple, votre ordinateur possède un port inhabituel pour l'échange des données avec un ordinateur distant via le protocole HTTP. C'est l'antivirus Internet qui est chargé du contrôle du trafic HTTP. Afin de pouvoir rechercher la présence éventuelle de code malveillant dans ces données, il faudra ajouter ce port à la liste des ports soumis à un contrôle.

Lors du lancement de n'importe quel composant de Kaspersky Anti-Virus, le port 1110 est ouvert pour écouter toutes les connexions entrantes. Si ce port est occupé par une autre application, le port 1111, 1112, etc. sera choisi pour l'écoute.

Si vous utilisez simultanément Kaspersky Anti-Virus et un pare-feu d'un autre éditeur, il faudra configurer ce pare-feu pour qu'il autorise le processus *avp.exe* (processus interne de Kaspersky Anti-Virus) sur tous les ports cités.

Par exemple, votre pare-feu possède une règle pour *iexplorer.exe* qui permet à ce processus d'établir une connexion sur le port 80.

Cependant Kaspersky Anti-Virus qui intercepte la requête de connexion lancée par *iexplorer.exe* sur le port 80 la transmet à son processus *avp.exe* qui tente, à son tour, d'établir une connexion avec la page Web demandée. Si aucune règle d'autorisation n'a été définie pour le processus *avp.exe*, le pare-feu bloquera la requête. Par conséquent, l'utilisateur ne pourra pas ouvrir la page Web.

15.6. Analyse de la connexion sécurisées

Les connexions à l'aide du protocole SSL protège le canal d'échange des données sur Internet. Le protocole SSL permet d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus mal intentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL.

Kaspersky Anti-Virus 7.0 recherche la présence de virus dans le trafic du protocole SSL. En cas de tentative de connexion avec une ressource en ligne en mode sécurisé, un message (cf. ill. 99) demandera la confirmation de l'utilisateur.

Ce message contient des informations relatives au logiciel à l'origine de la connexion sécurisée ainsi que des renseignements sur le port et l'adresse distant. Pour poursuivre l'analyse ou pour l'annuler, sélectionnez une des deux actions suivantes :

- **Traiter** : procéder à la recherche de virus dans le trafic lors de la connexion à une ressource en ligne en mode sécurisé.
- **Ignorer** : poursuivre la connexion avec la ressource Internet sans recherche la présence d'éventuels virus dans le trafic.

Pour appliquer ultérieurement l'action choisie à chaque tentative de connexion SSL dans la séance actuelle de travail du navigateur, cochez la case ☑ **Appliquer à tous les cas**.

Illustration 69. Notification de la découverte d'une connexion SSL

Afin d'analyser les connexions cryptées, Kaspersky Anti-Virus remplacer les certificats de sécurité par son propre certificat de sécurité autosigné. Dans certains cas, les programmes qui établissent la connexion ne reconnaissent pas ce certificat, ce qui veut dire que la connexion ne sera pas établie. Dans de tels cas, il est conseillé de choisir **Ignorer** dans la notification sur l'analyse de la connexion sécurisée :

- Lors de la connexion à une ressource de confiance telle que le site de votre banque où vous gérez vos comptes. Dans ce cas, il est primordial d'obtenir la confirmation de l'authenticité du certificat de la banque.
- Si le programme qui établit la connexion analyse le certificat de la ressource interrogée. Ainsi, MSN Messenger lors de l'établissement d'une connexion sécurisée avec le serveur vérifie l'authenticité de la signature numérique de Microsoft Corporation.

La configuration de l'analyse des connexions SSL s'opère dans la rubrique **Contrôle du trafic** de la fenêtre de configuration de l'application (cf. ill. 70) :

Analyser toutes les connexions sécurisées : recherche la présence de virus dans tout le trafic qui transite via le protocole SSL.

Confirmer l'analyse en cas de découverte d'une connexion protégée : demande la confirmation de l'utilisateur à chaque tentative d'établissement d'une connexion SSL.

Ne pas analyser les connexions sécurisées : absence de recherche de virus dans le trafic transmis via le protocole SSL.

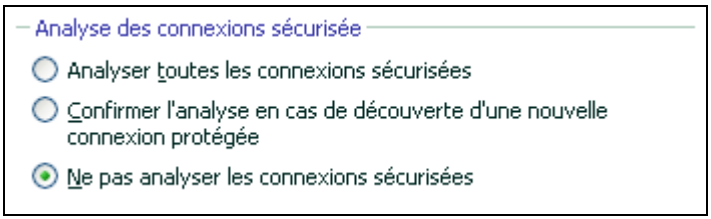


Illustration 70. Configuration de l'analyse des connexions sécurisées

15.7. Configuration des paramètres du serveur proxy

Dans la rubrique **Serveur proxy** (cf. ill. 71)de la fenêtre de configuration de l'application, vous pouvez configurer les paramètre de connexion au serveur proxy (si la connexion s'opère via un serveur proxy). Kaspersky Anti-Virus utilise ces paramètres dans quelques composants de la protection en temps réel ainsi que pour l'actualisation des bases et des modules de l'application.

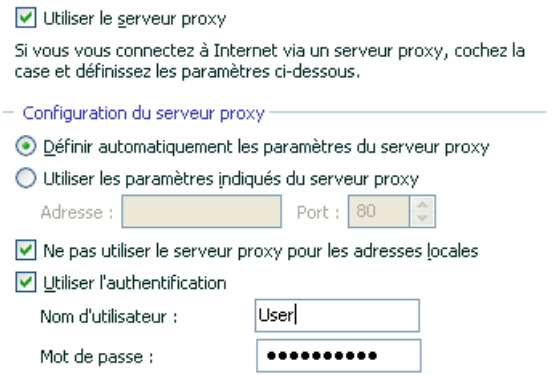


Illustration 71. Configuration des paramètres du serveur proxy

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

- Sélectionnez les paramètres du serveur proxy à utiliser:

  Définir automatiquement les paramètres 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 paramètres indiqués du proxy serveur : 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.

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

- 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 **Utiliser l'authentification** et saisissez dans les champs de la partie inférieure le nom d'utilisateur 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'autorisation NTML en utilisant les données du compte utilisateur sous lequel la tâche est exécutée (par exemple, la mise à jour (cf. point 6.6, p. 67).

  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. Si l'autorisation réussit, le nom et le mot de passe saisis seront utilisés par la suite. Dans le cas contraire, il faudra à nouveau saisir les paramètres d'autorisation.

  Lorsque vous cliquez sur le bouton **Annuler** dans la fenêtre des paramètres d'autorisation, la source actuelle des mises à jour sera remplacée par la suivante dans la liste et les paramètres d'autorisation indi-

qués dans cette fenêtre ou définis dans l'interface du programme seront ignorés. Autrement dit, une tentative d'autorisation NTLM à l'aide du compte utilisateur sous lequel la tâche a été lancée est exécutée.

En cas de mise à jour depuis un serveur FTP, la connexion est établie par défaut avec le serveur en mode passif. En cas d'échec de cette connexion, la tentative de connexion sera réalisée en mode actif.

Le temps prévu pour établir la connexion est défini par défaut à 1 minute. Si la connexion n'a pas pu être établie à la fin de ce délai, une tentative de connexion est lancée avec le prochain serveur de mise à jour et ainsi de suite jusqu'à ce qu'une connexion ait pu être établie ou tant que tous les serveurs de mise à jour disponible n'ont pas été contactés.

15.8. 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 zone de notification de la barre des tâches de Microsoft Windows et les infobulles.

Pour configurer l'interface de Kaspersky Anti-Virus:

Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Apparence** (cf. ill. 72).

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

- Utilisation d'éléments graphiques propres et de la palette des de couleurs dans l'interface du logiciel.

  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.

  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

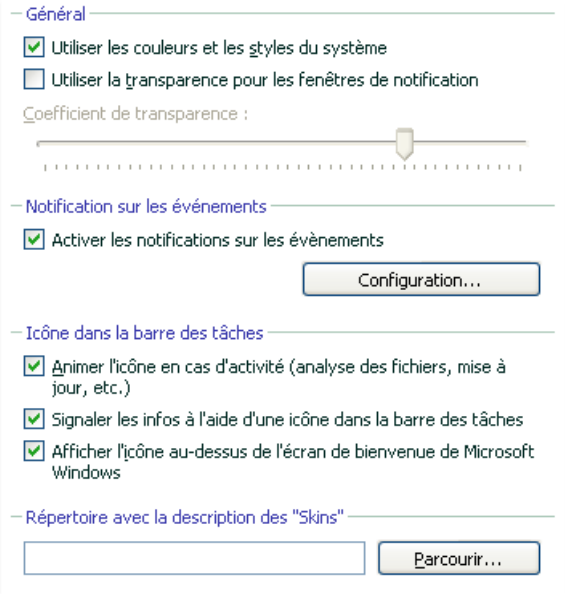


Illustration 72. Configuration des paramètres de l'interface du programme

- 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 zone de notification de la barre des tâches de Microsoft Windows. 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**.

- Animer ou non l'icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows.

  L'icône de l'application varie en fonction de l'opération exécutée. Par exemple, lors de l'analyse d'un script, une image représentant un script apparaît sur le fond de l'icône. Une image représentant une lettre apparaît pendant l'analyse du courrier. L'icône est animée par défaut. 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 qui apparaît est grisée.

- *Signaler ou non la réception d'informations de Kaspersky Lab.*

  Par défaut, chaque fois que des informations sont reçues, une icône spéciale apparaît dans la zone de notification de la barre des tâches de Microsoft Windows. Un clic sur cette icône permet d'ouvrir une fenêtre contenant le texte des informations. Si vous souhaitez désactiver la notification désélectionnez la case ☑ **Signaler les infos à l'aide d'une icône dans la barre des tâches**.

- 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**.

N'oubliez pas que la modification des paramètres de l'interface de Kaspersky Anti-Virus n'est pas préservée lors du rétablissement des paramètres par défaut ou de la suppression du programme.

15.9. Utilisation des services complémentaires

Kaspersky Anti-Virus vous propose également les services complémentaires suivants (cf. ill. 73)::

- Lancement de Kaspersky Anti-Virus au démarrage du système d'exploitation (cf. point 15.11, p. 213) ;
- Avertissement de l'utilisateur en cas d'événements particuliers (cf. point 15.9.1, p. 203).
- 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 (cf. point 15.9.2, p. 208).
- Exportation/importation des paramètres de fonctionnement de Kaspersky Anti-Virus (cf. point 15.9.3, p. 210);

- Rétablissement des paramètres par défaut (cf. point 15.9.4, p. 210).

Pour passer à la configuration de l'utilisation de ces services :

Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Services**.

Vous pouvez, dans la partie droite, décider d'activer ou non les services complémentaires.

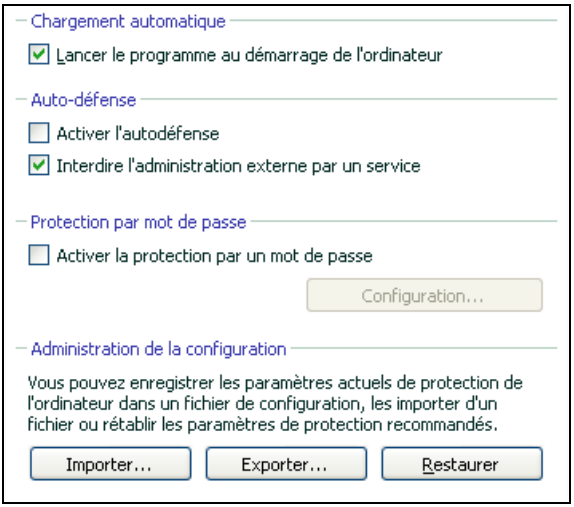


Illustration 73. Configuration des services complémentaires

15.9.1. 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 zone de notification de la barre des tâches de Microsoft Windows.
- Notification sonore.
- Messages électroniques.
- Enregistrements dans le journal des événements.

Pour utiliser ce service :

1. Cochez la case **Activer les notifications sur les événements** dans le bloc **Notification sur les événements** dans la rubrique **Apparence** de la fenêtre de configuration de l'application (cf. ill. **72**).
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 15.9.1.1, p. 204).
3. Configurez les paramètres d'envoi des notifications par courrier électronique si vous avez choisi ce mode (cf. point 15.9.1.2, p. 206).

15.9.1.1. 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, *bases de l'application 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 bases de l'application.

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. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Apparence** (cf. ill. 72).
2. Cochez la case **Activez les notifications sur les événements** dans le groupe **Notification sur les événements** et passez à la configuration détaillée à l'aide du bouton **Configuration**.

Dans la fenêtre **Configuration des notifications sur les événements** (cf. ill. 74), vous pouvez définir les modes d'envoi suivants pour les notifications :

- *Infobulles* au-dessus de l'icône du logiciel dans la zone de notification de la barre des tâches de Microsoft Windows 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.

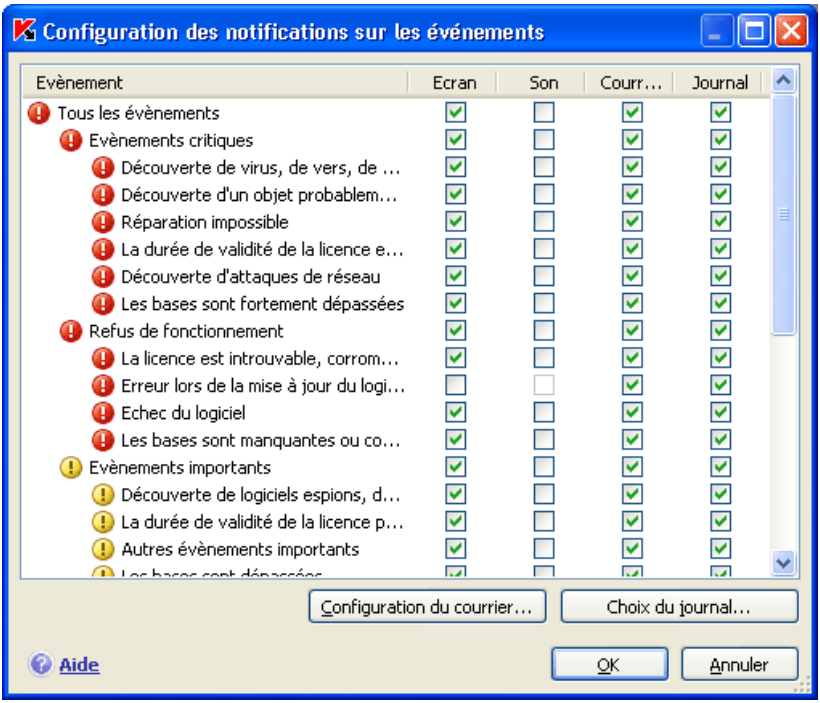


Illustration 74. Evénement survenus pendant le fonctionnement du logiciel et modes de notification choisis

- *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 ☑ **Courrier électronique** en regard de l'événement au sujet duquel vous souhaitez être averti et configurez les paramètres d'envoi des notifications (cf. point 15.9.1.2, p. 206).

- *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 15.9.1.3, p. 207).

15.9.1.2. Configuration de l'envoi des notifications par courrier électronique

Après avoir sélectionné les événements (cf. point 15.9.1.1, p. 204) au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications. Pour ce faire :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Apparence** (cf. ill. 72).
2. Cliquez sur le bouton **Configuration** dans le bloc **Notification sur les événements**.
3. Dans la fenêtre **Configuration de notifications sur les événements**, cochez la case ☑ dans la partie **Message** pour les événements qui déclencheront l'envoi d'une notification par courrier électronique.
4. 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 notification au nom de l'utilisateur**.
   - 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.

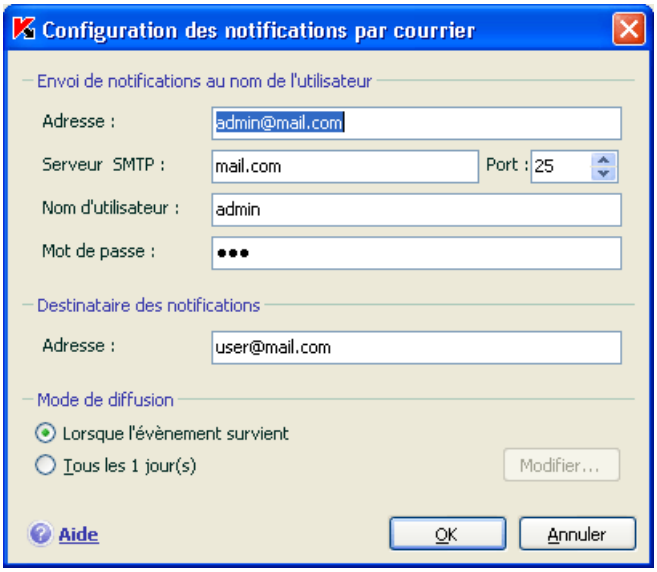


Illustration 75. Configuration de la notification par courrier électronique

15.9.1.3. Configuration du journal des événements

Pour configurer le journal des événements :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Apparence** (cf. ill. 72).
2. Cliquez sur le bouton **Configuration** du bloc **Notification sur les événements**.

Dans la fenêtre **Configuration des notifications sur les événements**, sélectionnez le type d'événements que vous voulez enregistrer dans le journal et cliquez sur le bouton **Choix 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**.

15.9.2. 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 ces 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.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de l'application contre la modification et la suppression des fichiers sur le disque ou des clés dans la base de registres système est accessible.

Afin d'activer l'utilisation des mécanismes d'autodéfense du logiciel :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Services** (cf. ill. 73).
2. Opérez la configuration requise dans le bloc **Auto-défense** :

   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 enregistrement 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.

   Afin de permettre aux programmes d'administration à distance (par exemple, RemoteAdmin) d'accéder à l'administration de Kaspersky Anti-Virus, il faut ajouter ces programmes à la liste des applications

de confiance et activer pour celles-ci le paramètre **Ne pas contrôler l'activité de l'application** (cf. point 6.9.2, p. 78).

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

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** dans le groupe du même nom 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. ill. 76). 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 faire confiance aux personnes à qui vous confiez ces tâches.

Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions que vous avez sélectionnées, il devra saisir le mot de passe.

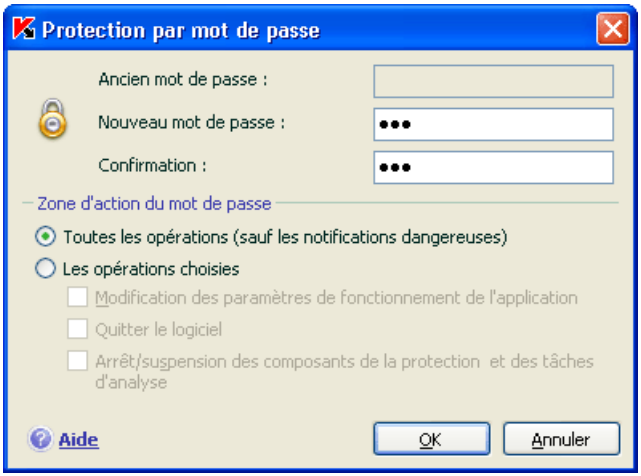


Illustration 76. Configuration de la protection par mot de passe

15.9.3. Exportation/importation des paramètres de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet d'exporter et d'importer ses paramètres.

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

Pour exporter les paramètres actuels de fonctionnement du logiciel :

1. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Service** (cf. ill. 73).
2. Cliquez sur le bouton **Exporter** dans le bloc **Administration de la configuration**.
3. 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 de configuration de l'application et sélectionnez la rubrique **Service**.
2. Cliquez sur **Importer** et sélectionnez le fichier contenant les paramètres que vous souhaitez importer dans Kaspersky Anti-Virus.

15.9.4. 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. Ouvrez la fenêtre de configuration de l'application et sélectionnez la rubrique **Services** (cf. ill. 73).
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.

La liste propose les composants du logiciel dont les paramètres ont été modifiés par l'utilisateur. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la liste.

Ces paramètres uniques sont : des règles d'exclusion prédéfinies pour une auto-protection des composants du programme, les listes des adresses mails de confiances et les règles d'application de la Défense Proactive.

Parmi les paramètres que vous pouvez conserver, il y a la liste des adresses Internet et des numéros d'accès de confiance utilisée par l'antivirus Internet, les règles d'exclusion pour les composants du programme ainsi que les règles pour les applications de la défense proactive.

Les règles d'exclusions composées pour les composants du logiciel, les listes d'adresse de confiance utilisées par l'antivirus Internet et les règles pour les applications de la défense proactives figurent parmi ces paramètres uniques

Ces listes sont composées lors de l'utilisation du logiciel, sur la base de tâches individuelles et des exigences de sécurité. Cette opération requiert beaucoup de temps. Pour cette raison, nous vous conseillons de conserver ces paramètres lors de la restauration de la configuration initiale du programme.

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. 35). Suivez les instructions affichées.

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

15.10. Service d'Assistance Technique aux utilisateurs

Les informations relatives à l'assistance technique octroyée par Kaspersky Lab sont reprises dans la section **Assistance Technique** (cf. ill. 77) de la fenêtre principale de l'application.

La partie supérieure propose des informations générales sur l'application : version de l'application, date d'édition des bases utilisées par l'application ainsi que de brèves informations sur le système d'exploitation installé sur votre ordinateur.

Si des problèmes surviennent pendant votre utilisation de Kaspersky Anti-Virus, assurez-vous que la solution n'est pas proposée dans cette aide ou dans la banque de solution du site de l'assistance technique de Kaspersky Lab. La banque des solutions est une rubrique distincte du site du service d'assistance technique qui contient les recommandations sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées. Tentez de trouver la réponse à votre question ou la solution à votre problème dans cette ressource. Pour passer à la banque de solutions, cliquez sur le lien Assistance Technique.

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

N'oubliez pas que pour bénéficier des services de l'assistance technique vous devez être utilisateur enregistré d'une version commerciale de Kaspersky Anti-Virus. L'assistance des utilisateurs de versions d'évaluation n'est pas prévue.

L'enregistrement de l'utilisateur s'opère via l'Assistant d'activation de l'application (cf. point 3.2.2, p. 36) si l'activation de l'application s'effectue à l'aide d'un code d'activation. Dans ce cas, à la fin de l'enregistrement, l'utilisateur recevra un numéro de client qui est visible dans la rubrique **Assistance Technique** (cf. ill. 77) de la fenêtre principale. Le numéro de client est un numéro d'identification personnelle qui est une condition indispensable à l'obtention de l'assistance technique par téléphone ou via le formulaire en ligne.

Pour obtenir des informations sur les formations aux logiciels de Kaspersky Lab, cliquez sur le lien Cours en ligne.

Si vous activez l'application à l'aide d'un fichier de licence, suivez la procédure d'enregistrement directement sur le site Internet du service d'assistance technique.

En cas de problème, vous pouvez contacter le support technique en vous reportant à la section B.2, p. 254.

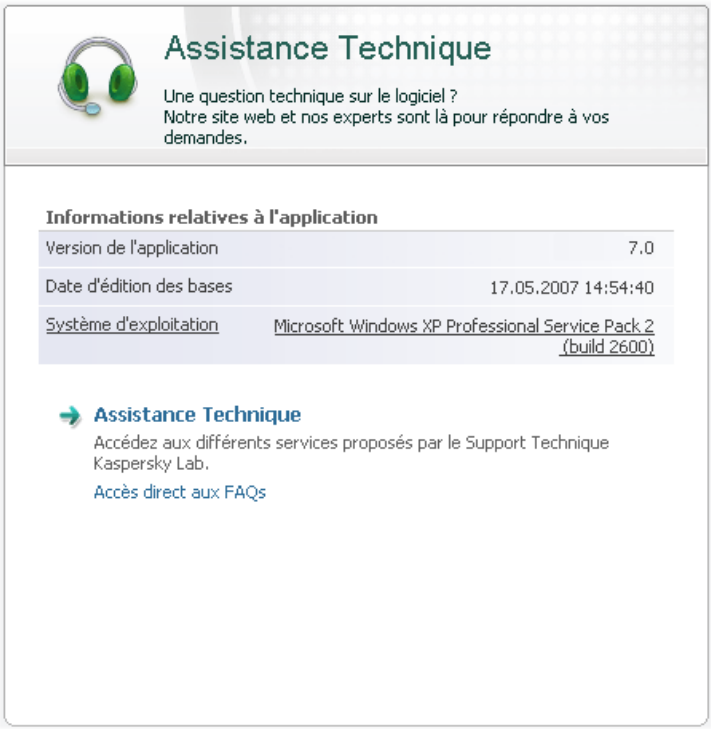


Illustration 77. Informations relatives à l'assistance technique

15.11. 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. 44) 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.

Au cas où des connexions contrôlées par le logiciel seraient établies lorsque vous arrêtez d'utiliser l'ordinateur, un message s'affichera pour indiquer la déconnexion. Ceci est indispensable pour quitter correctement le programme. La déconnexion s'opère automatiquement après 10 secondes ou lorsque vous cliquez sur **Oui**. La majorité des connexions interrompues seront rétablies après un certain temps.

N'oubliez pas que si vous téléchargez un fichier sans l'aide d'un gestionnaire de téléchargement au moment de la déconnexion, le transfert des données sera interrompu. Vous devrez reprendre le téléchargement du fichier à zéro.

Vous pouvez annuler la déconnexion. Pour ce faire, cliquez sur **Non** dans la fenêtre d'avertissement. Le logiciel continuera à fonctionner.

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 7.0 → Kaspersky Anti-Virus 7.0**.

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 **Services** (cf. ill. 73) et cochez la case ☑ **Lancer le programme au démarrage de l'ordinateur**.

CHAPITRE 16. 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 du fonctionnement des composants de l'application;
- lancement, arrêt, suspension et reprise de l'exécution des tâches liées à la recherche de virus;
- obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques;
- Analyse des objets sélectionnés;
- Mise à jour des bases 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 été 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 :

ACTIVATE	Activation de l'application via Internet à l'aide d'un code d'activation
ADDKEY	Activation de l'application à l'aide d'un fichier de licence (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)

START	lancement du composant ou de la tâche
PAUSE	suspension du composant ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
RESUME	reprise du fonctionnement du composant ou de la tâche
STOP	arrêt du composant ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
STATUS	affichage de l'état actuel du composant ou de la tâche
STATISTICS	affichage des statistiques du composant 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	remise à l'état antérieur à la mise à jour (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.

16.1. Activation de l'application

L'activation de l'application peut être réalisée de deux manières :

- via Internet à l'aide d'un code d'activation (commande ACTIVATE);
- à l'aide du fichier de licence (commande ADDKEY).

Syntaxe de la commande :

```
ACTIVATE <code_d'activation>
ADDKEY <nom_du_fichier>
/password=<votre_mot_de_passe>
```

Description des paramètres:

<code_d'activation>	Le code d'activation que vous avez reçu à l'achat du logiciel.
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application.
<nom_du_fichier>	Nom du fichier de licence de l'application avec l'extension **.key*.

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>
```

16.2. Administration des composants de l'application 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]:< fi-
chier_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 des commandes suivantes: **START** : exécution du composant de protection en temps réel et d'une tâche. **STOP** : arrêt du composant de protection en temps réel ou d'une tâche. **PAUSE** : suspension de la protection en temps réel ou d'une tâche. **RESUME** : reprise de la protection en temps réel ou d'une tâche. **STATUS** : affichage de l'état actuel de la protection en temps réel ou d'une tâche. **STATISTICS** : affichage des statistiques relatives à la protection en temps réel ou à une tâche. N'oubliez pas que l'exécution des commandes PAUSE et STOP requiert la saisie d'un mot de passe.
<profil|nom_de_la_tâche>	En guise de valeur du paramètre **<profil>**, vous pouvez indiquer n'importe lequel des composants de la protection en temps réel de l'application ainsi que les modules faisant partie des composants, les tâches créées d'analyse à la demande ou de mise à jour (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-dessous). En guise de valeur du paramètre **<nom_de_la_tâche>**, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour défini par l'utilisateur.
<votre_mot_de_passe>	Mot de passe d'accès à Kaspersky Anti-Virus, défini dans l'interface de l'application.

/R[A]:<fichier_de_rapport>	**R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/R[A]:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Il est possible d'indiquer un chemin d'accès relatif ou absolu au fichier. Si le paramètre n'est pas défini, les résultats de l'analyse sont affichés à l'écran. Tous les événements son repris.

<profile> est remplacé par l'une des valeurs suivantes :

RTP	Tous les composants de la protection La commande `avp.com START RTP` lance tous les composants de la protection en temps réel si la protection a été complètement désactivée ou suspendue. Cette commande lance également n'importe lequel des composants de protection dont le fonctionnement a été interrompu depuis l'interface graphique ou via la commande `PAUSE` de la ligne de commande. Si le composant a été arrêté depuis l'interface de l'application ou via la commande `STOP` de la ligne de commande, il ne sera pas lancé via la commande `avp.com START` **<**`profil`**>** où <profil> est remplacé par la valeur pour un composant particulier de la protection, par exemple `avp.com START FM`.
FM	Antivirus de fichiers
EM	Antivirus de courrier électronique
WM	Antivirus Internet Valeurs pour les sous-composants d'Antivirus Internet: **httpscan** – analyse du trafic http ; **sc** – analyse des scripts.
BM	Défense proactive

	Analyse pour les sous-composants de la Défense proactive : **og** – analyse des macros de Microsoft Office; **pdm** – analyse de l'activité de l'application.
UPDATER	Mise à jour
Rollback	Remise à l'état antérieur à la dernière mise à jour
SCAN_OBJECTS	Tâche "Analyse"
SCAN_MY_COMPUTER	Tâche "Mon poste de travail"
SCAN_CRITICAL_AREAS	Tâche "Secteurs critiques"
SCAN_STARTUP	Tâche "Objets de démarrage"
SCAN_QUARANTINE	Analyse des objets en quarantaine
SCAN_ROOTKITS	Recherche des outils de dissimulation d'activité
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
```

Afin d'afficher l'état actuel de la défense proactive de votre ordinateur, saisissez dans la ligne de commande:

```
avp.com STATUS BM
```

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>
```

16.3. 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 16.1, page 217). 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	boîtes aux lettres.

/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	Confirmation de l'action par l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmation de l'action par 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 boîtes aux lettres.
-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) dépasse la valeur indiquée 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 **<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 boîtes aux lettres 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
```

16.4. Mise à jour du logiciel

La commande de mise à jour des modules des bases et des modules de Kaspersky Anti-Virus possède la syntaxe suivante :

```
avp.com UPDATE [<source_des_mises_à_jour>]
[/R[A]:<fichier_de_rapport>] [/C:<nom_de_fichier>]
[/APP=<on|off>]
```

Description des paramètres:

[<source_de_mise_à_jour>]	Serveur HTTP, serveur FTP pour répertoire de réseau pour le chargement de la mise à jour. Ce paramètre peut prendre comme valeur le chemin d'accès complet à la source de la mise à jour ou l'URL. Si le chemin d'accès n'est pas indiquée, 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_de_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de l'application lors de la mise à jour. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de Kaspersky Anti-Virus qui seront utilisées.
/APP=<on|off>	Activer/désactiver la mise à jour des modules de l'application

Exemples :

Mettre à jour les bases de Kaspersky Anti-Virus, 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=on /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

16.5. 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>
```

16.6. Exportation des paramètres de la protection

Syntaxe de la commande :

```
avp.com EXPORT <profil> <nom_de_fichier >
```

Description des paramètres:

<profil>	Composant ou tâche dont les paramètres sont exportés. Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point 16.2 à la page 217.
<nom_de_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*) 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*, ce fichier peut être utilisé uniquement pour consulter les paramètres principaux de fonctionnement de l'application.

Exemples :

```
avp.com EXPORT c:\ settings.cfg
```

16.7. Importation des paramètres

Syntaxe de la commande :

```
avp.com IMPORT <nom_de_fichier>
[/password=<votre_mot_de_passe>]
```

<nom_de_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.
<votre_mot_de_passe>	Mot de passe de Kaspersky Anti-Virus défini via l'interface utilisateur.

Cette commande ne pourra être exécutée sans la saisie du mot de passe.

Exemple :

```
avp.com IMPORT c:\ settings.dat
/password=<mot_de_passe>
```

16.8. Lancement de l'application

Syntaxe de la commande :

```
avp.com
```

16.9. Arrêt 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.

Cette commande ne pourra être exécutée sans la saisie du mot de passe.

16.10. 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>]
```

Description des paramètres:

[on|off]	Active/désactive la création d'un fichier de trace.
[file]	Recevoir la trace dans un fichier.
<niveau_de_trace>	Pour ce paramètre, il est possible de saisir un chiffre compris entre 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
```

16.11. 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 command particulière, vous pouvez utiliser une des commandes suivantes :

```
avp.com <commande> /?
avp.com HELP <commande>
```

16.12. 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 17. 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 17.1, p. 232) ;
- au départ de la ligne de commande (cf. point 17.2, p. 234)

17.1. 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.

La modification de la composition vous permet d'installer les composants manquants de Kaspersky Anti-Virus ou de supprimer ceux qui gênent votre travail ou qui sont inutiles.

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 toujours dans cette source et que vous y avez accès.
2. Sélectionnez **Démarrez → Programmes → Kaspersky Anti-Virus 7.0 → 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. Sélection de l'opération

Vous devez d'abord définir 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 6. , p. 32) 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.

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* : fichier de licence du programme.
- *Bases de l'application* : toutes les signatures des programmes dangereux, des virus et des autres menaces qui datent de la dernière mise à jour.
- *Objets du dossier de sauvegarde* : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure.
- *Objets de la quarantaine* : objets qui sont peut-être modifiés par des virus ou leur modification. Ces objets contiennent un code semblable au code d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des bases de l'application.
- *Paramètres de la protection* : valeurs des paramètres de fonctionnement de tous les composants du logiciel.
- *Données iSwift* : base contenant les informations relatives aux objets analysés dans le système de fichiers NTFS. Elle permet d'accélérer l'analyse des objets. Grâce à cette base, Kaspersky Anti-Virus analyse uniquement les objets qui ont été modifiés depuis la dernière analyse.

Attention.

Si un laps de temps important s'est écoulé 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 2. 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**.

17.2. Procédure de suppression de l'application via la ligne de commande

Pour supprimer Kaspersky Anti-Virus 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 17, p. 232).

Pour supprimer l'application en mode caché sans redémarrage de l'ordinateur (le redémarrage devra être réalisé manuellement après l'installation), saisissez :

```
msiexec /x <nom_du_paquetage> /qn
```

CHAPITRE 18. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquentes des utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Anti-Virus. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : Kaspersky Anti-Virus 7.0 peut-il être utilisé simultanément avec les logiciels d'autres éditeurs ?

Afin d'éviter tout risque de conflit, nous vous conseillons de supprimer les logiciels antivirus d'éditeurs tiers avant d'installer Kaspersky Anti-Virus.

Question : Kaspersky Anti-Virus n'analyse pas le fichier une deuxième fois. Pourquoi ?

En effet, Kaspersky Anti-Virus ne procèdera pas à une nouvelle analyse d'un fichier si ce dernier n'a pas été modifié depuis la dernière analyse.

Et cela, grâce aux nouvelles technologies iChecker et iSwift. Ces technologies reposent sur l'utilisation d'une base de données des sommes de contrôle des objets et la conservation des sommes de contrôle dans les flux NTFS complémentaires.

Question : a quoi sert l'activation de l'application? Kaspersky Anti-Virus fonctionnera-t-il sans fichier de licence ?

Kaspersky Anti-Virus peut fonctionner sans licence, mais dans ce cas la mise à jour de l'application et le service d'assistance technique seront inaccessibles.

Si vous n'avez pas encore pris la décision d'acheter Kaspersky Anti-Virus, nous pouvons vous transmettre une licence d'évaluation qui sera valide deux semaines ou un mois. Une fois la durée de validité écoulée, la licence sera bloquée.

Question : depuis l'installation de Kaspersky Anti-Virus, l'ordinateur a un comportement bizarre (« écran bleu », redémarrage constant, etc.) Que faire ?

Une telle situation est rare mais peut se produire en cas d'incompatibilité entre Kaspersky Anti-Virus et un autre programme installé sur votre ordinateur.

Pour rétablir le bon fonctionnement de votre système d'exploitation, suivez ces instructions :

1. Appuyez sur **F8** au tout début du démarrage de l'ordinateur jusqu'à ce que le menu de sélection du mode de démarrage apparaisse.
2. Sélectionnez le point **Mode sans échec** et chargez le système d'exploitation.
3. Lancez Kaspersky Anti-Virus.
4. Sélectionnez la section **Service** dans la fenêtre de configuration de l'application.
5. Désélectionnez la case **Lancer le programme au démarrage de l'ordinateur** et cliquez sur **OK**.
6. Redémarrer le système d'exploitation en mode normal.

Consultez ensuite nos solutions en ligne pour résoudre votre souci. Pour ce faire, ouvrez la fenêtre principale de l'application et sélectionnez la rubrique **Assistance technique** où vous cliquerez sur le lien Accès direct aux FAQs.

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. Ces fichiers seront également analysés par l'Antivirus Courrier si ils sont repris dans le filtrages des objets joints aux messages électroniques :

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 de 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, par exemple, *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, png : 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 d'un 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 :

1. 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*

2. 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**.

3. 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 le type de la menace à exclure selon l'encyclopédie des virus est indiqué. Dans ce cas, la menace indiquée ne sera pas identifiée dans les objets. L'utilisation de ces menaces sans indication du type de menace 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 en fonction de la classification de l'encyclopédie des virus

Pour ajouter des menaces d'un statut particulier conformément à la classification de l'encyclopédie des virus en guise d'exclusion, 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.

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. Nos bases sont actualisées 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 zone de notification de la barre des tâches de Microsoft Windows ;
- 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® 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://support.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/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/DVD 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/DVD, 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 licence 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/DVD-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 Il est interdit de transmettre le code d'activation et le fichier de clé de licence à un tiers. Le code d'activation et le fichier de clé de licence sont des informations strictement confidentielles.

1.1.7 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 posses-

sion, 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 œuvre 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/DVD-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.