KASPERSKY LAB

Kaspersky Anti-Virus® 6.0

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS® 6.0

Manuel de l'utilisateur

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

http://www.kaspersky.fr/

Date d'édition: janvier 2007

Sommaire

CHAPITRE 1. MENACES SUR LA SECURITE INFORMATIQUE

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

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

Les grandes entreprises ne sont pas les seules 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 un serveur, 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 d'une page 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

Cette catégorie regroupe les applications qui n'ont pas de fonctions malveillantes mais qui peuvent faire partie du milieu de développement de codes malveillants ou être utilisées par un individu mal intentionné à titre d'assistant pour un programme malveillant. Cette catégorie de programme contient par exemple des programmes avec des vulnérabilités et des failles, 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 rootkits modifient le système d'exploitation de l'ordinateur et remplacent ses fonctions fondamentales afin de dissimuler sa propre présence et les actions exécutées par l'individu mal intentionné sur l'ordinateur infecté.

Autres programmes dangereux

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

Attaques de pirates informatiques

Les attaques de pirates informatiques sont le fait d'individus mal intentionnés ou de programmes malveillants qui veulent s'emparer

d'informations sauvegardées sur l'ordinateur de la victime, mettre le système hors service ou obtenir un contrôle total sur les ressources de l'ordinateur. Vous trouverez une description détaillées des attaques bloquées par Kaspersky Anti-Virus dans la section Liste des attaques de réseau découvertes.

Certains types d'escroquerie via Internet

Le **phishing** est un type d'escroquerie en ligne qui consiste à diffuser un message électronique visant à voler des informations confidentielles, à caractère financier dans la majorité des cas. Un message de phishing doit ressembler le plus possible à un message que pourrait envoyer une banque ou une entreprise connue. Le message contient un lien vers un site fictif créé spécialement par l'individu mal intentionné et qui est une copie conforme du site de l'organisation prétendument à l'origine du message. Une fois qu'elle arrive sur ce site, la victime est invitée à saisir, par exemple, son numéro de carte de crédit ou d'autres informations confidentielles.

La n**umérotation vers un site Internet payant** est un type d'escroquerie qui repose sur l'utilisation non autorisée de sites Internet payants (bien souvent, des sites à contenu pornographique). Les programmes installés par l'individu mal intentionné (les dialers) ouvrent une connexion par modem entre votre ordinateur et le numéro payant. Dans la majorité des cas, le tarif de cet appel est très élevé, ce qui se traduit par une lourde facture de téléphone pour l'utilisateur.

Publicités envahissantes

Il s'agit des fenêtres pop up et des bannières qui apparaissent lorsque vous visitez un site Internet quelconque. En règle générale, les informations présentées n'ont aucun intérêt. Les fenêtres pop up et les bannières distraient l'utilisateur et augmentent le volume de trafic.

Courrier indésirable

Il s'agit de l'envoi anonyme de messages non sollicités. On peut ranger dans cette catégorie les messages publicitaires, les messages à caractères politique ou de propagande, les messages qui vous invitent à venir en aide à une personne quelconque, etc. Il existe une catégorie spéciale de messages non sollicités qui reprend les propositions pour obtenir des quantités importantes d'argent ou qui invitent le destinataire à participer à une pyramide. Il ne faut pas oublier les messages qui visent à voler les mots de passe, les messages dont le contenu doit être transmis à vos amis (les chaînes), etc. Le courrier indésirable augmente considérablement la charge des serveurs de messagerie et le risque de perte d'informations cruciales pour l'utilisateur.

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 d'une base des signatures des menaces qui est actualisée en permanence. Cette méthode requiert au moins une infection pour ajouter la signature de la menace dans la base 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) selon les paramètres définis par les experts de Kaspersky Lab dès qu'ils se manifestent.

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 et de se faire du soucis inutilement.
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 signatures des menaces (cf. point 5.6, p. 57) et les modules de l'application. 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 les 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. 57) régulièrement les signatures des menaces livrées avec le logiciel. Réalisez cette opération plusieurs fois par jour en cas d'épidémie (les bases antivirus 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. 56) (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 signatures des menaces 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 et les disquettes d'installation ainsi que tout média contenant des logiciels et des informations de valeur.
- Créez un disque de secours (cf. point 14.10, p. 197) 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 point **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 6.0

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

Ce qui différencie Kaspersky Anti-Virus 2006 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 6.0

Kaspersky Anti-Virus 6.0 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 les menaces inconnues.

Il n'est plus indispensable d'installer plusieurs logiciels afin d'assurer la sécurité complète. Il suffit simplement d'installer Kaspersky Anti-Virus 6.0.

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 2006.

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. 116) constitue le principal avantage du logiciel. Il analyse le comportement des applications installées, est à l'affût de changement dans la base de registre, surveille l'exécution des macros et lutte contre les menaces dissimulées. Le composant 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 réalisées par le programme malveillant 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 : il est désormais possible de réduire la charge sur le processeur central et les sous-systèmes de disque et d'augmenter la vitesse de l'analyse des fichiers. Ce résultat est obtenu grâce au recours aux technologies iChecker ™ et iSwift ™. Ainsi, l'application évite les analyses répétées d'un même fichier.
- 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, ceux dont l'infection entraînerait des conséquences irréversibles, est reprise dans une tâche séparée. Vous pouvez configurer cette tâche de telle sorte qu'elle soit lancée automatiquement à chaque démarrage du système.
- La protection du courrier sur l'ordinateur de l'utilisateur contre les programmes malveillants a été considérablement améliorée. Le logiciel analyse n'importe quel message dans le flux de messagerie des protocoles suivants :
    - IMAP, SMTP et POP3 quel que soit le client de messagerie utilisé ;
    - NNTP, 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 dans le système de messagerie ont été intégrés aux clients de messagerie les plus connus comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- Elargissement de la fonction de notification de l'utilisateur (cf. point 14.11.1, p. 201) lorsque des événements définis se produisent pendant l'utilisation du logiciel. Vous pouvez choisir le mode de notification pour chaque type d'événement : courrier électronique, avertissement sonore, infobulle, consignation dans le journal des événements.
- Analyse du trafic transitant sur les connexions sécurisées via SSL.

- Ajout de la technologie d'autodéfense du logiciel, de protection contre l'administration non autorisée à distance du service 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.

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, joint des commentaires et des conseils à ses actions et offre une rubrique d'aide détaillée.

Nouveautés au niveau de la mise à jour du programme

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

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

La protection offerte par Kaspersky Anti-Virus 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 chaque composant en fonction des besoins d'un utilisateur particulier ou de l'entreprise dans son ensemble.

Kaspersky Anti-Virus comprend :

Des composants de protection (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.

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

La protection en temps réel de l'ordinateur est assurée par les composants 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, EXECUTES et ENREGISTRES sur l'ordinateur et tous les disques connectés. Chaque fichier sollicité sera intercepté par Kaspersky Anti-Virus et soumis à une analyse antivirus pour trouver des virus connus. 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 14.2, p. 176)ou mis en quarantaine (cf. point 14.1, p. 172).

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, regroupes les propriétés de divers types et les méthodes de diffusion 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 dangereux potentiellement 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 raison d'un niveau de protection trop bas ou de tout autre motif.

Kaspersky Anti-Virus contient trois tâches 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 *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.

Les experts de Kaspersky Lab recommande d'exécuter ces tâches au moins une fois par semaine.

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 bases de messagerie une fois par semaine ou une tâche pour la recherche d'éventuels virus dans le répertoire **Mes documents**.

2.2.3. Services du programme

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

Mise à jour

Afin d'être toujours prêt à neutraliser tout virus ou programme malveillant, à intercepter le courrier indésirable, il faut veiller à ce que Kaspersky Anti-Virus soit toujours à jour. Le composant *Mise à jour* a été conçu à cette fin. Il assure la mise à jour des signatures des menaces et des modules internes de Kaspersky Anti-Virus utilisés.

La copie des mises à jour permet de sauvegarder la mise à jour des signatures de menaces, des pilotes de réseau et des modules de

l'application depuis les serveurs de Kaspersky Lab dans un répertoire local afin de les rendre accessibles aux autres ordinateurs du réseau dans le but de réduire le trafic Internet.

Rapport

Un rapport est généré pendant l'utilisation du programme pour 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.

Disque de secours

Kaspersky Anti-Virus propose un service spécial qui permet de créer un disque de secours pour restaurer le système.

La création d'un tel disque est utile lorsque les fichiers système ont été endommagés par une attaque de virus et qu'il est impossible de charger le système d'exploitation. Dans ce cas, grâce au disque de secours, vous pourrez démarrer l'ordinateur et restaurer le système à son état antérieur à l'infection.

Assistance technique

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

A l'aide des liens prévus à cet effet, vous pouvez accéder au forum des utilisateurs des logiciels de Kaspersky Lab, consulter la liste des

questions fréquemment posées où vous trouverez peut-être la solution à votre problème. De plus, vous pouvez contacter directement le service d'assistance technique en remplissant un formulaire en ligne afin de signaler une erreur ou de transmettre des commentaires sur le fonctionnement du logiciel.

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

2.3. Configurations matérielle et logicielle

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

Configuration générale :

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

*Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a***):**

- Liaison Internet active pour les mises à jour des bases antivirales
- Processeur Intel Pentium 300 Mhz ou supérieur.
- 64 Mo de mémoire vive disponible.

Microsoft Windows 2000 Professional (Service Pack 2 ou suivant), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 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® 6.0 chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr – rubrique **Boutique en ligne / Particuliers**).

Le pack logiciel en boite contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés
- 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 33 caractères (exemple de format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) imprimé sur le manuel d'utilisation ou la pochette du CD-Rom
    - sur le CDROM 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® 6.0 en ligne, et dés la réception de votre paiement, vous recevrez un email contenant des liens personnels pointant 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 6.0

Kaspersky Anti-Virus peut être installé partiellement ou complètement.

En cas d'installation partielle, vous pouvez sélectionner les composants à installer. Libre à vous d'installer par la suite les autres composants, mais vous devrez pour ce faire utiliser le fichier d'installation original. Pour cette raison, il est conseillé de copier le fichier de l'installation du logiciel sur le disque dur.

Vous pouvez installer l'application à l'aide d'un des moyens suivants :

- à l'aide de l'assistant d'installation (cf. point 3.1, p. 30) ;
- au départ de la ligne de commande (cf. point 3.3, p. 40) ;
- via Kaspersky Administration Kit (cf. "Manuel de déploiement de Kaspersky Administration Kit").

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

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

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

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

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

- **Suivant :** confirme l'action et passe au point suivant dans le processus d'installation.
- **Précédent** : revient au point précédent dans l'installation.

- **Annuler** interrompt l'installation.
- **Terminer** conclut l'installation du logiciel sur l'ordinateur.

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

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

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

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

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

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

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

Etape 3. Examen du contrat de licence

Cette fenêtre reprend le contrat de licence 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.

Etape 4. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le répertoire dans lequel vous souhaitez installer Kaspersky Anti-Virus. Il s'agit par défaut de : **<Disque>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0**.

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

Si vous saisissez le nom 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 5. Choix du type d'installation

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

Complète. Tous les composants de Kaspersky Anti-Virus seront installés sur votre ordinateur. Pour voir la suite de l'installation, consultez l'Etape 5.

Personnalisée. Dans ce cas, vous pouvez sélectionner les composants que vous souhaitez installer. Pour de plus amples informations, consultez l'Etape 6

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

Etape 6. Sélection des composants à installer

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

Lorsque vous décidez de réaliser une installation personnalisée, vous devez composer la liste des composants de Kaspersky Anti-Virus que vous souhaitez installer. Par défaut, les composants de la protection et le composant de recherche de virus sont sélectionnés.

Si vous ne souhaitez pas installer un composant, sélectionnez le point **Le composant ne sera pas accessible** 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. Recherche d'autres logiciels antivirus éventuellement installés

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

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

En dessous de la liste des logiciels antivirus découverts, vous pourrez décider de les supprimer automatiquement ou manuellement.

Si Kaspersky Anti-Virus Personal ou Kaspersky Anti-Virus Personal Pro figurent parmi cette liste, il est conseillé de conserver les clés de licence utilisées par ces logiciels avant de les supprimer. Vous pourrez en effet les utiliser en tant que clé pour Kaspersky Anti-Virus 6.0. 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.

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

Etape 8. Préparation finale pour l'installation de l'application

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 signatures des menaces si ceux-ci ont été enregistrés sur l'ordinateur lors de la suppression de la version antérieure de Kaspersky Anti-Virus (par exemple, vous aviez installé la version bêta et vous installez maintenant la version commerciale).

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 signatures des menaces, vous pourrez les utiliser avec la version que vous installer. Pour ce faire, cochez la case ☑ **Signatures des menaces.** Les signatures des menaces 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**.

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

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

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

Etape 9. 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 2006 est lancé à la fin de la procédure d'installation du logiciel. Son rôle est de vous aider à réaliser la configuration initiale du logiciel sur la base des particularités et des tâches de votre ordinateur.

L'interface de l'Assistant de configuration se présente sous la forme d'un Assistant 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

3.2.1. Utilisation des objets sauvegardés de la version 5.0

Cette fenêtre de l'Assistant s'affiche lors de l'installation sur la version 5.0 de Kaspersky Anti-Virus. Vous devrez choisir les données utilisées par la version 5.0 qui devront être transmises dans la version 6.0. Il peut s'agir d'objets en quarantaine, dans le dossier de sauvegarde ou de paramètres de la protection.

Pour utiliser ces données avec la version 6.0, cochez les cases adéquates.

3.2.2. Activation du logiciel

La procédure d'activation du logiciel consiste à installer la licence que Kaspersky Anti-Virus utilisera pour confirmer la présence d'une licence et sa durée de validité.

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

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

Attention !

Activer le logiciel maintenant (requiert l'accès à Internet) Si vous n'êtes pas connecté à Internet au moment de l'installation, vous pouvez réaliser l'activation plus tard au départ de l'interface du logiciel (cf. point 14.5, p. 188).

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, la licence commerciale s'activera automatiquement pour toute sa durée de validité.
- **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 clé de licence gratuite dont la validité est limitée par la licence pour la version d'évaluation de l'application .
- **Utiliser votre clé de licence acquise antérieurement non expirée**. Sélectionnez cette option si vous possédez déjà une clé de licence valide pour ce logiciel Kaspersky .
- **Activer l'application plus tard**. Sélectionnez cette option si vous êtes en attente de votre licence commerciale. L'activation du logiciel sera reportée à plus tard. Ce logiciel Kaspersky sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser les signatures des menaces une fois que vous aurez activé le logiciel au moyen d'un des trois points précédents).

En cas de sélection des deux premières options, l'activation de l'application est réalisée via le serveur Web de Kaspersky Lab, ce qui requiert un accès à

Internet. Avant de lancer la procédure d'activation, vérifiez et, le cas échéant, modifiez les paramètres de connexion au réseau (cf. point 13.4.3, p. 166) dans la fenêtre qui s'ouvre à l'aide du bouton **Paramètres LAN**. Pour obtenir de plus amples informations sur la configuration des paramètres de réseau, contactez votre administrateur système ou votre fournisseur d'accès Internet.

3.2.2.2. Saisie du code d'activation

Saisissez le code d'activation que vous avez reçu à l'achat du logiciel.

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

3.2.2.3. Principe d'activation de la licence par le code d'activation

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, le logiciel s'activera automatiquement pour la durée de la licence

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

3.2.2.4. Principe d'activation de la licence par le fichier de licence

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

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

3.2.2.5. Fin de l'activation du logiciel

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

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 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 le monitorage de la base de registres 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 défense 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 signatures des menaces et des modules du logiciel. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de mise à jour de logiciel et de la programmer :

- **Automatique**. Kaspersky Anti-Virus vérifie 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 jours à 15h30** (l'intervalle peut varier en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.
- **Manuel**. Vous lancez vous-même la procédure de mise à jour du logiciel.

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

Si vous souhaitez passer à la configuration des paramètres de la mise à jour (sélectionner les paramètres de réseau, sélectionner la ressource au départ de laquelle la mise à jour sera réalisée, indiquer le serveur de mise à jour le plus proche de votre emplacement), 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 au logiciel

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

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

Indiquez ensuite les tâches qui seront concernées :

- **Toutes les opérations (sauf les alertes)**. Le mot de passe est nécessaire pour lancer n'importe quelle action du logiciel à l'exception de la manipulation des messages relatifs à la découverte d'objets dangereux.
- **Sélectionnez les actions protégées par un mot de passe:**

- **Enregistrement des paramètres de fonctionnement de l'application** : le mot de passe est requis lorsque l'utilisateur tente d'enregistrer les modifications apportées aux paramètres du logiciel.
- **Quitter le logiciel** : le mot de passe est requis pour quitter le logiciel.
- **Arrêt/pause des composants de la protection et des tâches de recherche de virus** : le mot de passe est requis pour suspendre ou arrêter n'importe quel composant ou n'importe quelle tâche liée à la recherche de virus.

3.2.7. 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 correct 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 6.0, 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.

Vous pouvez également avoir recours à une des méthodes suivantes pour l'installation de l'application.

Pour installer l'application en mode caché sans redémarrage de l'ordinateur (le redémarrage devra être réalisé manuellement après l'installation), saisissez :

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

Pour installer l'application en mode caché avec redémarrage de l'application, saisissez :

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

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

Si vous utilisez déjà Kaspersky Anti-Virus 5.0 Personal ou Kaspersky Anti-Virus 5.0 Personal Pro, vous pouvez réaliser une mise à niveau jusque Kaspersky Anti-Virus 6.0.

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

Attention !

Lors de la mise à niveau de la version 5.0 à la version 6.0 de Kaspersky Anti-Virus au départ d'un répertoire de réseau dont l'accès est protégé par un mot de passe, la version 5.0 sera supprimée et l'ordinateur redémarrera sans installer la version 6.0 de l'application. Cela s'explique par le fait que le programme d'installation ne jouit pas des privilèges d'accès au répertoire de réseau. Afin de résoudre ce problème, lancez l'installation uniquement depuis une ressource locale.

CHAPITRE 4. INTERFACE DU LOGICIEL

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

- L'icône de la barre des tâches (cf. point 4.1, p. 42);
- Le menu contextuel (cf. point 4.2, p. 43);
- La fenêtre principale (cf. point 4.3, p. 44);
- Fenêtre de configuration des paramètres du logiciel (cf. point 4.4, p. 47).

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

- Microsoft Office Outlook (cf. point 8.2.2, p. 100).
- Microsoft Outlook Express.
- TheBat! (cf. point 8.2.3, p. 102).
- Microsoft Internet Explorer.
- Microsoft Windows Explorer (cf. point 11.2, p. 139).

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 de la barre des tâches

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

Cette icône est un indicateur du fonctionnement de Kaspersky Anti-Virus. Elle reflète l'état de la protection et illustre également diverses tâches fondamentales exécutées par l'application.

Si l'icône est activée  (en couleur), cela signifie que la protection de l'ordinateur est activée. Si l'icône n'est pas activée  (noir et blanc) cela signifie que la protection est désactivée ou que certains des 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 signatures des menaces et des modules logiciels de Kaspersky Anti-Virus est en cours.
- Une erreur s'est produite dans un des composants de Kaspersky Anti-Virus.

L'icône donne également accès aux éléments principaux de l'interface du logiciel : le menu contextuel (cf. point 4.2, p. 43) et la fenêtre principale (cf. point 4.3, p. 44);

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

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

4.2. Menu contextuel

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

Illustration 1. Menu contextuel

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

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

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

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

Activation : passe à l'activation du logiciel. 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. 44).

Suspension de la protection/Activation de la protection : désactive temporairement/active le fonctionnement des composants de la protection (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.

Quitter : quitte Kaspersky Anti-Virus.

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 deux panneaux :

- Le panneau de gauche est réservé à la *navigation*. Il permet de passer rapidement et simplement à n'importe quel composant, de lancer les recherches de virus et d'accéder aux services du logiciel;
- Le panneau de droite est à caractère *informatif* : il contient les informations relatives au composant sélectionné dans le panneau de gauche, permet d'accéder à la configuration de chacun d'entre eux,

propose les instruments pour l'exécution de la recherche des virus, la manipulation des fichiers en quarantaine et des copies de réserve, la gestion des clés de licence, etc.

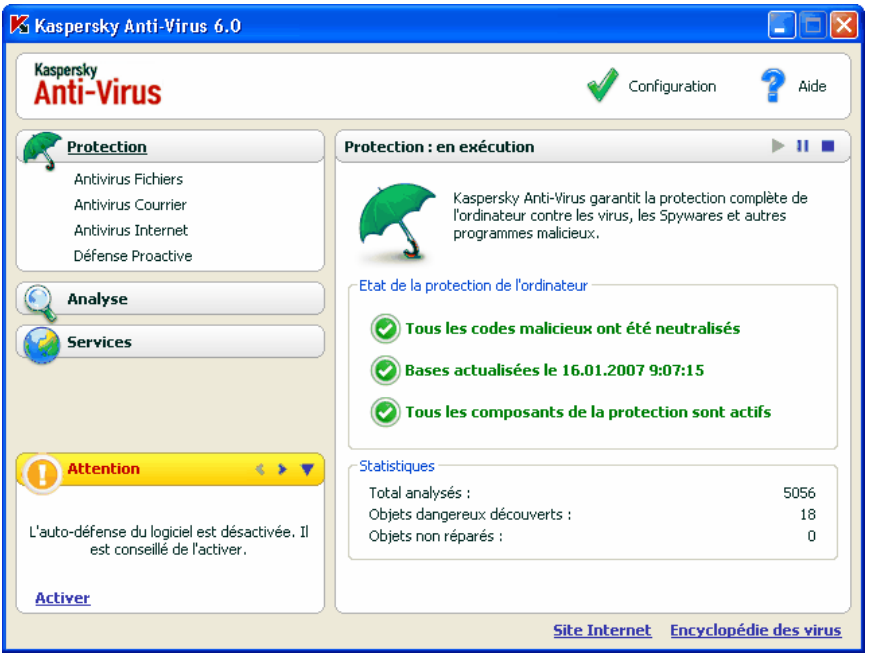
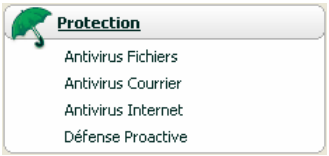
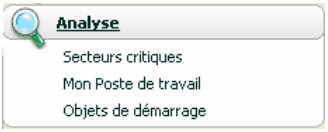


Illustration 2. Fenêtre principale de Kaspersky Anti-Virus

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 tâche principale de cette fenêtre est de vous informer sur l'état de la protection de votre ordinateur. La section **Protection** est prévue précisément à cette fin. 	Pour consulter les informations générales sur le fonctionnement de Kaspersky Anti-Virus, les statistiques de fonctionnement du logiciel, vérifier le bon fonctionnement de tous les composants, sélectionnez la section **Protection** dans le panneau de navigation. Pour consulter les paramètres d'un composant concret d'un composant, il suffit de sélectionner le nom du composant au sujet duquel vous souhaitez obtenir des informations dans la section **Protection**.
La section **Recherche de virus** est prévue pour la recherche d'objets malveillants. 	Cette section contient la liste des objets que vous pouvez soumettre individuellement à l'analyse antivirus. Les tâches qui, selon les experts de Kaspersky Lab, vous seront les plus utiles sont reprises dans cette section. Il s'agit de la recherche de virus dans les secteurs critiques, parmi les objets de démarrage ainsi que l'analyse complète de l'ordinateur.
La section **Services** contient les fonctions complémentaires de Kaspersky Anti-Virus. 	Vous pouvez passer à la mise à jour du logiciel, à la consultation des rapports sur le fonctionnement de n'importe quel composant de Kaspersky Anti-Virus, à la manipulation des objets en quarantaine ou des copies de sauvegarde, à la création d'un disque de secours ou à la fenêtre d'administration des clés de licence.

Section du panneau de navigation de la fenêtre principale	**Fonction**
La section **Commentaires et conseils** vous accompagne tout au long de l'utilisation du logiciel 	Cette section vous offrira toujours des conseils pour renforcer la protection de l'ordinateur. C'est ici que vous trouverez également les commentaires sur le fonctionnement actuel du logiciel et sur ces paramètres. Grâce aux liens repris dans cette section, vous pouvez accéder directement à l'exécution de l'action recommandée dans un cas concret ou en savoir plus sur les informations.

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

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

4.4. Fenêtre de configuration des paramètres du logiciel

La fenêtre de configuration des paramètres de Kaspersky Anti-Virus peut être ouverte depuis la fenêtre principale (cf. point 4.3, p. 44). Pour ce faire, cliquez sur le lien Configuration dans la partie supérieure.

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 du logiciel, des tâches liées à la recherche de virus 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.

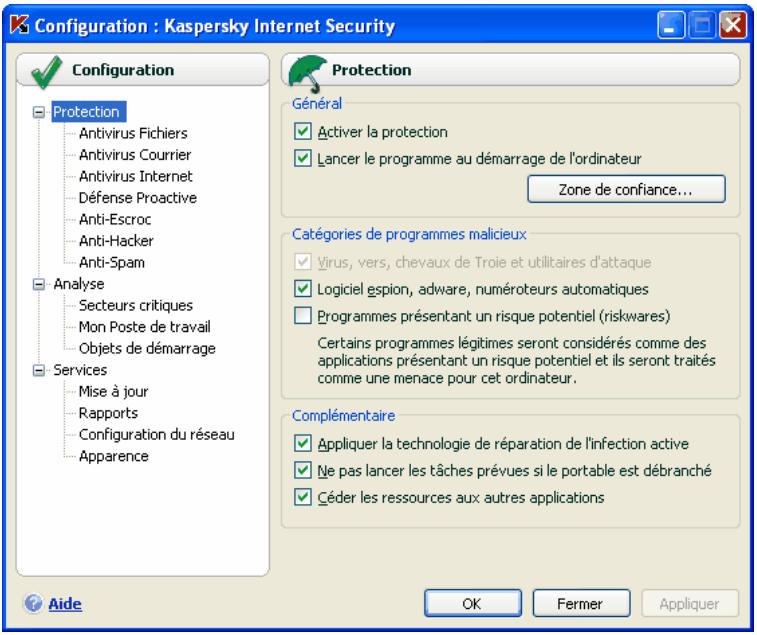


Illustration 3. Fenêtre de configuration de Kaspersky Anti-Virus

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. 34). 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 et 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. 49) 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. 57).
- Analyser l'ordinateur (cf. point 5.3, p. 55).

5.1. Etat de la protection de l'ordinateur

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

L'**Etat de la protection** illustre l'état actuel de la protection de votre ordinateur à l'aide d'indices spéciaux (cf. point 5.1.1, p. 50). Les statistiques (cf. point 5.1.2, p. 53) affichent les résultats du travail actuel du logiciel.

5.1.1. Indices de protection

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

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

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

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

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

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

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

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

Aucun objet malveillant n'a été découvert

Kaspersky Anti-Virus n'a découvert aucun objet dangereux sur l'ordinateur.

Tous les objets malveillants ont été neutralisés

Kaspersky Anti-Virus a réparé tous les objets infectés et supprimés ceux qu'il n'a pas pu réparer.

Des objets malveillants ont été découverts

Votre ordinateur est actuellement exposé à un risque d'infection. Kaspersky Anti-Virus a découvert des objets malveillants qu'il faut absolument neutraliser. Pour ce faire, cliquez sur Réparer tous. Le lien Détails vous permet d'obtenir de plus amples informations sur les objets malveillants.

Le redémarrage de l'ordinateur est indispensable

Le traitement des objets malveillants requiert le redémarrage de l'ordinateur. Enregistrez et fermez tous les fichiers avec lesquels vous travailliez et cliquez sur Redémarrer l'ordinateur.

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

Les signatures ont été diffusées (date, heure)

Le logiciel n'a pas besoin d'être mis à jour. Toutes les bases utilisées par Kaspersky Anti-Virus contiennent les informations les plus récentes pour la protection de l'ordinateur.

Les signatures sont dépassées

Les modules internes de l'application et les bases de données de Kaspersky Anti-Virus n'ont pas été actualisées depuis quelques jours. Vous risquez d'infecter votre ordinateur avec de nouveaux programmes malveillants apparues depuis la dernière mise à jour de l'application. Il est vivement recommandé de mettre à jour Kaspersky Anti-Virus. Pour ce faire, cliquez sur Mettre à jour.

Le redémarrage de l'ordinateur est indispensable

La mise à jour correcte du logiciel requiert le redémarrage du système. Enregistrez et fermez tous les fichiers avec lesquels vous travailliez et cliquez sur Redémarrer l'ordinateur.

Les signatures sont dépassées

Il y a longtemps que Kaspersky Anti-Virus n'a plus été mis à jour. Vous exposez les données de votre ordinateur à un grand risque. Il faut mettre le logiciel à jour le plus vite possible. Pour ce faire, cliquez sur Mettre à jour.

Les signatures sont complètement ou partiellement corrompues

Les fichiers des signatures des menaces sont complètement ou partiellement corrompus. Il est conseillé de lancer à nouveau la mise à jour. Si l'erreur se reproduit, contactez le service d'assistance technique de Kaspersky Lab.

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

Tous les composants de la protection sont actifs

Tous les vecteurs de propagation des programmes malveillants sont protégés par Kaspersky Anti-Virus Suite. Tous les composants de la protection sont activés.

La protection n'est pas installée

Lors de l'installation de Kaspersky Anti-Virus, aucun des composants de la protection en temps réel n'a été installé. Le présent mode autorise unique la recherche d'éventuels virus dans les objets. Pour garantir la protection maximale de l'ordinateur, il est conseillé d'installer les composants de la protection.

Certains composants de la protection sont inactifs

Le fonctionnement d'un ou de plusieurs composants de la protection a été suspendu pour un certain temps. Afin de rétablir le fonctionnement du composant inactif, sélectionnez-le dans la liste et cliquez sur ▶.

Tous les composants de la protection sont inactifs

La protection de l'ordinateur est complètement désactivée. Aucun de ses composants ne fonctionne. Pour rétablir le fonctionnement des composants, sélectionnez l'élément **Activation de la protection** dans le menu contextuel qui s'ouvre lorsque vous cliquez sur l'icône de l'application dans la barre des tâches.

Certains composants de la protection sont incorrects

Le fonction d'un ou de plusieurs composants de la protection de Kaspersky Anti-Virus s'est soldé par un échec. Il est conseillé dans ce cas d'activer le composant ou de redémarrer l'ordinateur (l'enregistrement des pilotes du composant après l'application d'une mise à jour s'impose peut-être).

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

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

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

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

Examinons la *barre d'état* du composant cité dans l'exemple, à savoir Antivirus Fichiers :

- *Antivirus Fichiers : actif* : la protection des fichiers est assurée selon les paramètres du niveau sélectionné. (cf. point 7.1, p. 82).
- *Antivirus Fichiers : pause* : l'antivirus de fichiers a été désactivé pour un temps déterminé. Le composant sera activé automatiquement une fois ce laps de temps écoulé ou après le redémarrage du logiciel. Vous pouvez activer vous-même la protection des fichiers. Pour ce faire, cliquez sur ▶ dans la barre d'état.
- *Antivirus Fichiers* : *inactif*. L'utilisateur a arrêté le composant. Vous pouvez activer la protection des fichiers. Pour ce faire, cliquez sur ▶ dans la barre d'état.

- *Antivirus Fichiers : ne fonctionne pas*. La protection des fichiers est inaccessible pour une raison quelconque. Par exemple, vous ne possédez pas de licence d'utilisation du logiciel.
- *Antivirus Fichiers : échec*. Le composant s'est arrêté suite à un échec. Dans ce cas, contactez le service d'assistance technique de Kaspersky Lab.

Si le composant contient plusieurs modules, la section **Etat** vous renseigne sur l'état du fonctionnement : sont-ils actifs ou pas. Pour les composants qui ne possèdent pas de modules distincts, vous verrez leur propre état, le niveau de protection offert et, pour certains composants, les actions exécutées sur les objets dangereux.

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

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

5.1.3. Statistiques

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

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

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

- des informations sur les objets découverts (cf. point 14.3.2, p. 182) et le statut qui leur a été attribué;
- le journal des événements (cf. point 0, p. 182);
- des statistiques générales sur l'analyse de l'ordinateur (cf. point 14.3.4, p. 184);

- les paramètres de fonctionnement du logiciel (cf. point 14.3.5, p. 184).

Si la recherche de virus est en cours à ce moment, le groupe **Statistiques** affiche une barre de progression de l'analyse.

5.2. 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.

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

Après avoir sélectionné la tâche **Mon poste de travail** dans la partie gauche de la fenêtre principale, vous pouvez consulter les statistiques de la dernière analyse et les paramètres de la tâche : le niveau de protection sélectionnée et l'action exécutée sur les objets dangereux.

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

cliquez sur **Analyser** dans la partie droite de la fenêtre.

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 **Recherche de virus** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Secteurs critiques** dans la partie gauche de la fenêtre principale, vous pouvez consulter les statistiques de la dernière analyse et 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 :

cliquez sur **Analyser** dans la partie droite de la fenêtre.

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. 6).

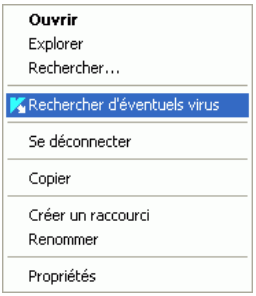


Illustration 6. Recherche d'éventuels virus dans un objet sélectionné à l'aide des outils Windows

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 signatures des menaces et les modules interne 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 la dernière version des mises à jour, Kaspersky Anti-Virus les télécharge et les installe en arrière plan.

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

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

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

5.7. 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 16, p. 224).

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 ou de toute l'application afin de pouvoir fournir aux opérateurs du service d'assistance technique toutes les informations dont ils ont besoin.

Afin d'enregistrer le rapport dans un fichier :

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

Afin d'enregistrer directement le rapport de tous les composants de Kaspersky Anti-Virus (composants de la protection, tâches de recherche de virus, fonctions de services),

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

   ou

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

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

CHAPITRE 6. ADMINISTRATION COMPLEXE DE LA PROTECTION

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

- Désactivation/activation du logiciel (cf. point 6.1, p. 60).
- Sélection des logiciels contrôlés contre lesquels Kaspersky Anti-Virus vous protégera (cf. point 6.2, p. 65).
- Constitution de la liste des exclusions pour la protection (cf. point 6.3, p. 66).
- Création de tâches personnalisées de recherche de virus et de mise à jour (cf. point 6.4, p. 75).
- Configuration du lancement des tâches à l'heure qui vous convient (cf. point 6.5, p. 77).
- Configuration des paramètres de performance (cf. point **6.6**, p. 79) de la protection de l'ordinateur.

6.1. Désactivation/activation de la protection de votre ordinateur

Par défaut, Kaspersky Anti-Virus est lancé au démarrage du système comme en témoigne le message *Kaspersky Anti-Virus 6.0* qui apparaît dans le coin supérieur droit de l'écran. La protection est garantie pendant toute la séance de travail. Tous les composants de la protection 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** 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 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 Kaspersky Anti-Virus :

1. Sélectionnez **Suspension de la protection** dans le menu contextuel (cf. point 4.2, p. 43)
2. Dans la fenêtre de désactivation (cf. ill. 7), sélectionnez la durée au terme de laquelle la protection sera réactivée :
   - **Dans <intervalle de temps>** : la protection sera activée au terme de l'intervalle indiqué. Pour sélectionner la valeur, utilisez la liste déroulante.
   - **Après le redémarrage du logiciel :** la protection sera activée si vous lancez le programme depuis le menu **Démarrer** ou après le redémarrage du système (pour autant que le lancement du programme au démarrage de l'ordinateur (cf. point 6.1.5, p. 64).
   - **Uniquement à la demande de l'utilisateur** : la protection sera activée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Activation de la protection** dans le menu contextuel du programme.

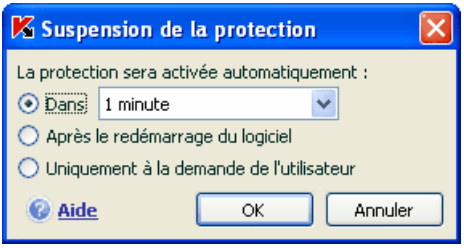


Illustration 7. Fenêtre de suspension de la protection de votre ordinateur

Astuce.
Vous pouvez également désactiver la protection de votre ordinateur de l'une des deux méthodes suivantes :

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

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

- Le nom des composants désactivés apparaît en grisé dans la section **Protection** de la fenêtre principale.
- L'icône de l'application dans la barre des tâches est en noir et blanc.
- Le troisième indice de protection (cf. point 5.1.1, p. 50) de votre ordinateur indique *Aucun composant de la protection n'est chargé*.

6.1.2. Désactivation complète de la protection de l'ordinateur

La désactivation complète signifie l'arrêt du fonctionnement des composants de la protection. 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 6.3, p. 66).

Pour désactiver complètement la protection de l'ordinateur :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus.
2. Cliquez sur le Configuration dans la section **Protection**.
3. Dans la fenêtre des paramètres du logiciel, désélectionnez la case **Activer les protections**.

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 inactive dans la barre des tâches est grise.
- L'indice de la protection (cf. point 5.1.1, p. 50) de votre ordinateur indique *Tous les composants de la protection sont inactifs*.

6.1.3. Suspension / désactivation du composant de la protection, de la recherche de virus ou de la mise à jour

Il existe plusieurs moyens de désactiver un composant de la protection ou une tâche liée à la mise à jour ou à la recherche de virus. Toutefois, avant de faire quoi que ce soit, nous vous conseillons de définir la raison pour laquelle vous souhaitez les suspendre. Le problème pourrait également être résolu en modifiant, par exemple, le niveau de protection. Ainsi, si vous utilisez une base de données qui selon vous ne peut contenir de virus, il suffit de reprendre ce répertoire et les fichiers qu'il contient dans les exclusions (cf. point 6.3, p. 66).

Pour suspendre un composant de la protection, la recherche de virus ou la mise à jour

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

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

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

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

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

Dans ce cas, l'état du composant (tâche) devient *désactivé (interrompu)*. La protection assurée par le composant ou la tâche qui était exécutée

sera arrêtée jusqu'à ce que vous la réactiviez en cliquant sur le bouton . Pour la recherche de virus et la mise à jour, vous aurez le choix entre les options suivantes : poursuivre l'exécution de la tâche interrompue ou la reprendre à zéro.

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

6.1.4. Rétablissement de la protection de l'ordinateur

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

- *Au départ du menu contextuel*.

  Sélectionnez le point **Activation la protection**.

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

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

L'état de la protection redevient immédiatement *fonctionne*. L'icône du logiciel dans la barre des tâches redevient active (en couleur). Le troisième indice de protection (cf. point 5.1.1, p. 50) de l'ordinateur indique **Tous les composants de la protection sont actifs**.

6.1.5. Fin de l'utilisation du logiciel

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Anti-Virus, sélectionnez le point **Quitter** dans le menu contextuel (cf. point 4.2, p. 43) 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 6.0 → Kaspersky Anti-Virus 6.0**.

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 **Protection** et cochez la case ☑ **Lancer l'application au démarrage de l'ordinateur**.

6.2. Types de programmes malveillants contrôlés

Kaspersky Anti-Virus vous protège contre divers types de programmes malveillants. Quelle que soit la configuration du programme, les virus, les chevaux de Troie et les utilitaires d'attaque sont toujours décelés et neutralisés. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une plus protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

Afin de sélectionner les types de programmes malveillants contre lesquels Kaspersky Anti-Virus vous protégera, passez à la section **Protection**, de la fenêtre de configuration du logiciel (cf. point 4.4, p. 47).

Les types de menaces (cf. point 1.3, p. 12) figurent dans le bloc **Catégories de programmes malicieux** :

- ☑ **Virus, vers, chevaux de Troie et utilitaires d'attaque**. Ce groupe reprend les programmes malveillants les plus répandus et les plus dangereux. Cette protection est le niveau minimum admissible. Conformément aux recommandations des experts de Kaspersky Lab, Kaspersky Anti-Virus contrôle toujours les programmes malveillants de cette catégorie.
- ☑ **Logiciel espion, Adwares, numéroteurs automatiques**. Ce groupe recouvre tous les riskwares qui peuvent entraîner une gêne ou certains dommages.

- **Programmes présentant un risque potentiel**. Ce groupe reprend les logiciels qui ne sont pas malveillants ou dangereux mais qui dans certaines circonstances peuvent servir à endommager votre ordinateur.

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

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

Les experts de Kaspersky Lab ne conseillent pas de désactiver le contrôle du deuxième groupe. Lorsque Kaspersky Anti-Virus considère un programme comme étant dangereux alors que, d'après vous ce n'est pas le cas, il est conseillé de l'exclure (cf. point 6.3, p. 66).

6.3. 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 convaincu que celui-ci est tout à fait sain.

Il est possible d'exclure des fichiers d'un certain format, des fichiers selon un masque, certains secteurs (par exemple, un répertoire ou un programme), des processus ou des objets en fonction de la classification de l'Encyclopédie des virus (état attribué à l'objet par le programme suite à l'analyse).

Attention !

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

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

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

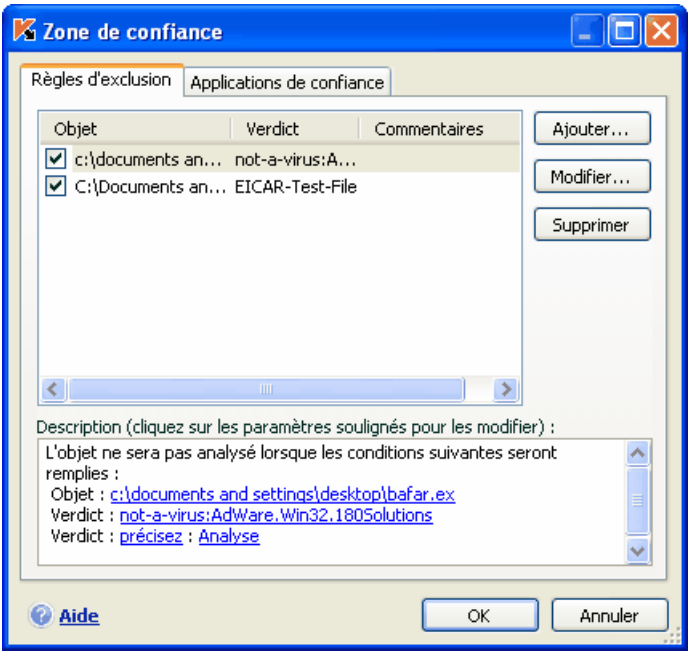


Illustration 8. Constitution de la zone de confiance

6.3.1. Règles d'exclusion

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

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

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

Les riskwares n'ont pas de fonction malveillante mais ils peuvent être utilisés en tant que "complice" d'autres programmes malveillants car il présentent des failles et des erreurs. Les programmes d'administration à distance, les clients IRC, les serveurs FTP, tous les utilitaires d'arrêt ou de dissimulation de processus, les détecteurs de frappe de clavier, les décrypteurs de mot de passe, les dialers, etc. appartiennent à cette catégorie. Un tel programme n'est pas considéré comme un virus (not-a-virus) mais il peut appartenir à un sous-groupe tel que Adware, Joke, Riskware, etc. (pour obtenir de plus amples informations sur les programmes malveillants découverts par Kaspersky Anti-Virus, consultez l'encyclopédie des virus à l'adresse www.viruslist.com/fr). De tels programmes peuvent être bloqués après l'analyse. Dans la mesure où certains d'entre eux sont très populaires auprès des utilisateurs, il est possible de les exclure de l'analyse. Pour ce faire, il faut ajouter le nom ou le masque de l'objet 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 la classification sera not-a-virus:RemoteAdmin.Win32.RAdmin.22.

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

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

1. Cliquez sur **Ajouter** dans la fenêtre **Règles d'exclusion**.
2. Dans la fenêtre qui apparaît (cf. ill. 9), 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.

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

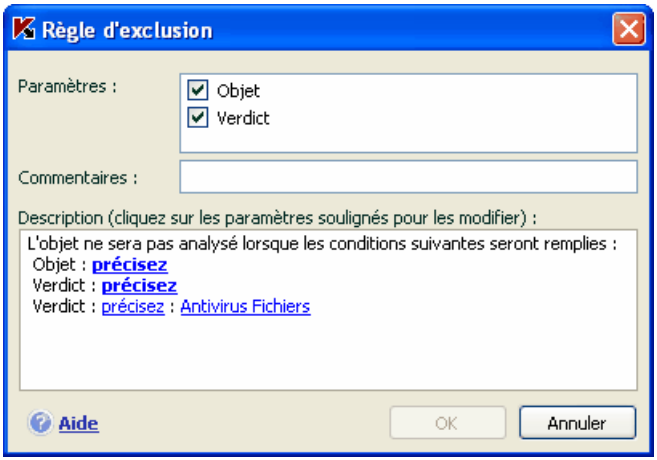


Illustration 9. Création d'une règle d'exclusion

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

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

3. Définissez la valeur du type d'exclusion sélectionné. Pour ce faire, cliquez avec le bouton gauche de la souris dans la section **Description** sur le lien précisez, situé à côté du type d'exclusion :

   - Pour le type **Objet**, saisissez dans la fenêtre qui s'ouvre son nom (il peut s'agir d'un fichier, d'un répertoire quelconque ou d'un masque de fichiers (cf. point A.2, p. 232). 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-répertoires, le fichier **winword.exe** situé dans n'importe quel dossier de **C:\Program Files** sera ignoré.

- Pour la **Classification** 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. 233).

  Pour certaines classifications, 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 verdicts suivants :

  - *Invader* (intrusion dans les processus du programme). Pour ce verdict, 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 ce verdict, 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 **Verdict**. 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 indiqué. Dans la fenêtre qui s'ouvre, cochez la case en regard des composants qui exploiteront la règle d'exclusion.

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

1. Cliquez sur Ajouter à la zone de confiance dans la fenêtre de notification (cf. ill. 10).

Illustration 10. Notification sur la découverte d'un objet dangereux

2. Dans la boîte de dialogue qui s'affiche, vérifiez si tous les paramètres vous conviennent. Les champs reprenant le nom de l'objet et le type de menace attribué sont remplis automatiquement sur la base des renseignements qui figurent dans la notification. Afin de créer une règle, cliquez sur **OK**.

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

1. Sélectionnez dans le rapport l'objet que vous souhaitez ajouter aux exclusions.
2. Ouvrez le menu contextuel et sélectionnez le point **Ajouter à la zone de confiance** (cf. ill. 11).
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**.

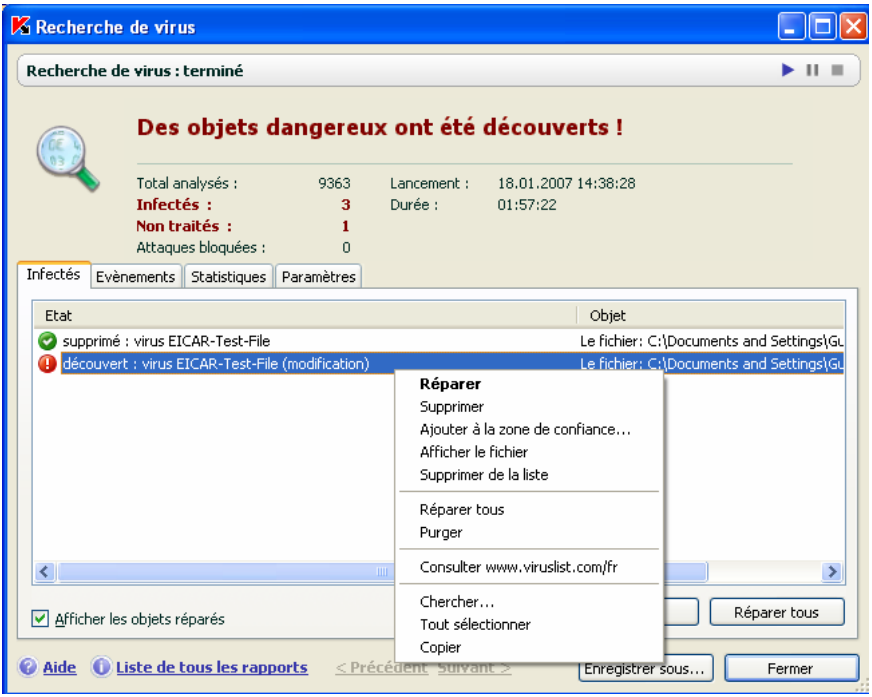


Illustration 11. Création d'une règle d'exclusion au départ du rapport

6.3.2. Applications de confiance

L'exclusion des applications de confiance est disponible dans les versions de Kaspersky Anti-Virus installées sur Microsoft Windows NT 4.0/2000/XP/Vista.

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 registre 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 6.3.1, p. 67).

De plus, certaines actions considérées comme dangereuses sont en réalité normales dans le cadre du fonctionnement de divers programmes. Ainsi, l'interception du texte tapé avec le clavier est une action tout à fait normale pour les programmes de permutation automatique de la disposition du clavier (Punto Switcher, etc.). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

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

La constitution de la liste des applications de confiance s'opère sur l'onglet spécial **Applications de confiance** (cf. ill. 12). Cette liste contient par défaut les applications dont l'activité n'est pas analysée sur la base des recommandations des experts de Kaspersky Lab. Si vous estimez que les applications de cette liste ne sont pas de confiance, désélectionnez les cases correspondantes. Vous pouvez modifier la liste à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer** situés à droite.

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

1. Cliquez sur le bouton **Ajouter…** situé dans la partie droite de la fenêtre
2. Dans la fenêtre **Application de confiance** (cf. ill. 13) qui s'ouvre, sélectionnez l'application à l'aide du bouton **Parcourir…**. Cette action entraîne l'affichage d'un menu contextuel qui vous permettra au départ du point **Parcourir…** de passer à la boîte de dialogue standard de sélection des fichiers et d'indiquer le chemin d'accès au fichier exécutable ou de consulter la liste des applications ouvertes à l'instant au départ du point **Applications** et de sélectionner l'application souhaitée.

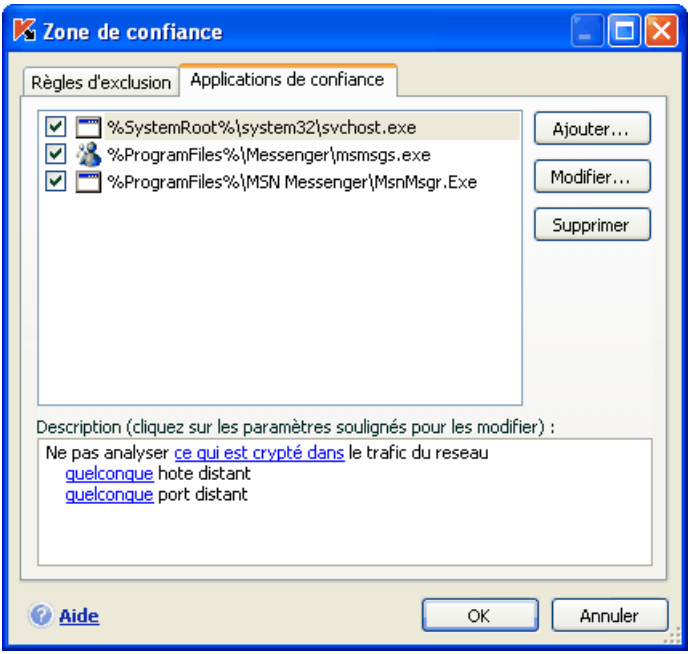


Illustration 12. Liste des applications de confiance

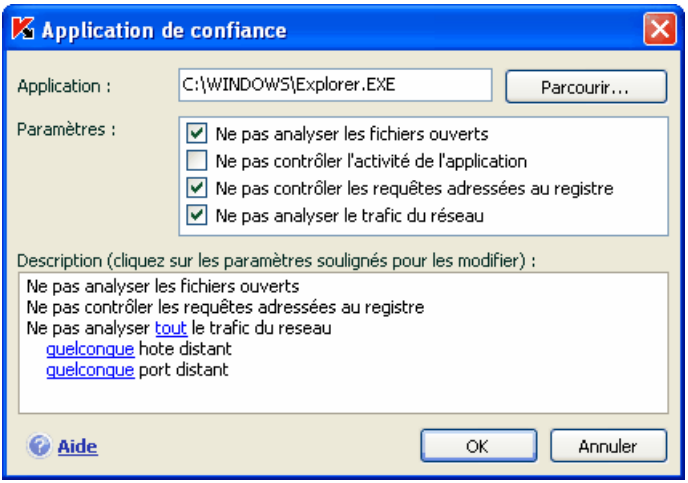


Illustration 13. Ajout d'une application à la liste des applications de confiance

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. 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.

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

N'oubliez pas que cette fonction n'est pas disponible sous Microsoft Windows 98/ME.

Kaspersky Anti-Virus 6.0 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 au départ d'une source à laquelle vous n'avez pas accès (par exemple, le répertoire de mise à jour du réseau) ou pour laquelle vous ne connaissez pas les paramètres d'autorisation du serveur proxy. Vous pouvez utiliser ce service afin de lancer la mise à jour au nom d'un utilisateur qui jouit de ces privilèges.

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

1. Sélectionnez le nom de la tâche dans la section **Analyser (Services)** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.
2. Cliquez sur le bouton **Configuration** dans la boîte de dialogue de configuration de la tâche et passez à l'onglet **Complémentaire** dans la fenêtre qui s'affiche (cf. ill. 14).

Pour activer ce service, cochez la case **Lancement de la tâche au nom de l'utilisateur**. Saisissez en dessous les données du compte sous lequel la tâche sera exécutée: nom d'utilisateur et mot de passe.

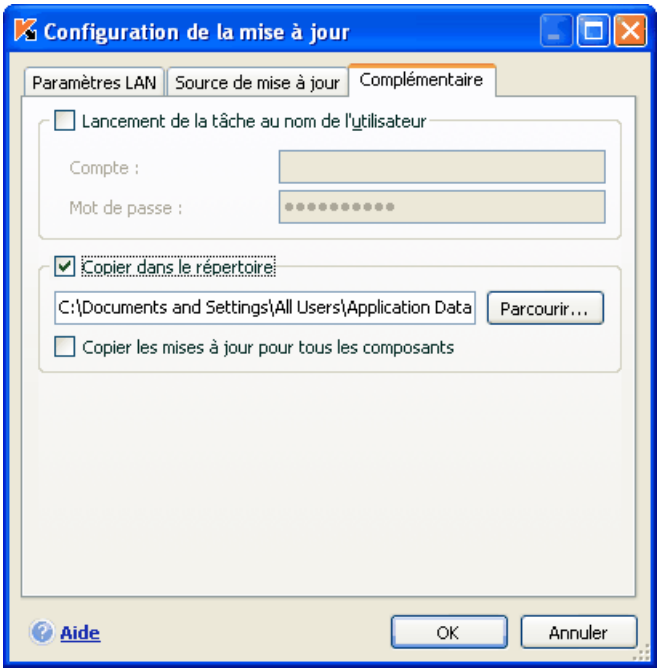


Illustration 14. Configuration du lancement de la mise à jour au nom d'un autre utilisateur

6.5. Programmation du lancement de tâches liées à la recherche de virus et à la mise à jour

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

Le lancement des tâches de recherche de virus créées lors de l'installation de l'application, se produit automatiquement à l'heure programmée. Pour la mise à jour, le lancement programmé est également désactivé. Elle est réalisée automatiquement 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 du lancement automatique. Pour ce faire, sélectionnez le nom de la tâche dans la section **Analyser** (pour la recherche de virus) ou **Services** (pour la mise à jour) et cliquez sur le lien Configuration afin d'ouvrir la boîte de dialogue de configuration.

Afin d'activer le lancement programmer d'une tâche, cochez la case en regard de la condition de lancement de la tâche dans le bloc **Mode de lancement**. Vous pouvez modifier les conditions de lancement de l'analyse dans la fenêtre **Programmation** (cf. ill. 15) en cliquant sur **Modifier**.

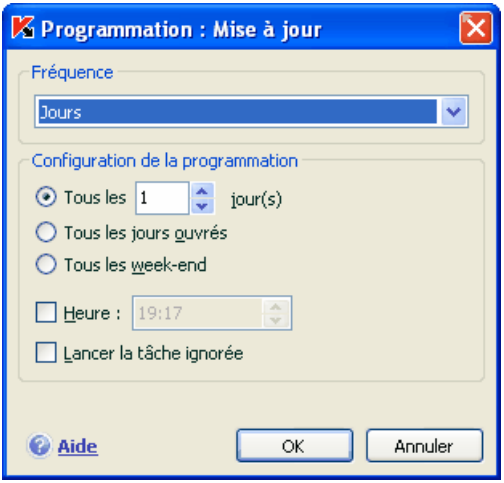


Illustration 15. Programmation de l'exécution de la tâche

L'élément le plus important à définir, c'est la fréquence de lancement. Vous avez le choix entre les options suivantes :

Heure définie. La tâche est exécutée une fois au jour et à l'heure indiqués.

Au démarrage de l'application. La tâche est lancée chaque fois que Kaspersky Anti-Virus est ouvert.

Après chaque mise à jour. La tâche est lancée après chaque mise à jour des signatures des menaces (ce point concerne uniquement les tâches liées à la recherche de virus).

Minutes. L'intervalle entre les lancements de la tâche se mesure en quelques minutes uniquement. Précisez le nombre de minutes entre chaque lancement dans les paramètres de programmation. L'intervalle maximum est de 59 minutes.

Heures. L'intervalle entre les lancements de la tâche est mesuré en heures. Si vous avez choisi cette fréquence, indiquez l'intervalle dans les paramètres de programmation : **Toutes les X heure(s)** et définissez l'intervalle X. Pour une mise à jour toutes les heures, sélectionnez *Toutes les 1 heure(s).*

Jour. Le programme est mis à jour une fois tous les X jours. Dans les paramètres de programmation, définissez la fréquence de lancement de la tâche :

- Sélectionnez **Tous les X jours** et précisez l'intervalle *X* si vous souhaitez qu'un certain nombre de jours s'écoule entre les lancements de la tâche. Ainsi, afin que l'analyse ait lieu un jour sur deux, définissez *Tous les 2 jours*.
- Sélectionnez **Tous les jours ouvrés** si vous souhaitez lancer l'analyse tous les jours du lundi au vendredi.
- Sélectionnez **Tous les week-ends** si vous voulez que la tâche soit lancée uniquement les samedi et dimanche.

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

Semaines. La tâche est lancée certains jours de la semaine. Si vous avez choisi cette fréquence, il vous faudra cocher les jours de lancement de l'analyse dans les paramètres de la programmation. Indiquez également l'heure de lancement de l'analyse dans le champ *Heure*.

Mois. La tâche d'analyse est lancée une fois par mois à l'heure indiquée.

Si pour une raison quelconque le lancement de la tâche a été ignoré (par exemple, votre ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique des tâches ignorées dès que cela sera possible. Pour ce faire, cochez la case ☑ **Lancer la tâche ignorée** dans la fenêtre de programmation.

6.6. Configuration de la productivité

Afin d'économiser les batteries des ordinateurs portables et afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

- 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. 57) ou lancer l'analyse antivirus manuellement (cf. point 5.3, p. 55). Pour utiliser le service d'économie de la batterie, cochez la case correspondante dans la case ☑ **Ne pas lancer les tâches prévues si le portable est débranché**.

- L'exécution des tâches liées à la recherche de virus augmentent 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, cochez la case ☑ **Céder les ressources aux autres applications**.

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

Afin de configurer le paramètre des performances pour la recherche de virus,

Sélectionnez la rubrique **Protection** dans la fenêtre principale du logiciel et cliquez sur le lien Configuration. La configuration des paramètres de la performance a lieu dans le bloc **Complémentaire** (cf. Illustration 16).

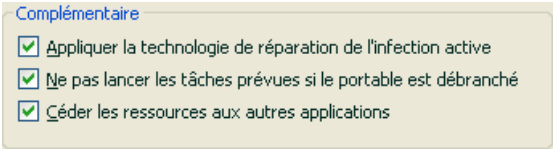


Illustration 16. Configuration de la productivité

6.7. 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 6.0 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 à la recherche de virus (cf. point 5.3, p. 55). Si vous souhaitez utiliser la réparation étendue, cochez la case ☑ **Appliquer la technologie de réparation de l'infection active** .

Pour activer/désactiver la technologie de réparation de l'infection active :

Sélectionnez la rubrique **Défense** dans la fenêtre principale et cliquez sur le lien Configuration. La configuration des paramètres de performance s'opère dans le bloc **Complémentaire**

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 de 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 barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un fichier est analysé.

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

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

Le processus d'analyse contient les étapes suivantes :

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

tente de le neutraliser. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier est supprimé.

b. Si le fichier contient un code semblable à un code malveillant et que ce verdict ne peut pas être garanti à 100%, le fichier est réparé et placé en *quarantaine.*

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

7.1. Sélection du niveau de protection des fichiers

L'antivirus de fichiers protège les fichiers que vous utilisez selon un des niveaux suivants (cf. ill. 17):

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

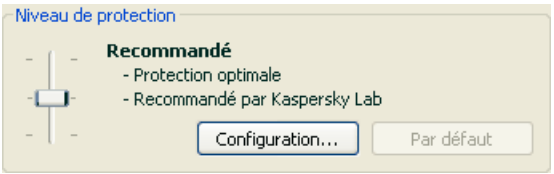


Illustration 17. Niveau de protection d'Antivirus Fichiers

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 **Utilisateur**. Voici un exemple d'une situation où le niveau Utilisateur serait le plus indiqué pour la protection des fichiers.

Exemple:

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

Conseil pour la sélection du niveau :

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

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

Pour modifier les paramètres du niveau de protection actuel :

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

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

7.2. Configuration de la protection des fichiers

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

- Les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 7.2.1, p. 84);
- Les paramètres qui définissent la zone protégée (cf. point 7.2.2, p. 87);
- Les paramètres qui définissent les actions à réaliser sur l'objet dangereux (cf. point 7.2.5, p. 92). .
- Les paramètres complémentaires de fonctionnement de l'Antivirus Fichiers (cf. point 7.2.3, page 89).

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. 230) 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.

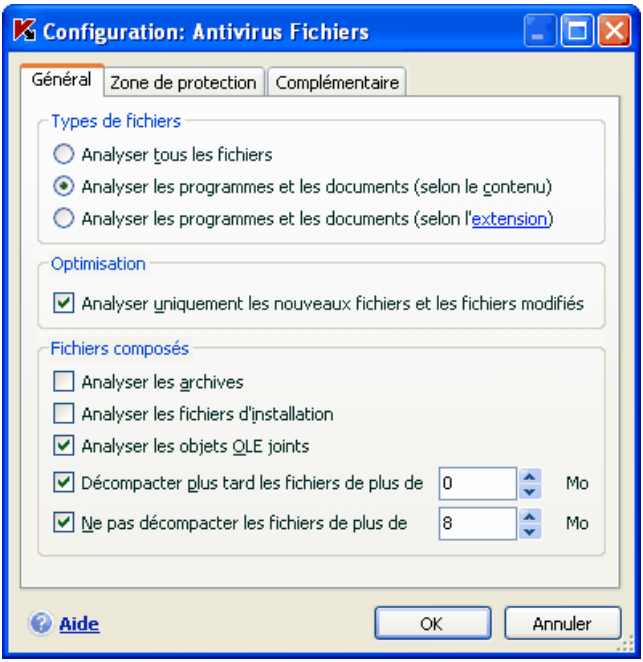


Illustration 18. Sélection du type de fichier soumis à l'analyse antivirus

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

- **Analyser les archives/uniquement les nouvelles archives** : analyse les archives au format ZIP, CAB, RAR, ARJ
- **Analyser les/uniquement les nouveaux fichiers d'installation** : recherche la présence d'éventuels virus dans les archives autoextractibles.
- **Analyser les/uniquement les nouveaux objets OLE joints** : analyse les objets intégrés au fichier (exemple : tableau Excel, macro dans un document Microsoft 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. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration
2. Cliquez sur le bouton **Configuration** et sélectionnez l'onglet **Zone de protection** dans la fenêtre qui s'ouvre (cf. 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 :

- Indiquer uniquement les répertoires, disques ou fichiers qui doivent être protégés.
- 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.

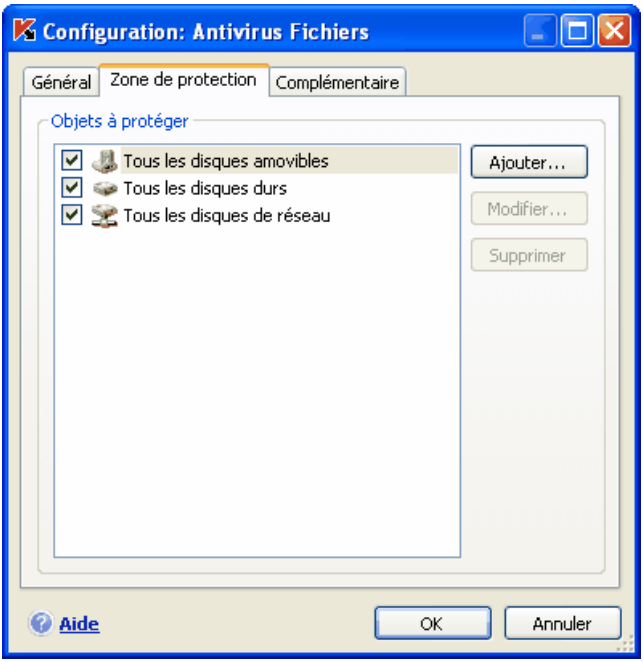


Illustration 19. Constitution de la zone protégée

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

- **C:\dir*.*** ou **C:\dir*** ou **C:\dir** : tous les fichiers du répertoire *C:\dir*
- **C:\dir*.exe** : tous les fichiers *.exe du répertoire *C:\dir*
- **C:\dir*.ex?** tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère
- **C:\dir\test** : uniquement le fichier *C:\dir\test*
- Afin que l'analyse de l'objet sélectionné soit complète, cochez la case **Y compris les sous-répertoires**.

Attention.

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

7.2.3. Configuration des paramètres complémentaires

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

Pour configurer les paramètres complémentaires de l'antivirus fichiers :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et à l'aide du lien Configuration, ouvrez la fenêtre de configuration du composant.
2. Cliquez sur le bouton **Configuration** et dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Complémentaire** (cf. ill. 20).

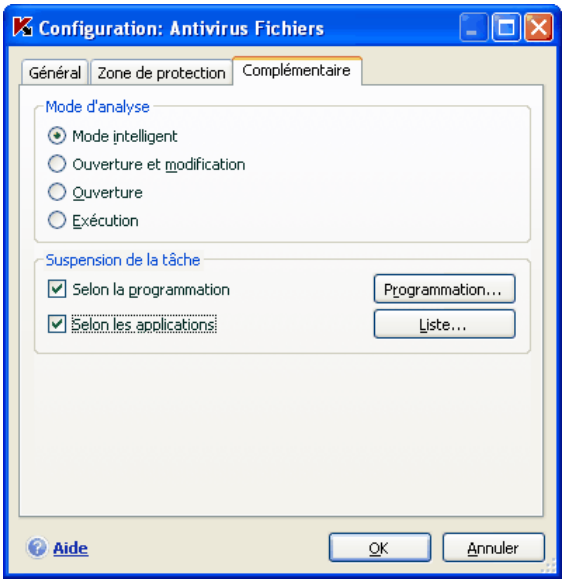


Illustration 20. Configuration des paramètres complémentaires de l'Antivirus Fichiers.

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

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

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

Le mode intelligent est utilisé par défaut.

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

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

Afin de suspendre l'activité du composant pour un certain temps, cochez la **Selon la programmation** et dans la fenêtre (cf. 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.

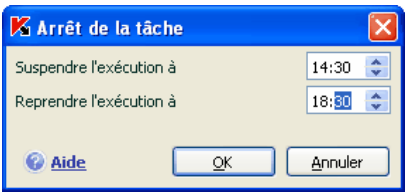


Illustration 21. Suspension du composant

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.

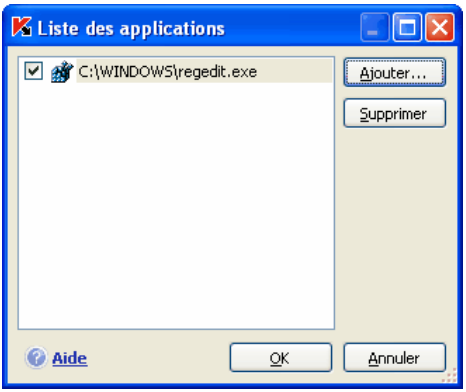


Illustration 22. Constitution de la liste des applications

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

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

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

7.2.4. Restauration des paramètres de protection des fichiers par défaut

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

Pour restaurer les paramètres de protection des fichiers par défaut :

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

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

7.2.5. Sélection de l'action exécutée sur les objets

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

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

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*) (cf. point 1.3, p. 12).
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le code du fichier contient une séquence de code semblable à celle d'un virus inconnu ou le code modifié d'un virus connu.

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

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

Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 23).

Illustration 23. 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	L'antivirus de fichiers affiche un

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
	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	L'antivirus de fichiers bloque l'accès à l'objet. Les informations sont consignées dans le rapport (cf. point 14.3, p. 178). Vous pouvez plus tard tenter de réparer cet objet.
Bloquer l'accès **Réparer**	L'antivirus de 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 14.1, p. 172). 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**	L'antivirus de 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 14.2, p. 176).
Bloquer l'accès **Réparer** **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 **Antivirus Fichiers** dans la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc Statistiques.
2. Sélectionnez les objets qui vous intéressent sur l'onglet **Infectés** et cliquez sur **Actions** → **Réparer tous**.

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

CHAPITRE 8. 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 les messages en mode sécurisé (SSL) via les protocoles POP3 et IMAP.

L'icône de Kaspersky Anti-Virus dans la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un 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 *signatures de menaces* utilisées par le logiciel et d'un algorithme heuristique. Les signatures 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 signatures de menaces.
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 est inclus dans l'objet du message.

[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 !

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. 100) 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. 102) 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, 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 dans la Boîte de réception.

8.1. Sélection du niveau de protection du courrier

Kaspersky Anti-Virus assure la protection du courrier selon un des 3 niveaux suivants (cf. ill. 24):

Elevé : 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 **Elevé**, à l'exclusion des pièces jointes et des messages dont l'analyse dure plus de trois minutes.

Faible : 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 minutes.

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

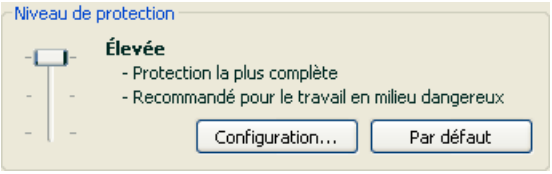


Illustration 24. Sélection du niveau de protection du courrier

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 l'un des niveaux proposés par défaut ne convient pas à vos exigences, vous pouvez modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**. Voici un exemple d'une situation où le niveau Utilisateur serait le plus indiqué pour la protection du courrier.

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 **Elevé** 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 proposé par défaut :

cliquez sur **Configuration…** dans la fenêtre des paramètres de l'antivirus de messagerie électronique, modifiez les paramètres selon vos besoins et 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. 98);

Les paramètres qui définissent l'analyse des messages dans Microsoft Office Outlook (cf. point 8.2.2, p. 100) et The Bat! (cf. point 8.2.3, p. 102).;

> Attention !
>
> Cette version de Kaspersky Anti-Virus ne prévoit pas les modules externes de l'Antivirus Courrier pour les versions 64 bits des clients de messagerie.

- Les paramètres qui définissent les actions à réaliser sur les objets dangereux des messages (cf. point 8.2.5, p. 104).

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 le 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. Cliquez sur **Configuration…** dans la fenêtre des paramètres de l'antivirus de messagerie électronique.
2. Dans la fenêtre de configuration de l'antivirus de messagerie électronique (cf. ill.), sélectionnez l'onglet **Général** et choisissez l'option **Uniquement le courrier entrant** dans le bloc **Zone de protection**.

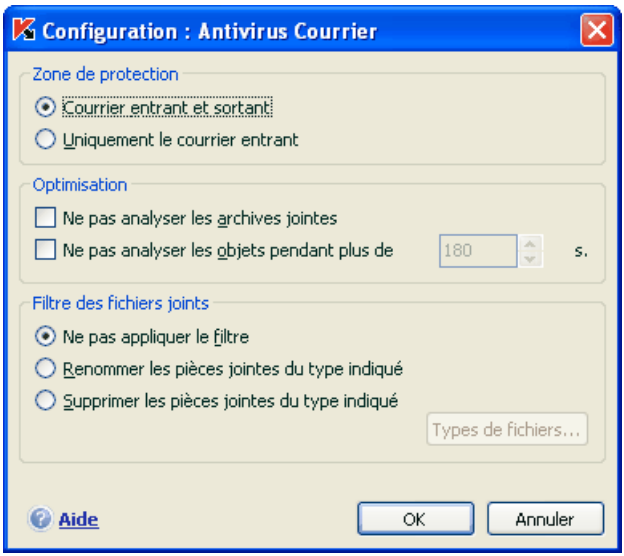


Illustration 25. Configuration de la protection du trafic de messagerie

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.

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 230.

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 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 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.

Attention !

Cette version de Kaspersky Anti-Virus ne prévoit pas les modules externes de l'Antivirus Courrier pour la version 64 bits de Microsoft Office Outlook.

Le plug-in prend la forme de l'onglet **Protection du courrier électronique** dans le menu **Services** → **Paramètres**(cf. ill. 26).

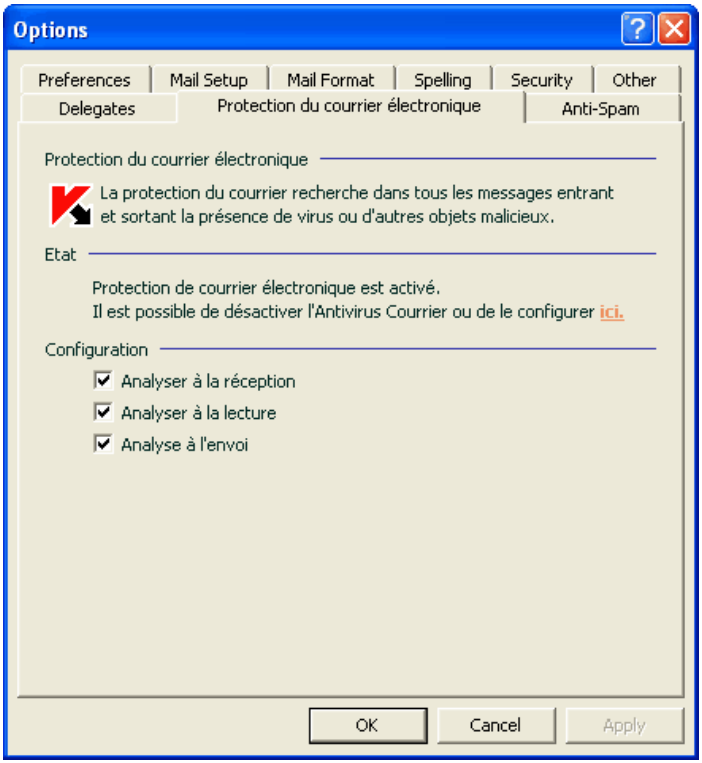


Illustration 26. Configuration détaillée de la protection du courrier dans Microsoft Office Outlook

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 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.

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. 98).

Cette version de Kaspersky Anti-Virus ne prévoit pas les modules externes de l'Antivirus Courrier pour la versions 64 bits de The Bat !

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. 27) sont appliqués à tous les modules antivirus de l'ordinateur compatibles avec The Bat!

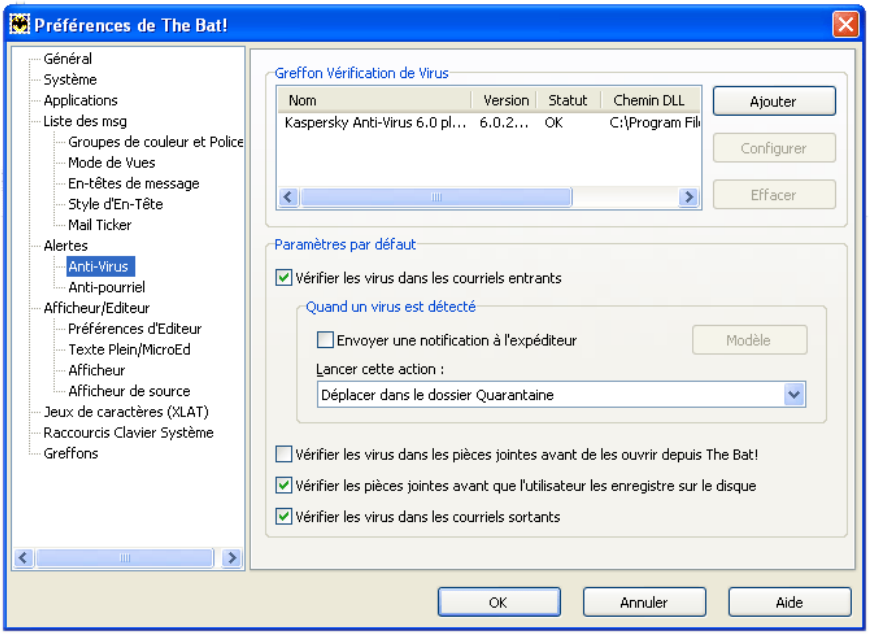


Illustration 27. Configuration du courrier dans The Bat!

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. 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. Sélectionnez **Antivirus Courrier** dans la fenêtre principale et cliquez sur le lien Configuration pour passer à la fenêtre de configuration du composant.
2. Cliquez sur **Par défaut** dans la section **Niveau de protection**

8.2.5. 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 (en-tête, 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 1.3 à la page 12);
- *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, l'antivirus de messagerie 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 Kaspersky Anti-Virus et sélectionnez **Antivirus Courrier**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 28).

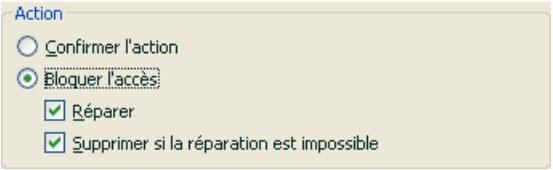


Illustration 28. Sélection de l'action à réaliser sur l'objet dangereux du message

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	L'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	L'antivirus Courrier bloque l'accès à l'objet. Les informations relatives à cette situation sont consignées dans le rapport (cf. point 14.3, p. 178). Vous pouvez plus tard tenter de réparer cet objet.

Action choisie	Résultat de l'action
◉ **Bloquer l'accès** ☑ **Réparer**	L'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. 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]	L'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** ◉ **Réparer** ☑ **Supprimer**	En cas de découverte d'un objet infecté ou potentiellement infecté, l'antivirus Courrier le supprime sans prévenir l'utilisateur.

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 14.2, p. 176) 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 sur 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 : l'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 14.7, p. 191). 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 (connexion à Internet via un modem), 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 barre des tâches 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. L'icône  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 *signatures de menaces* utilisées par Kaspersky Anti-Virus et d'un algorithme heuristique. Les signatures 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 signatures de menaces.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
    a. Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandée est infecté.
    b. Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

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.

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. 29):

Elevé : 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 **Elevé**, 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.

Faible : 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 de signatures de menaces. L'utilisation de ce niveau est recommandée uniquement si d'autres moyens de protection du trafic Internet sont installés sur votre ordinateur.

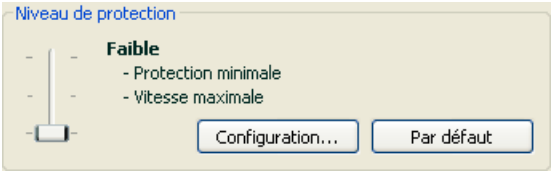


Illustration 29. Sélection du niveau de protection d'Internet

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 un des niveaux ne correspond pas à vos besoins, vous pouvez créer le niveau **Utilisateur.** Voici des exemples de situations où cela 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 **Elevé** 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 :

cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus Internet, modifiez les paramètres de la protection Internet (cf. point 9.2, p. 110) selon vos besoins et 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) lancés.

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

- Définir l'algorithme d'analyse, en choisissant la sélection complète ou partielle des signatures des menaces.
- indiquer les objets du trafic HTTP qu'il ne faudra pas soumettre à la recherche d'objets dangereux;
- composer la liste des adresses dont le contenu est fiable.

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. Définition de l'algorithme d'analyse

L'analyse des données reçues via Internet peut s'opérer selon l'un des deux algorithmes suivants :

- *Analyse continue* : technologie d'identification du code malveillant dans le trafic du réseau qui procède à l'analyse "en vol" des données. Supposons

que vous téléchargiez un fichier depuis un site Web. L'antivirus Internet analyse le fichier au fur et à mesure du téléchargement. Cette technologie accélère la livraison de l'objet analysé à l'utilisateur. L'analyse continue recours à un nombre restreint de signatures des menaces (uniquement les plus actives), ce qui réduit considérablement la sécurité de l'utilisation d'Internet.

- *Analyse avec mise en tampon* : technologie d'identification du code malveillant dans le trafic du réseau qui procède à l'analyse de l'objet une fois qu'il a été entièrement copié dans la mémoire tampon. Après cela, l'objet est soumis à l'analyse antivirus et, en fonction des résultats, est transmis à l'utilisateur ou est bloqué. Ce type d'analyse exploite toutes les signatures des menaces, ce qui augmente considérablement la probabilité d'identifier tout code malveillant. Toutefois, cette technologie s'accompagne d'une augmentation du temps de traitement de l'objet et de son transfert à l'utilisateur. Il peut également y avoir des problèmes en cas de copie et de traitement d'objets volumineux suite à l'expiration du délai de connexion au client http. Afin d'éviter de tels inconvénients, nous vous conseillons de limiter la mise en cache des fragments de l'objet reçu via Internet. Une fois ce délai écoulé, chaque partie du fichier reçue sera transmise directement à l'utilisateur. L'objet aura été analysé entièrement à la fin de la mise en cache. Cela permet d'accélérer la vitesse de transfert de l'objet, d'éviter les problèmes liés aux déconnexions, le tout, sans réduire le niveau de protection de l'ordinateur.

Afin de sélectionner l'algorithme d'analyse qui sera suivi par l'antivirus Internet :

1. Cliquez sur **Configuration** dans la fenêtre de configuration de l'antivirus Internet.
2. Sélectionnez la valeur adéquate dans le bloc **Algorithme d'analyse** de la fenêtre qui s'affiche (cf. ill. 30).

Par défaut, l'antivirus Internet analyse les données avec mise en tampon et en utilisant les signatures des menaces complètes. La durée de mise en cache des fragments du fichier est également limitée à 1 seconde.

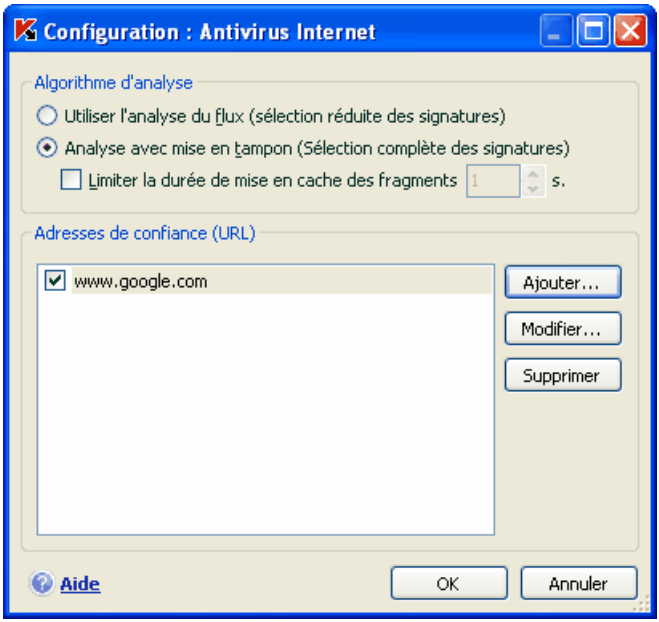


Illustration 30. Configuration du niveau de protection Internet

Attention !
Si vous écoutez la radio ou regardez la télévision via Internet ou si vous participez à des téléconférences en ligne et que vous êtes souvent confronté à des problèmes relatifs à la validité de l'objet requis, utilisez l'algorithme d'analyse des flux.

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. Cliquez sur **Configuration** dans la fenêtre de configuration de l'antivirus Internet.

2. Composez, dans la fenêtre qui s'ouvre (cf. ill. 30), 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. 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. Sélectionnez **Antivirus Internet** dans la fenêtre principale et cliquez sur le lien Configuration pour passer à la fenêtre de configuration du composant.
2. Cliquez sur **Par défaut** dans la section **Niveau de** protection

9.2.4. 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 Kaspersky Anti-Virus et sélectionnez **Antivirus Internet**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 31).

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 31. 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 14.3, p. 178).
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

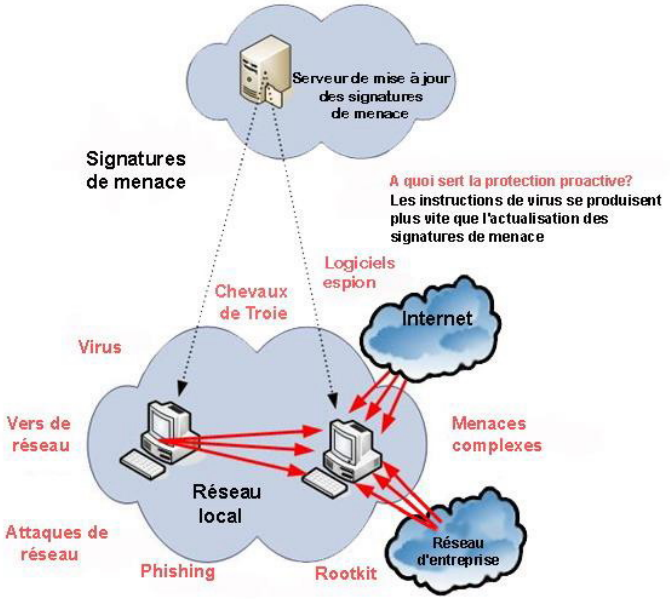
Attention !

Cette version ne contient pas les composants de défense proactive suivants : **Contrôle de l'intégrité de l'application** et **Analyse des macros VBA** pour les ordinateurs tournant sous Microsoft Windows XP Professional x64 Edition ainsi que pour les ordinateurs tournant sous 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 des signatures des menaces. 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 des signatures des menaces 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 de la base des signatures des menaces, 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 des 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 surveille également toutes les macros exécutées dans les applications Microsoft Office.

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, les macros 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 au logiciel et elle est actualisée en même temps que les signatures des menaces).
    - *Actions de chaque macro VBA lancée*. Les macros sont analysées à la recherche d'indices caractéristiques des activités malveillantes.
    - *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.

10.1. Configuration de la défense proactive

La défense proactive s'exécute dans le respect stricte de paramètres (cf. ill. 32) 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 un suivi rigoureux 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 10.1.1, p. 121) 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 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 du système d'exploitation.

  Vous pouvez créer vos propres règles (cf. point 10.1.4.2, p. 135) de contrôle en fonction de la clé de registres Microsoft Windows.

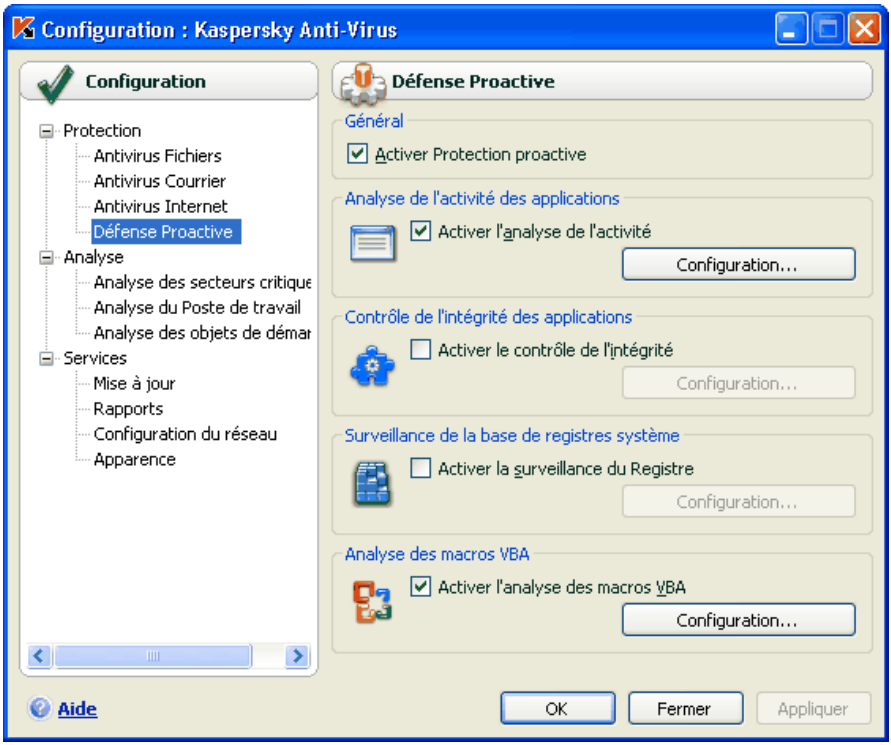


Illustration 32. Paramètres de la défense proactive

- *L'analyse des macros est réalisée*.

  Le contrôle de l'exécution des macros sur l'ordinateur est réglementé par la case **Activer l'analyse des macros VBA**. Cette case est cochée par défaut, et par conséquent, toutes les actions des macros Visual Basics for Applications sont soumises à un contrôle de la part de la défense proactive.

  Vous pouvez sélectionner les macros que vous estimez dangereuses et comment les traiter (cf. point 10.1.3, p. 129).

> 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.

Vous pouvez configurer les exclusions (cf. point 6.3.1, p. 67) pour les modules de la défense proactive et composer des listes d'applications de confiance (cf. point 6.3.2, p. 72).

Tous ces paramètres sont abordés en détails ci-après.

10.1.1. 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 défense 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 commencer à contrôler l'activité de l'application.

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 de l'installation cachée de programmes, de la copie automatique.

- *Lancement du navigateur avec les paramètres.* L'analyse de ce type d'activité permet d'identifier les tentatives de lancement cachée du navigateur avec des paramètres . Une telle activité est caractéristique pour le lancement d'un navigateur Internet depuis une application quelconque avec des paramètres définis de la ligne de commande. Par exemple, ce type d'action est exécuté si vous cliquez sur un lien vers une page Web quelconque dans un message électronique que vous avez reçu.

- *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.

- *Apparition d'activités dissimulées*. 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.
- *Protection du gestionnaire de tâches de Microsoft Windows*. Kaspersky Anti-Virus *protège* le gestionnaire de tâches contre l'intrusion de modules malveillants dont l'activité vise à bloquer le fonctionnement du gestionnaire de tâches.

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 6.3, p. 66)reprenant les applications que vous n'estimez pas dangereuses.

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

1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Analyse de l'activité des applications**.

Les activités dangereuses contrôlées par la défense proactive sont reprises dans la fenêtre **Configuration: analyse de l'activité** (cf. ill. 33).

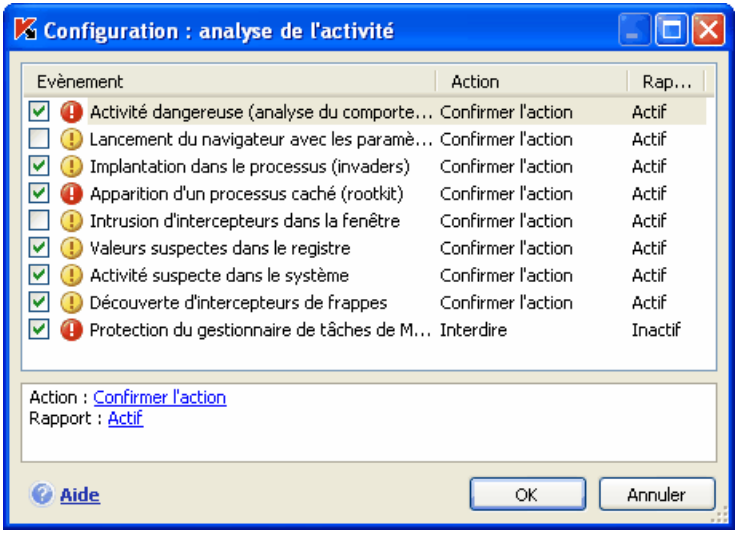


Illustration 33. Configuration du contrôle de l'activité des applications

Pour modifier une règle de contrôle de l'activité dangereuse, sélectionnez-la dans la liste de l'onglet **Evénements** 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 On / Off 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 On / Off.

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 sous 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 utilisateurs**.

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. Une activité dangereuse serait par exemple la modification d'un compte utilisateur au niveau du mot de passe.

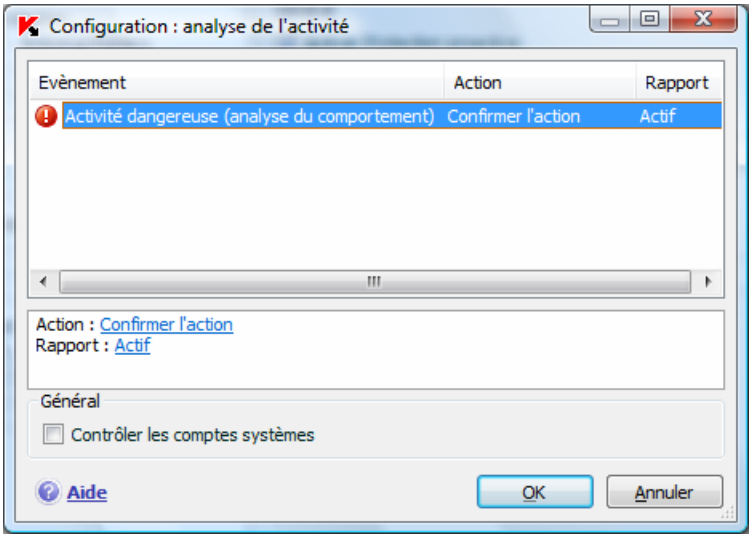


Illustration 34 Configuration du contrôle de l'activité des applications sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.1.2. 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 à 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 des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Contrôle de l'intégrité des applications**.

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

10.1.2.1. 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. 35). 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 critique à la liste et de créer une règle de contrôle :

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.

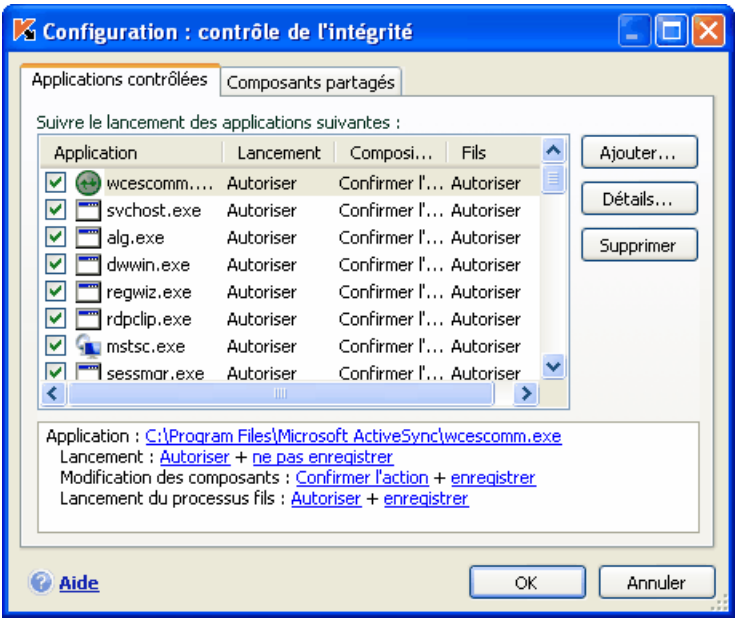


Illustration 35. Configuration du contrôle de l'intégrité de l'application

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 enregistrer / ne pas enregistrer.

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.

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.

10.1.2.2. 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. 36). 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.

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.

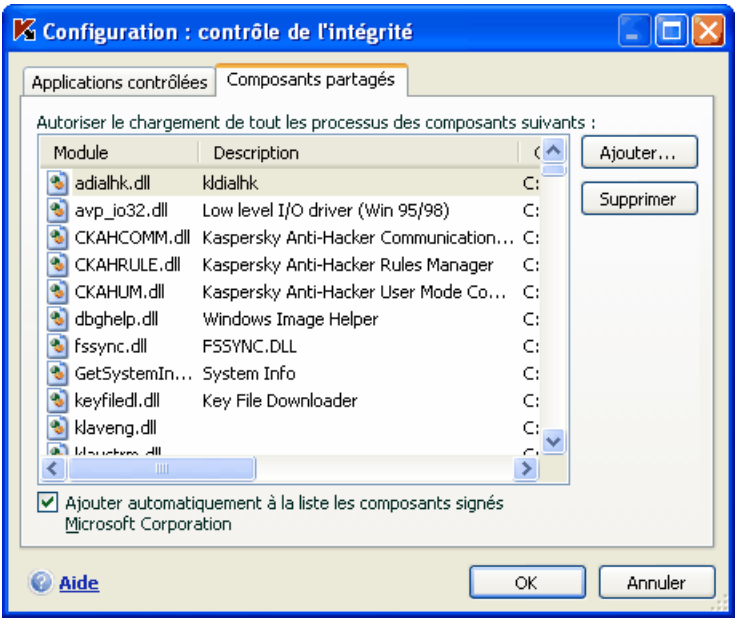


Illustration 36. Configuration de la liste des modules de confiance

10.1.3. Contrôle de l'exécution des macros VBA

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.

L'analyse et le traitement des macros dangereuses lancées sur votre ordinateur est garanti lorsque la case ☑ **Activer l'analyse des macros VBA** est cochée. La case est cochée par défaut, ce qui signifie que toute macro lancée est soumise à la recherche de comportements dangereux et en cas de découverte d'une activité suspecte, la défense proactive autorise ou non l'exécution de la macro.

Exemple:

La barre Adobe Acrobat, intégrée à Microsoft Office Word, permet de créer des fichiers PDF au départ de n'importe quel document grâce à la macro *PDFMaker*. La défense proactive considère les actions telles que l'intégration d'éléments dans un programme comme dangereuses. Si le

contrôle des macros est activé, Kaspersky Anti-Virus affichera un message d'avertissement à l'écran en cas d'exécution de la macro pour vous signaler qu'une macro dangereuse a été découverte. Vous pourrez alors décider soit d'arrêter l'exécution de la macro, soit l'autoriser.

Vous pouvez configurer la réaction de Kaspersky Anti-Virus face à l'exécution d'actions suspectes de la macro. Si vous êtes certain que l'action exécutée par la macro dans le cadre de l'utilisation d'un objet particulier, par exemple un document Microsoft Word, n'est pas dangereuse, il est conseillé de rédiger une règle d'exclusion. Lorsque la situation correspondant aux conditions de la règle d'exclusion se présentera, l'action suspecte exécutée par la macro sera ignorée par la défense proactive.

Pour passer à la configuration de l'analyse des macros :

1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Analyse des macros VBA**.

La configuration des règles de traitement des macros dangereuses s'opère sur l'onglet **Configuration de l'analyse des macros VBA** (cf. ill. 37). Par défaut, il contient les règles applicables aux actions considérées comme dangereuses par les experts de Kaspersky Lab. Il s'agit par exemple de l'insertion de modules dans un programme, de la suppression de fichiers, etc.

Chaque macro est associée à une action qui sera exécutée par Kaspersky Anti-Virus suite à la découverte de la macro.

Si vous estimez qu'une des actions reprises dans la liste des action suspectes ne représente aucun danger, désélectionnez la case en regard de son nom. Par exemple, vous travaillez en permanence avec un logiciel qui exécute une macro pour l'ouverture de plusieurs fichiers en écriture et vous êtes absolument certain que cette opération n'est pas dangereuse.

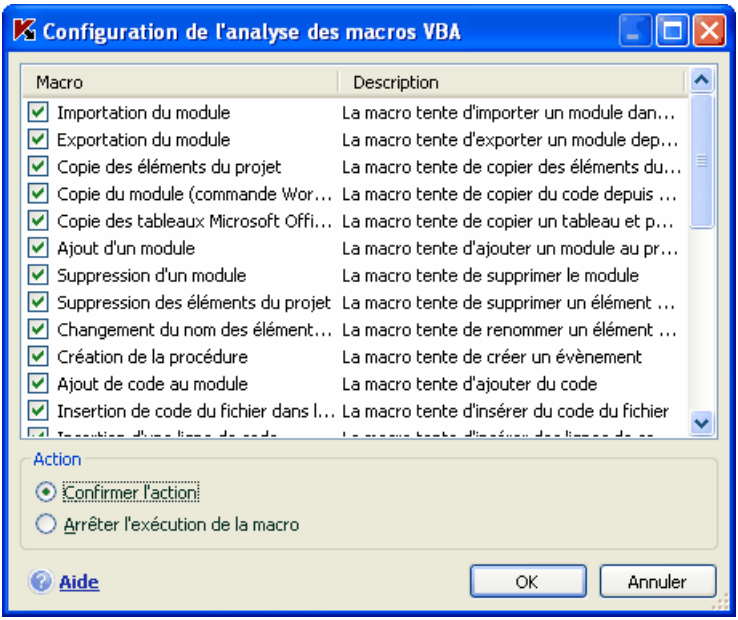


Illustration 37. Configuration des paramètres d'analyse des macros VBA

Afin que Kaspersky Anti-Virus ne bloque pas l'exécution de la macro :

désélectionnez la case en regard de l'action correspondante. Cette action ne sera plus considérée comme dangereuse et sera ignorée par la défense proactive.

Par défaut, chaque fois que le programme découvre une action suspecte réalisée par la macro, il affiche un message à l'écran pour confirmer l'autorisation ou non de l'exécution de la macro.

Afin que le programme bloque automatiquement l'exécution de toutes les actions dangereuses sans demander l'avis préalable de l'utilisateur :

sélectionnez le traitement **Arrêter l'exécution de la macro** dans la fenêtre reprenant la liste des macros.

10.1.4. 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**.

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

1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Surveillance de la base de registres système**.

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 **Groupes de clés de registres** (cf. ill. 38).

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 38. 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 10.1.4.1, p. 133) de la base de registres système qui feront partie du groupe contrôlé dans l'onglet **Règles**. Il peut s'agir d'un seul objet ou de plusieurs.
3. Sur l'onglet **Règles**, créez une règle (cf. point 10.1.4.2, p. 135) pour les objets du registre. Vous pouvez créer plusieurs règles de traitement et définir leur priorité.

10.1.4.1. 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. 39).

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.
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.

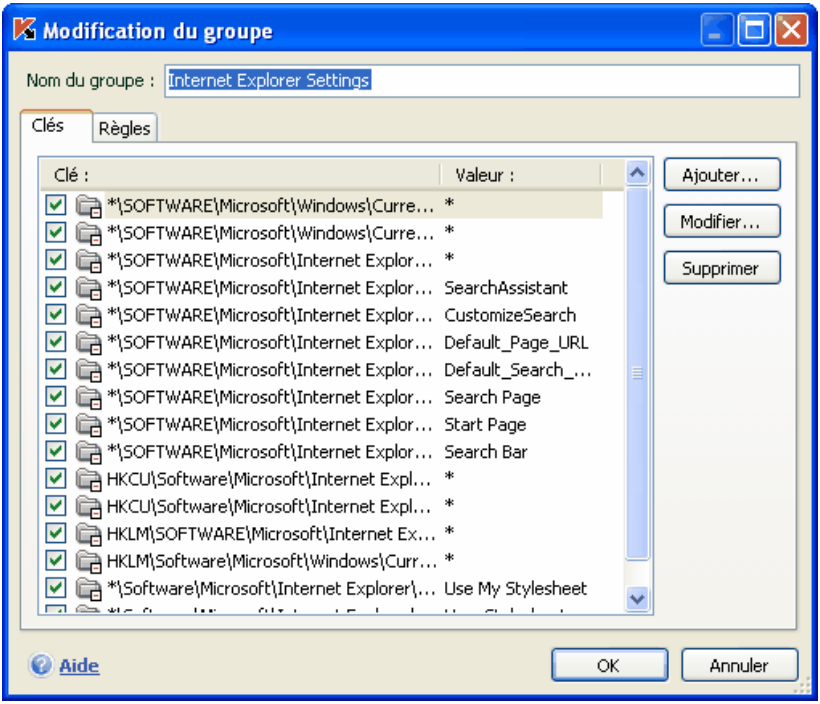


Illustration 39. Ajout d'une clé à contrôler

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.

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

La règle de contrôle des objets 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 à 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 l'objet 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. 40).

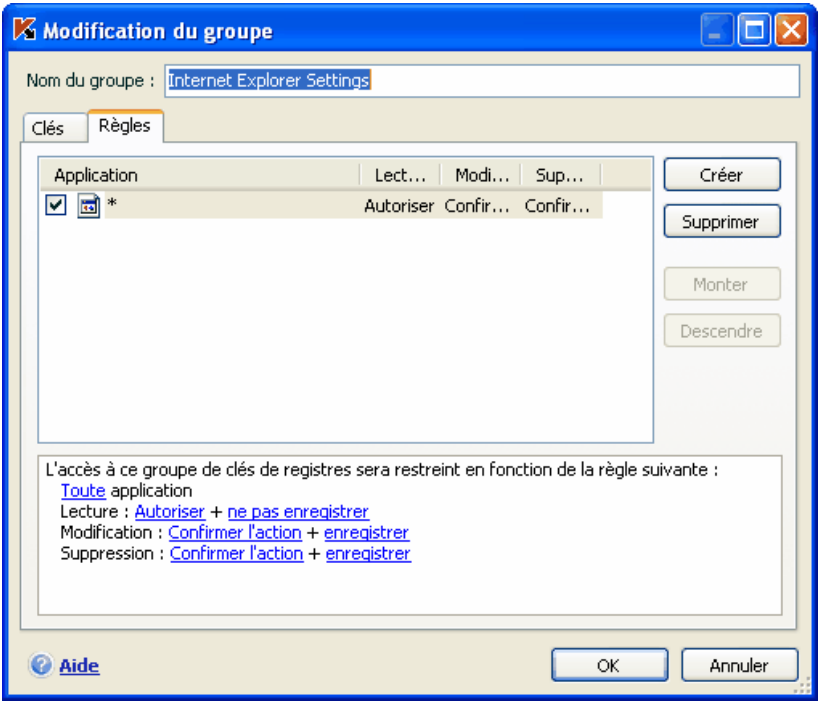


Illustration 40. Création d'une règle de contrôle des clés de la base de registre système

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 quelconque. Il devient sélectionné. 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 enregistrer / ne pas enregistrer.

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 VOTRE 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 2006 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 2006 propose par défaut trois tâches de recherche de virus :

Secteurs critiques

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

Mon poste de travail

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

Objets de démarrage

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

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres (cf. point 11.4, p. 141) et même programmer le lancement de la tâche (cf. point 6.5, p. 77).

Il est possible également de créer des tâches personnalisées (cf. point 11.3, p. 140) de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des bases de messagerie une fois par semaine ou une tâche pour la recherche de la présence éventuelle de virus dans 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 **Recherche de virus** dans la partie gauche de la fenêtre principale de l'application reprend la liste complète des tâches liées à la recherche de virus créées sur votre ordinateur.

11.1. Administration des tâches liées à la recherche de virus

Les tâches liées à la recherche de virus peuvent être lancées manuellement ou automatiquement selon un horaire défini (cf. point 6.5, p. 77).

Afin de lancer la tâche manuellement :

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

Les tâches en cours d'exécution 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 barre des tâches.

Pour suspendre l'exécution de la tâche :

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

Pour suspendre l'exécution de la tâche :

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

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 **Analyser** dans la fenêtre principale du programme. La liste des objets sera reprise dans la partie droite de la fenêtre sous la barre d'état (cf. ill. 41).

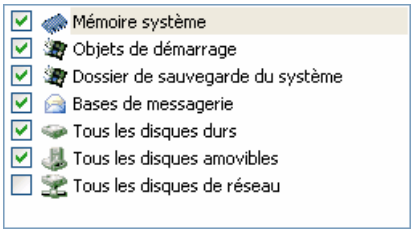


Illustration 41. Liste des objets à analyser

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

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

Pour le confort de l'utilisateur, de nouvelles zones d'analyse ont été ajoutées telles que les bases de messagerie, 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.

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

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

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc. (cf. ill. 42). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

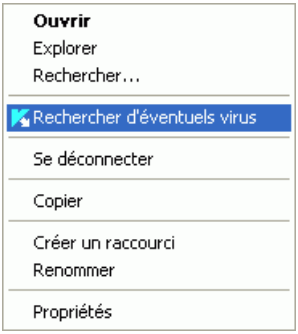


Illustration 42. Analyse d'un objet au départ du menu contextuel de Microsoft Windows

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

Attention !

Le nombre de tâches 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. 139), indiquer les paramètres d'exécution de la tâche (cf. point 11.4, p. 141) et, le cas échéant, programmer (cf. point 6.5, p. 77)le lancement automatique.

Afin de renommer une tâche :

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

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

Pour supprimer une tâche :

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

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

Attention !

Vous pouvez uniquement renommer les tâches que vous avez créées.

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 :

sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.

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. 142);

- 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. 143);
    - configurer le lancement des tâches au nom d'un autre compte utilisateur (cf. point 6.4, p. 75);
    - définir les paramètres complémentaires de l'analyse (cf. point 11.4.5, p. 149);
- restaurer les paramètres d'analyse utilisés par défaut (cf. point 11.4.3, p. 146);
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou potentiellement infecté (cf. point 11.4.4, p. 147);
- programmer le lancement automatique de la tâche (cf. point 6.5, p. 77).

De plus, vous pouvez définir des paramètres uniques de lancement pour toutes les tâches (cf. point 11.4.6, p. 150).

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. 43):

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

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

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

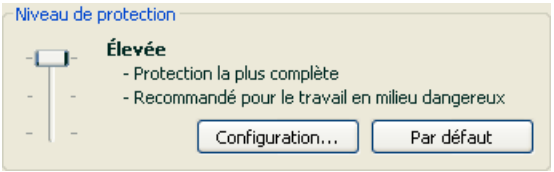


Illustration 43. Sélection du niveau de protection pour la recherche de virus

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 devient **Utilisateur**.

Pour modifier les paramètres du niveau de protection actuel :

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

Un quatrième niveau d'analyse est ainsi configuré : **Utilisateur** selon les paramètres que vous aurez défini.

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. 44). Choisissez l'une des trois options :

- **Analyser tous les fichiers**. Tous les objets 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 plusieurs formats de fichiers qui présentent un faible risque d'infection par un code malveillant suivie d'une activation de ce dernier. Les fichiers au format txt appartiennent à cette catégorie.
Il existe d'autre part des fichiers qui contiennent ou qui peuvent contenir un code exécutable. Il s'agit par exemple de fichiers exe, dll ou doc. Le risque d'intrusion et d'activation d'un code malveillant dans ces fichiers est élevé.

Avant de passer à la recherche de virus dans 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 l'extension, vous pourrez découvrir a liste des extensions des fichiers qui seront soumis à l'analyse dans ce cas (cf. point A.1, p. 230).

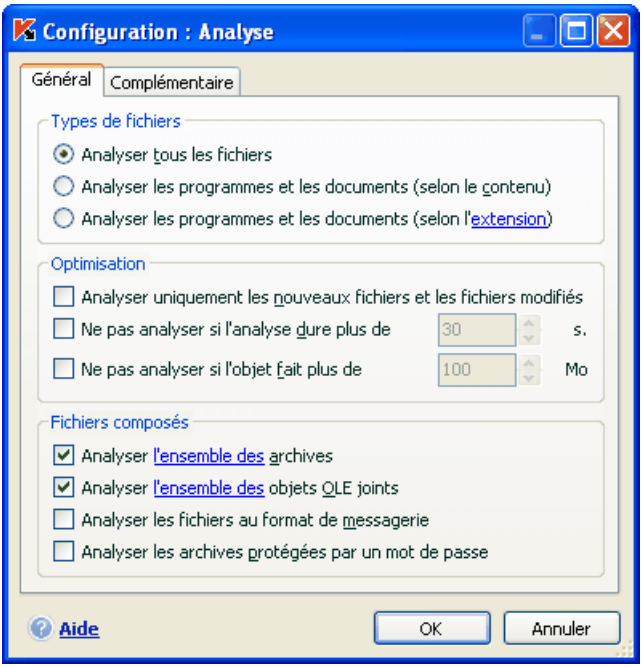


Illustration 44. Configuration des paramètres de l'analyse

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)**, le programme ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

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

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

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

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

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

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

Attention !

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

Pour supprimer de telles archives, cliquez sur le lien Supprimer archive dans la fenêtre de notification de découverte d'un objet dangereux. Ce message apparaît 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. 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 fichiers par défaut :

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

11.4.4. Sélection de l'action exécutée sur les objets

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

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

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*)
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Le fichier contient probablement une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

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

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

sélectionnez le nom de la tâche dans la section **Recherche de virus** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration de la tâche. Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 45).

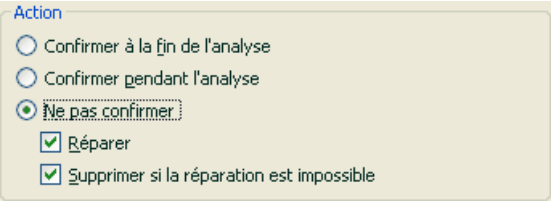


Illustration 45. Sélection de l'action à réaliser sur l'objet dangereux

Action choisie	**Conséquence en cas de découverte d'un objet infecté/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 il est placé en quarantaine (cf. point 14.1, p. 172). Les informations relatives à cette situation sont consignées dans le rapport (cf. point 14.3, p. 178). 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 14.2, p. 176)au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

11.4.5. Paramètres complémentaires pour la recherche de virus

En plus de la configuration des paramètres principaux de la recherche de virus, vous pouvez également définir des paramètres complémentaires (cf. ill. 46):

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

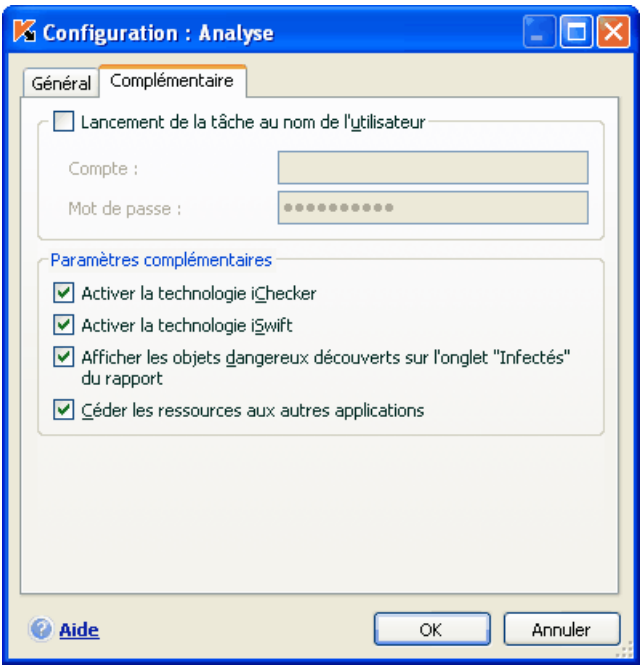


Illustration 46. Configuration complémentaire de l'analyse

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 des signatures des menaces, 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).

- **Activer 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.

  Le recours à la technologie iSwift n'est pas disponible sous Microsoft Windows 98SE/ME/ XP64.

- **Afficher les objets dangereux sur l'onglet "Infectés" du rapport** : affiche la liste des menaces découvertes sur l'onglet Infectés de la fenêtre du rapport (cf. point 14.3.2, p. 182). La désactivation de cette fonction peut être utile lors d'une analyse spéciale, par exemple en cas d'analyse de collections d'essai afin d'augmenter la vitesse d'analyse.

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

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

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

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

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

1. Sélectionnez la section **Analyser** dans la partie gauche de l'onglet et cliquez sur le lien Configuration.
2. Dans la boîte de dialogue de configuration qui s'affiche, définissez les paramètres de l'analyse : sélectionnez le niveau de protection (cf.

point 11.4.1, p. 142), réalisez la configuration complémentaire du niveau et indiquez l'action qui sera réalisée sur les objets (cf. point 11.4.4, p. 147).

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

CHAPITRE 12. ESSAI 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 lui attribue le statut **virus** et exécute l'action définie par l'administrateur pour les objets de ce type.

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

Préfixe	**Etat du virus d'essai**	**Actions lors du traitement de l'objet par l'application**
Pas de préfixe, « virus » d'essai standard	Le fichier contient le virus d'essai. Réparation impossible.	L'application identifie l'objet comme un objet malveillant qui ne peut être réparé et le supprime.
CORR–	Corrompu.	L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide).
SUSP- WARN-	Le fichier contient le virus d'essai (modification). Réparation impossible.	Cet objet est une modification d'un virus connu ou il s'agit d'un virus inconnu. Au moment de la découverte, les bases des signatures des menaces ne contenait pas la description de la réparation de cet objet. L'application place l'objet en quarantaine en vue d'un traitement ultérieur à l'aide des signatures des menaces actualisées.
ERRO-	Erreur de traitement.	Une erreur s'est produite lors du traitement de l'objet : l'application ne peut accéder à l'objet à analyser car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau).

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

La première colonne du tableau contient les préfixes qu'il faut ajouter en tête de la ligne du virus d'essai traditionnel. La deuxième colonne contient une description de l'état et la réaction de Kaspersky Anti-Virus face à divers types de virus d'essai. La troisième colonne contient les informations relatives au traitement que réserver l'application aux objets dont l'état est identique.

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

12.2. Vérification de l'Antivirus Fichiers

Afin de vérifier le fonctionnement de l'Antivirus Fichiers :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai téléchargé depuis le site officiel de l'organisation (cf. point 12.1, p. 152) ainsi que les versions modifiées du virus d'essai.
2. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec. Pour ce faire, cochez la case **Enregistrer les événements non critiques** dans la fenêtre de configuration des rapports (cf. point 14.3.1, p. 181).
3. Exécutez le virus d'essai ou sa modification.

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

Illustration 47. 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. 152) ainsi que les versions modifiées du virus d'essai.
2. Créez une nouvelle tâche de recherche de virus (cf. point 11.3, p. 140) et en guise d'objet à analyser, sélectionnez le dossier contenant la sélection de virus d'essais (cf. point 11.2, p. 139).
3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec. Pour ce faire, cochez la case **Enregistrer les événements non critiques** dans la fenêtre de configuration des rapports.
4. Exécutez la tâche (cf. point 11.1, p. 138) 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 48. 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 :

- **Signature des menaces et pilotes de réseau**

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

  Outre la mise à jour des signatures de menaces, 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 de signatures des menaces : standard ou étendues. Elles se différenciaient par le type d'objets dangereux contre lesquels elles assuraient une protection. Avec Kaspersky Anti-Virus, il n'est plus nécessaire de se soucier du choix des bases de signatures des menaces adéquates. Nos logiciels utilisent désormais les signatures des menaces qui offrent une protection contre divers types de programmes malveillants et d'objets présentant un risque potentiel.

- **modules logiciels**

  En plus des signatures des menaces connues, vous pouvez actualiser les modules internes 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. En voici quelques-uns :

http://downloads1.kaspersky-labs.com/updates/

http://downloads2.kaspersky-labs.com/updates/

ftp://downloads1.kaspersky-labs.com/updates/, etc.

Afin de pouvoir télécharger ces bases , votre ordinateur doit absolument être connecté à Internet.

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

- *Automatique*. Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Lorsque Kaspersky Anti-Virus découvre de nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est utilisé par défaut.
- *Programmé*. La mise à jour du logiciel est réalisée selon un horaire défini.
- *Manuel*. Vous lancez vous-même la procédure de mise à jour du logiciel.

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

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

La possibilité d'annuler (cf. point 13.2, p. 159) une mise à jour est indispensable, par exemple si les signatures des menaces que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

Parallèlement à la mise à jour, vous pouvez copier les mises à jour obtenues dans une source locale (cf. point 13.4.4, p. 168). Ce service permet d'actualiser les bases antivirus et les modules utilisés par les applications de la version 6.0 sur les ordinateurs du réseau en réduisant le trafic Internet.

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 13.4.1, p. 161).

Vous pouvez lancer la mise à jour du logiciel depuis :

- le menu contextuel (cf. point 4.2, p. 43);
- la fenêtre principale du logiciel (cf. point 4.3, p. 44).

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

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

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

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

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

N'oubliez pas que la copie des mises à jour dans une source locale aura lieu en même temps que l'exécution de la mise à jour, pour autant que ce service ait été activé (cf. point 13.4.4, p. 168).

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 signatures des menaces avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau la version antérieure des signatures après une mise à jour ratée.

Cette possibilité d'annuler la mise à jour est utile si, par exemple, une partie des signatures a été corrompue suite à une déconnexion pendant la mise à jour. Vous pouvez ainsi revenir à la version précédente et tenter d'actualiser à nouveau les signatures ultérieurement.

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

1. Sélectionnez le composant **Mise à jour** dans la section **Service** dans la fenêtre principale du logiciel.

2. Cliquez sur le bouton **Retour à l'état précédent** (appel du programme depuis l'aide) dans la partie droite de la fenêtre principale).

13.3. Création de tâches liées à la mise à jour

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

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

Pour créer une nouvelle tâche de mise à jour :

1. Sélectionnez le point **Mise à jour** de la section **Service** dans la fenêtre principale, ouvrez le menu contextuel d'un clic droit et sélectionnez le point **Enregistrer sous**.

2. Saisissez le nom de la tâche dans la fenêtre qui s'affiche puis cliquez sur **OK**. La nouvelle tâche figure désormais dans la section **Service** de la fenêtre principale du logiciel.

Attention !

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

La nouvelle tâche applique tous les paramètre de la tâche qui lui a servi de modèle, à l'exception de la programmation. Le lancement automatique de la nouvelle tâche est désactivé par défaut. Vous devrez dès lors procéder à une configuration complémentaire: indiquer la source de la mise à jour (cf. point 13.4.1, page. 161), définir les paramètres de connexion (cf. point **13.4.3**, p. 166) et, le cas échéant activer le lancement avec les privilèges (cf. point 6.4, p. 75) et configurer la programmation (cf. point 6.5, p. 77).

Pour renommer une tâche :

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

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

Pour supprimer une tâche :

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

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

Attention !

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

13.4. Configuration de la mise à jour

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

- la ressource d'où les fichiers seront copiés avant d'être installés (cf. point 13.4.1, p. 161);
- le mode de lancement de la mise à jour du logiciel (cf. point 13.4.2, p. 164);
- les éléments actualisés
- les actions à réaliser après la mise à jour du logiciel (cf. point 13.4.4, p. 168).

Tous ces paramètres sont abordés en détails ci-après.

13.4.1. Sélection de la source de la mise à jour

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

Les *serveurs de mise 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 signatures des menaces et des modules internes pour tous les produits de Kaspersky Lab.

Attention !

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

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

La sélection de la source de la mise à jour s'opère dans l'onglet **Source de mise à jour** (cf. ill. 49).

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. L'adresse du serveur au départ duquel la mise à jour sera téléchargée sera placée automatiquement au début de la liste. Lors de le mise à jour suivante depuis les serveurs de Kaspersky Lab, le logiciel contactera en premier lieu le serveur ayant fourni la mise à jour précédente.

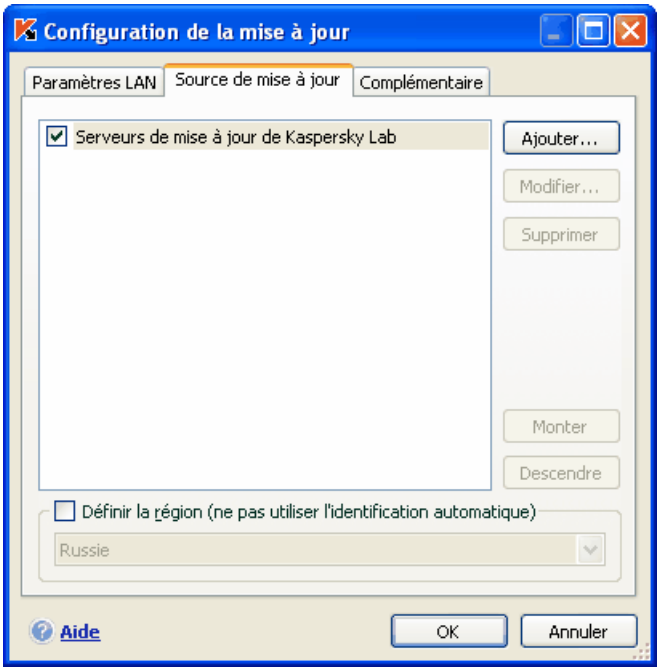


Illustration 49. Sélection de la source de la mise à jour

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

1. Cliquez sur **Ajouter…** ;
2. Sélectionnez le site FTP ou HTTP dans la fenêtre **Sélection de la source de mise à jour** ou indiquez son adresse IP, son nom symbolique ou l'URL dans le champ **Source**.

Attention !

Si vous avez sélectionné, en guise de source de mise à jour, une ressource située en dehors de l'intranet, il faudra prévoir un accès Internet.

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

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

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

Si plusieurs ressources ont été sélectionnées en guise de source de mise à jour, le logiciel les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible. Vous pouvez modifier l'ordre des sources dans la liste à l'aide des boutons **Monter**/**Descendre**

Modifiez la liste des sources à l'aide des boutons **Ajouter…**, **Modifier…**, **Supprimer**. Les serveurs de mise à jour de Kaspersky Lab 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.

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

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

Les objet de la mise à jour (cf. ill. 50) désignent les objets qui seront actualisés :

- Les signatures de menaces ;
- Les pilotes de réseau qui permettent aux composants de la protection d'intercepter le trafic de réseau ;
- Les modules de l'application.

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

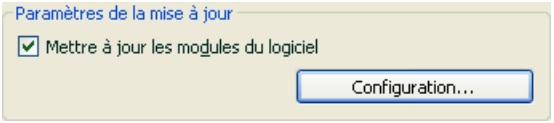


Illustration 50. Sélection des objets de la mise à jour

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

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

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

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

Le mode de mise à jour du logiciel (cf. ill. 51) désigne la manière dont la mise à jour sera lancée. Choisissez l'un des modes suivants :

Automatique. Kaspersky Anti-Virus vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source (cf. point 13.4.1, p. 161). 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 vous connectez à Internet à l'aide d'un modem et que vous avez choisi une ressource de réseau en tant que source de mise à jour, Kaspersky Anti-Virus tentera de réaliser la mise à jour selon un intervalle défini lors de la mise à jour antérieure. Les mises à jour réalisées au départ d'une source locales ont lieu à l'intervalle défini lors de la mise à jour précédente. Cela permet de régler automatiquement la fréquence des mises à jour en cas d'épidémie de virus ou d'autres situations dangereuses. Le logiciel recevra en temps opportuns les versions les plus récentes des signatures des menaces ou des modules de l'application, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

Illustration 51. 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 6.5 à la page 77).

Manuel. Vous lancez vous-même la procédure de mise à jour du logiciel. Kaspersky Anti-Virus vous avertira de la nécessité de réaliser la mise à jour :

- Tout d'abord, une infobulle apparaît au-dessus de l'icône de l'application dans la barre des tâches (pour autant que les notifications aient été activées) (cf. point 14.11.1, p. 201);
- Ensuite, le deuxième indice dans la fenêtre principale de l'application vous signale que la protection de l'ordinateur est dépassée (cf. point 5.1.1, p. 50);
- Troisièmement, la section des commentaires et des conseils de la fenêtre principale affiche des conseils sur la mise à jour du logiciel (cf. point 4.3, p. 44).

13.4.3. Configuration des paramètres de connexion

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

Tous les paramètres sont regroupés sur l'onglet spécial **Paramètres LAN** (cf. ill. 52).

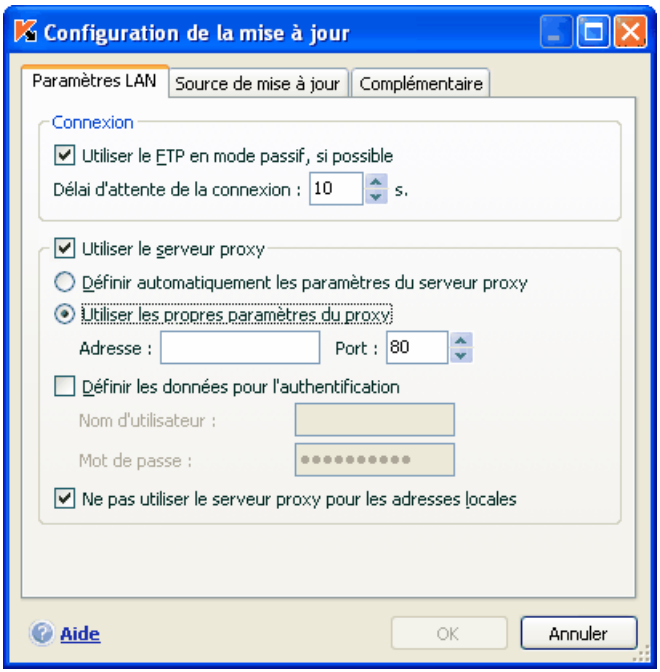


Illustration 52. Configuration des paramètres de réseau de la mise à jour

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

Précisez dans le champ **Délai d'attente de la connexion (sec)** la durée limite pour établir une connexion avec le serveur de mise à jour. Si la connexion n'a pu être établie à l'issue de cet intervalle, l'application tentera d'établir la connexion avec le serveur de mise à jour suivant. Ce processus se poursuit tant qu'une

connexion n'a pu être établie et tant que tous les serveurs disponibles n'ont pas été sollicités.

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

- Sélectionnez les paramètres du serveur proxy à utiliser pour la mise à jour :

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

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

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

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

  Si la case n'est pas cochée ou si les données ne sont pas définies, le système procédera à une tentative d'utilisation NTML en utilisant le compte utilisateur au nom duquel la mise à jour est lancée (cf. point 6.4, p. 75).

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

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

Ce paramètre n'est pas disponible si le logiciel est installé sous Microsoft Windows 9X/NT 4.0. Toutefois, le serveur proxy pour les adresses locales n'est pas utilisé par défaut.

13.4.4. Copie des mises à jour

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

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

Pour activer la copie des mises à jour, cochez la case **Copier dans le répertoire** de l'onglet **Complémentaire** (cf. ill. 53) 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.

Vous pouvez également définir le mode de copie des mises à jour ::

- *Complet* :pour la copie des signatures de menaces et des composants de toutes les applications de Kaspersky Lab de la version 6.0. Pour choisir la mise à jour complète, cochez la case **Copier les mises à jour de tous les composants**.
- *Partiel :* pour la copie des signatures de menaces et des mises à jour uniquement pour les composants installés de Kaspersky Anti-Virus 6.0. Pour choisir ce mode de mise à jour, il faut désélectionner la case **Copier les mises à jour de tous les composants**.

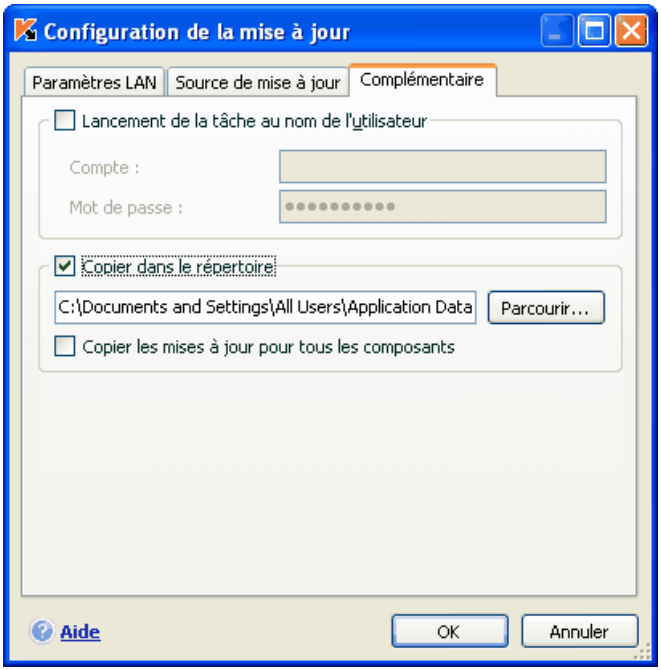


Illustration 53. Configuration du service de copie des mises à jour

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

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

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

13.4.5. Actions exécutées après la mise à jour du logiciel

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

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

Pourquoi ces objets et pas d'autres ?

La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infecté (cf. point 14.1, p. 172). Il se peut que la version actualisée des signatures des menaces de Kaspersky Anti-Virus puisse reconnaître et neutraliser le danger.

Par défaut, le logiciel analyse les objets en quarantaine après chaque mise à jour des signatures des menaces connues. Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et 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. 137). Il est conseillé de configurer le lancement automatique de cette tâche après chaque mise à jour des signatures des menaces (cf. point 6.5, p. 77).

CHAPITRE 14. 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 14.2, p. 176). Si un objet qui contenait des informations importantes n'a pu être complètement préservé pendant le traitement antivirus, vous pourrez toujours le restaurer au départ de la copie de sauvegarde.
- La quarantaine contient les objets potentiellement infectés qui n'ont pas pu être traités avec les signatures actuelles des menaces (cf. point 14.1, p. 172).

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 14.5, p. 188). Les experts de Kaspersky Lab ont tenté d'inclure tous les moyens possibles d'apporter cette assistance : assistance en ligne, forum de questions et de suggestions des utilisateurs, etc.
- Le service de notification des événements permet de configurer la notification aux utilisateurs des événements importants dans le fonctionnement de Kaspersky Anti-Virus (cf. point 14.11.1, p. 201). Il peut s'agir d'événements à caractère informatif ou d'erreurs qui nécessitent une réaction immédiate et dont il faut avoir conscience.
- L'autodéfense du logiciel et la restriction de l'accès protège les propres fichiers du logiciel contre les modifications réalisées par des personnes mal intentionnées, interdit l'administration externe du logiciel par des services et introduit des restrictions sur l'exécution de certaines actions à l'aide de Kaspersky Anti-Virus (cf. point 14.11.1.3, p. 204). Par exemple, une modification du niveau de protection peut fortement influencer la sécurité des données sauvegardées sur votre ordinateur.

- Le service d'administration des clés de licence vous permet d'obtenir des informations complémentaires sur la licence utilisée, d'activer votre copie du logiciel et d'administrer les fichiers des clés de licence (cf. point 14.5, p. 188).

Le logiciel propose également une aide (cf. point 14.3.7, p. 186) détaillée et des rapports complets (cf. point 14.3, p. 178) sur le fonctionnement de tous les composants de la protection et l'exécution de toutes les tâches liées à la recherche de virus.

La constitution de la liste des ports permet de régler le contrôle des données qui transitent via les ports issues de certains composants de protection de Kaspersky Anti-Virus (cf. point 14.7, p. 191).

La création d'un disque de secours permet de ramener l'ordinateur à l'état antérieur à l'infection (cf. point 14.10, p. 197). 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 0, p. 193).

Examinons en détails ces différents services.

14.1. Quarantaine pour les objets potentiellement infectés

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

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

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

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

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

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

  Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Anti-Virus le classe comme un objet potentiellement infecté.

L'analyseur heuristique de code, qui permet de déceler jusqu'à 92% des nouveaux virus, 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 **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.

14.1.1. Manipulation des objets en quarantaine

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

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

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

Pour manipuler les objets en quarantaine :

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

Vous pouvez réaliser les opérations suivantes dans l'onglet quarantaine (cf. ill. 54) :

- 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*.

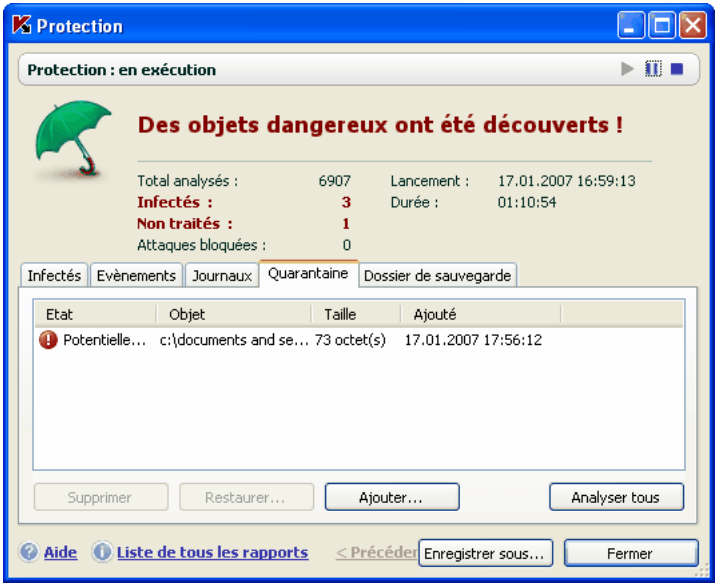


Illustration 54. Liste des objets en quarantaine

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

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

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

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

- 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. 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**.

14.1.2. Configuration de la quarantaine

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

- Définir le mode d'analyse automatique des objets en quarantaine après chaque mise à jour des signatures des menaces (pour de plus amples informations, consultez le point 13.4.4 à la page 168)

  Attention !

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

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

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

  Pour ce faire :

  3. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
  4. Sélectionnez **Rapports** dans l'arborescence.

5. Définissez dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. ill. 55) le délai de conservation au terme duquel les objets seront automatiquement supprimés.

Illustration 55. Configuration de la conservation des objets en quarantaine

14.2. 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.

14.2.1. Manipulation des copies de sauvegarde

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

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

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

Pour manipuler les copies des objets dangereux :

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

La partie centrale de l'onglet (cf. ill. 56) 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.

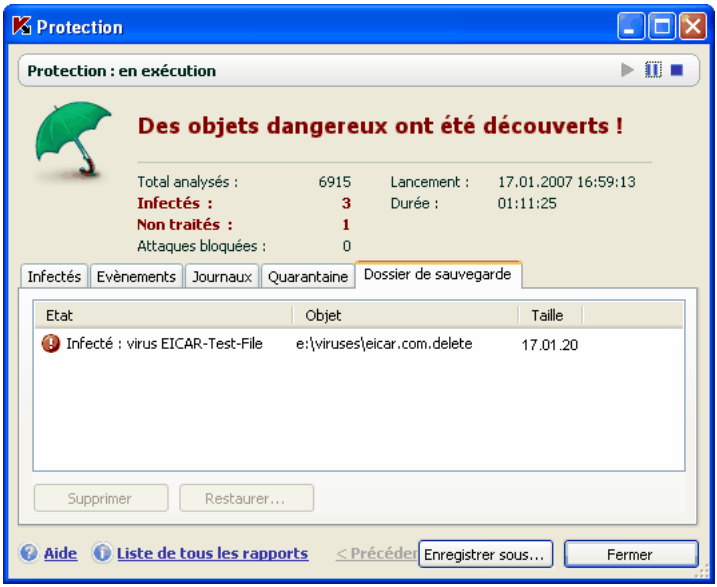


Illustration 56. Copies de sauvegarde des objets supprimés ou réparés

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

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

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

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

Il est conseillé d'examiner fréquemment le contenu du dossier et de le nettoyer à l'aide du bouton **Supprimer**. Vous pouvez également configurer l'application afin qu'elle supprime les copies les plus anciennes du répertoire (cf. point 14.2.2, p. 178).

14.2.2. 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 des paramètres de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Rapports** dans l'arborescence.
3. Définissez le délai de conservation des copies de sauvegarde dans le bloc **Quarantaine et Dossier de sauvegarde** (cf. ill. 55) dans la partie droite de la fenêtre.

14.3. 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 les **Rapports** de la section **Service** de la fenêtre principale du logiciel. Ces informations sont reprises dans le bloc **Rapports**.

Pour consulter les rapports :

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

La fenêtre s'ouvre sur l'onglet **Rapports** (cf. ill. 57). Vous y verrez les derniers rapports sur tous les composants et les tâches antivirus lancées au cours de cette session de Kaspersky Anti-Virus. Le résultat du fonctionnement est affiché en regard de chaque composant ou tâche. Exemple, *interrompu(e)* ou *terminée.* Si vous souhaitez consulter l'historique complet des rapports pour la session en cours, cochez la case **Afficher l'historique des rapports**.

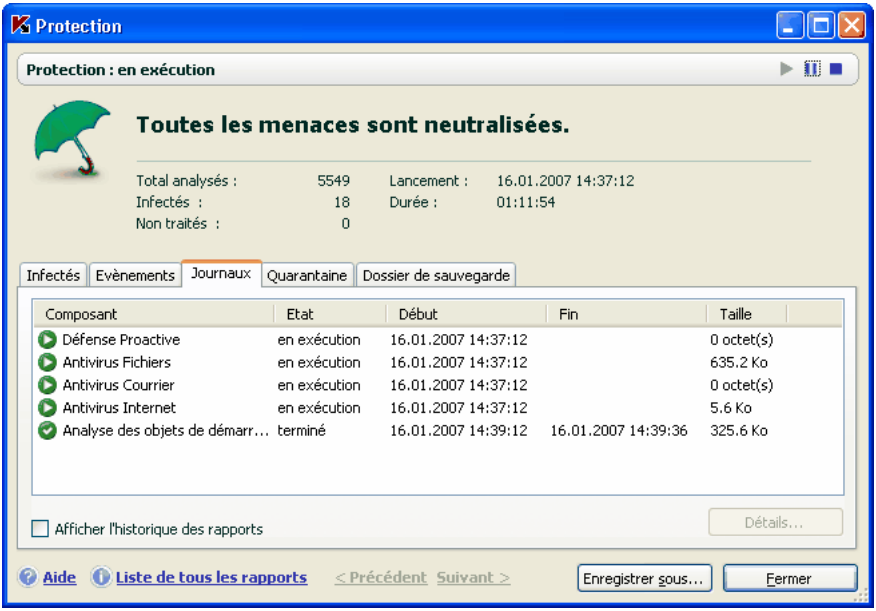


Illustration 57. Rapports sur le fonctionnement des composants du programme

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 **Infectés** contient la liste des objets dangereux découverts par le logiciel.
- **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 signatures des menaces.
- Les onglets **Macros** et **Registres** apparaissent uniquement dans le rapport de la défense proactive. Ils fournissent des informations sur toutes tentatives d'exécution de macros sur l'ordinateur et sur toutes les tentatives de modification de la base de registres système du système d'exploitation.

Tout le rapport peut être exporter dans un fichier au format texte. Cela peut-être utile lorsque vous ne parvenez pas à résoudre vous même un problème survenu pendant l'exécution d'une tâche ou le travail 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 **Enregistrer sous** et indiquez où vous souhaitez enregistrer le fichier.

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

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

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

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

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

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

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

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

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

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

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

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

14.3.1. Configuration des paramètres du rapport

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

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Anti-Virus en cliquant sur Configuration dans la fenêtre principale du logiciel.
2. Sélectionnez **Rapports** dans l'arborescence des paramètres.
3. Dans le bloc **Rapport** (cf. ill. 58), 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 58. Configuration des paramètres de constitution des rapports

14.3.2. Onglet Infectés

Cet onglet (cf. ill. 59) 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**.

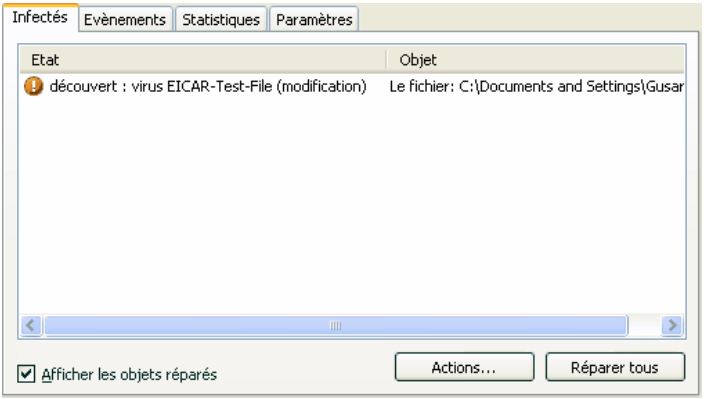


Illustration 59. Liste des objets dangereux découverts

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.

14.3.3. Onglet Evénements

Cet onglet (cf. ill. 60) 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 des signatures des menaces, pour autant que ce comportement ne soit pas annulé par une règle de contrôle de l'activité (cf. point 10.1.1, p. 121).

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.

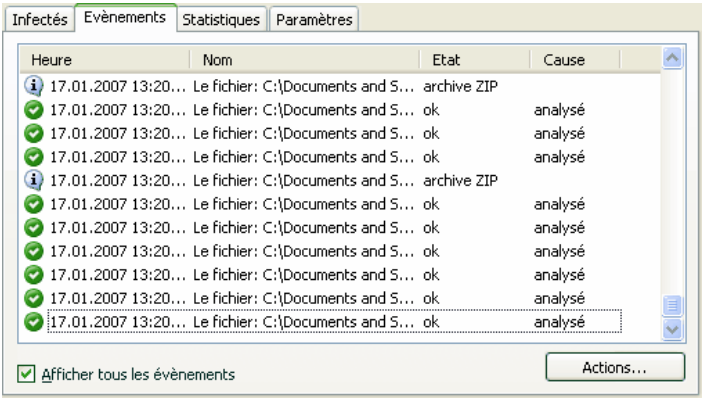


Illustration 60. Evénements survenus pendant

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.

14.3.4. 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. 61). 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.

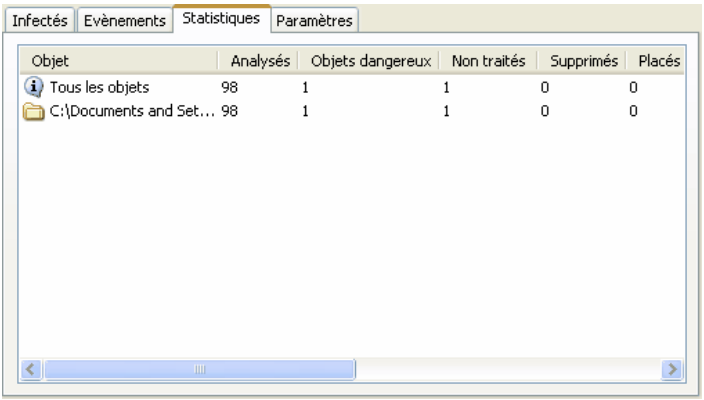


Illustration 61. Statistique du composant

14.3.5. Onglet Paramètres

Cet onglet (cf. ill. 62) présente tous les paramètres qui définissent le fonctionnement du composant 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. i 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.

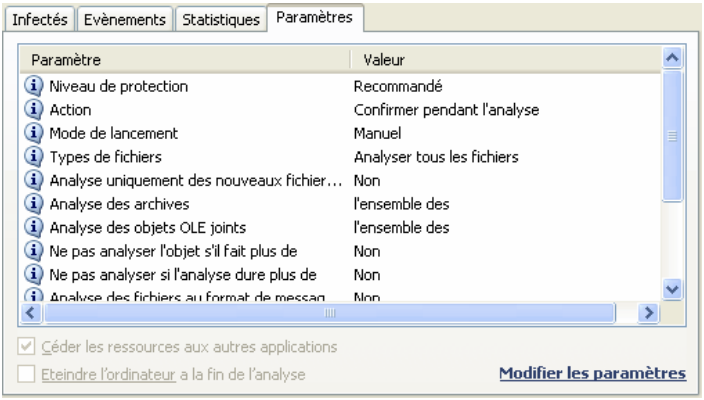


Illustration 62. Paramètres de fonctionnement du composant

- 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.

14.3.6. Onglet *Macros*

Toutes les macros que le système a tenté d'exécuter pendant la séance actuelle de Kaspersky Anti-Virus sont reprises sur l'onglet **Macros** (cf. ill. 63). Le rapport reprend le nom complet de chaque macro, l'heure de l'exécution et l'état suite au traitement de la macro.

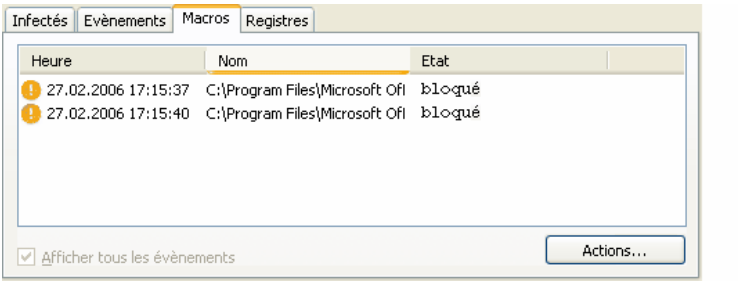


Illustration 63. Liste des macros dangereuses découvertes

Vous pouvez définir les événements que vous souhaitez voir sur cet onglet du rapport. Pour annuler la consultation des informations, désélectionnez la case

Afficher tous les événements

14.3.7. 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. 64), si l'enregistrement n'est pas contraire à la règle (cf. point 10.1.4.2, p. 135).

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.

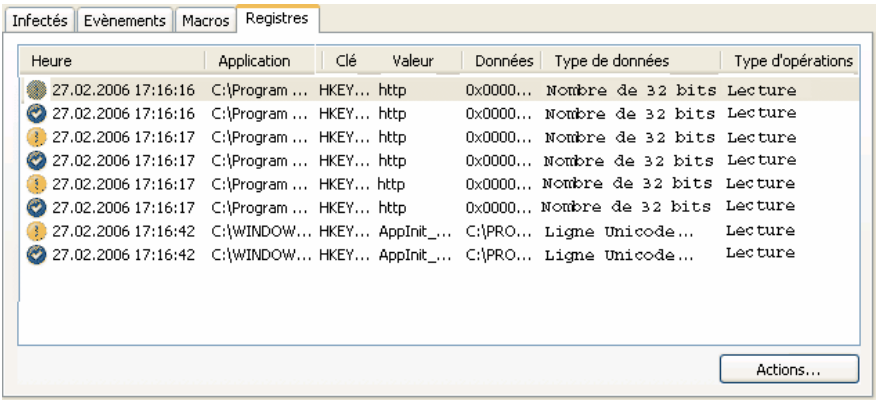


Illustration 64. Lecture et modification de clés de la base de registre

14.4. Informations générales sur le logiciel

La section **Service** de la fenêtre principale affiche des informations générales sur le logiciel (cf. ill. 65).

Ces informations sont scindées en trois blocs :

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

Toutes ces informations sont nécessaires lors des contacts avec le service d'Assistance technique de Kaspersky Lab (cf. point 14.5, p. 188).

Illustration 65. Informations relatives au logiciel, à la licence et au système sur lequel il est installé

14.5. Administration des licences

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

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

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

Une fois la licence commerciale expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettra à jour les signatures des menaces. Vous pourrez toujours analyser le serveur à l'aide de la recherche de virus et utiliser l'Antivirus Fichiers, mais uniquement sur la base des signatures des menaces d'actualité à la fin de validité de la licence. Par conséquent, nous ne

pouvons pas garantir une protection totale contre les nouveaux virus qui apparaîtraient après l'expiration de la licence.

Afin que le serveur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la licence d'utilisation de Kaspersky Anti-Virus. Deux semaines avant la date d'expiration, le programme vous avertira. Au cours des deux semaines suivantes, le programme affichera à chaque démarrage le message de circonstance.

Afin de renouveler la licence, vous devez absolument obtenir une nouvelle clé de licence. Pour ce faire :

1. Contactez la société où vous avez acheté le logiciel et achetez une clé de licence.

ou:

Achetez une nouvelle clé de licence ou un code d'activation directement chez Kaspersky Lab en cliquant sur le lien Activer dans la fenêtre des clés de licence. Remplissez le formulaire qui s'affiche dans notre site. Dès que le paiement aura été confirmé, la clé de licence ou le code d'activation de l'application sera envoyé à l'adresse électronique indiquée dans le formulaire de commande.

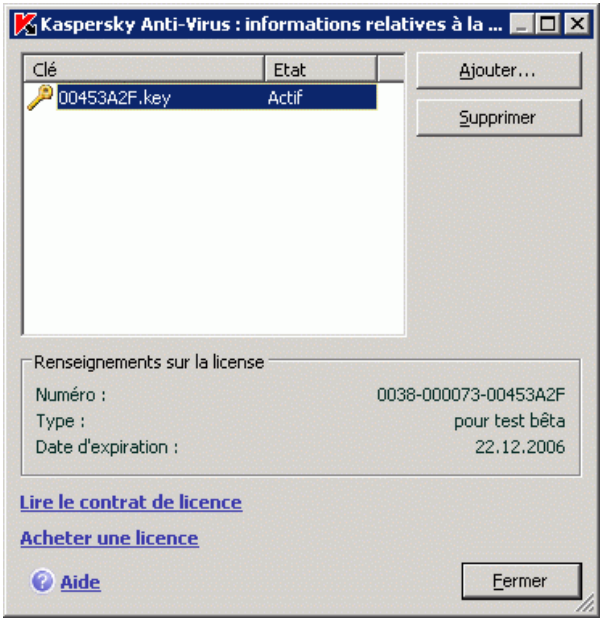


Illustration 66. Informations relatives à la licence

Les informations relatives à la clé de licence utilisée figurent dans le bloc **Informations relatives à la licence** de la section **Services** dans la fenêtre principale de l'application. Pour ouvrir la fenêtre d'administration des licences, cliquez avec le bouton gauche de la souris n'importe où dans le bloc. La fenêtre qui s'ouvre (cf. ill. 66) vous permet de consulter les informations sur la clé active, d'en ajouter une ou de la supprimer

Lorsque vous sélectionnez une clé dans la liste du bloc **Informations relatives à la clé**, vous pourrez voir le numéro de la clé, son type et sa durée de validité. Pour ajouter une nouvelle clé de licence, cliquez sur le bouton **Ajouter** et activez l'application à l'aide de l'Assistant d'activation (cf. point 14.5, p. 188). Pour supprimer une clé de la liste, cliquez sur **Supprimer**.

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

14.6. Service d'assistance technique aux utilisateurs

Kaspersky Anti-Virus vous offre un large éventail de possibilités pour régler les problèmes et les questions liées à l'utilisation du logiciel. Ils sont tous repris sous **Assistance technique** (cf. ill. 67) dans la section **Service**.

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

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

Assistance Technique en ligne. Cette solution permet une approche pas à pas de la définitions du souci rencontré afin de vous offrir la solution adéquate. Site internet : http://case.kaspersky.fr

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

Illustration 67. Informations relatives à l'assistance technique

14.7. 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 boîte de dialogue de configuration de Kaspersky Anti-Virus en cliquant sur le lien Configuration de la fenêtre principale.

2. Sélectionnez **Configuration du réseau** dans le groupe **Service** de l'arborescence des paramètres du logiciel.
3. Dans la partie droite de la fenêtre de configuration, cliquez sur **Configuration des ports**.
4. Modifiez la liste des ports soumis à un contrôle dans la fenêtre qui s'ouvre(cf. ill. 68).

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**.

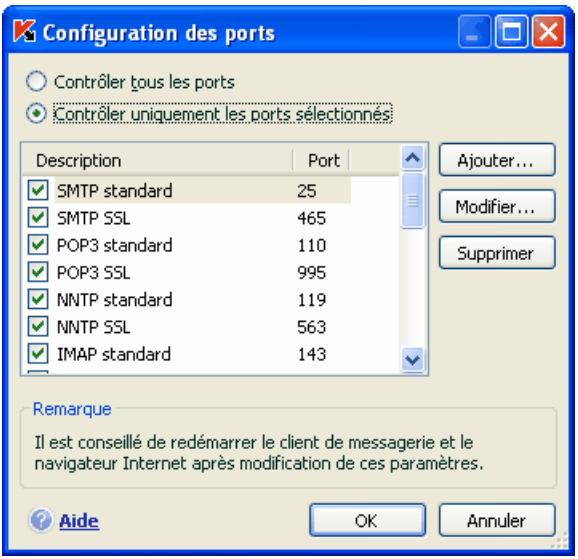


Illustration 68. Liste des ports contrôlés

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 conjointement Kaspersky Anti-Virus et un pare-feu d'un autre éditeur, il faudra créer dans les paramètres de celui-ci une règle d'autorisation pour le processus *avp.exe* (processus interne de Kaspersky Anti-Virus) pour tous les ports cités.

Supposons que le pare-feu possède une règle pour le processus *iexplorer.exe* qui autorise l'établissement d'une connexion pour ce processus sur le port 80.

Cependant, Kaspersky Anti-Virus, qui a intercepté une demande de connexion sur le port 80 à la demande du processus *iexplorer.exe*, transmet le processus à *avp.exe* qui tente à son tour d'établir une connexion avec la page Internet sollicitée. Si aucune règle d'autorisation n'existe pour le processus *avp.exe*, le pare-feu bloquera cette requête. Et l'utilisateur ne pourra pas accéder à la page Web.

14.8. Analyse de la connexion SSL

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 6.0 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. Vous devrez décider s'il est nécessaire ou non de soumettre cette connexion à la recherche de virus :

- **Traiter** : procéder à la recherche de virus lors de la connexion à une ressource en ligne en mode sécurisé.

  Nous vous conseillons d'analyser le trafic SSL si vous vous trouvez sur une ressource en ligne suspecte ou lors de l'ouverture d'une page

exécutant le transfert de données via SSL. Il s'agit probablement d'un indice du début de transfert d'un programme malveillant via le protocole sécurité.

- **Ignorer** : poursuivre la connexion avec la ressource en ligne en mode sécurisé sans recherche la présence d'éventuels virus dans le trafic.

Pour appliquer ultérieurement l'action choisie à chaque tentative de connexion SSL, cochez la case **Appliquer à tous**

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. Il est conseillé de désactiver l'analyse du trafic SSL dans les cas suivants :

- Lors de la connexion à une ressource de confiance telle que le site de votre banque où vous gérer 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.

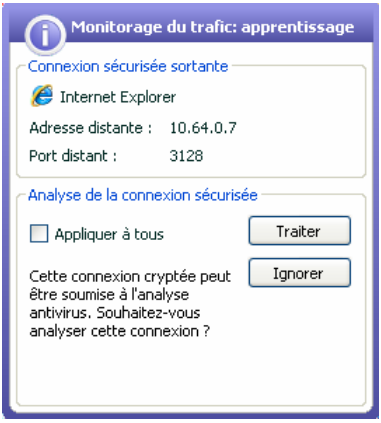


Illustration 69. Notification de la découverte d'une connexion SSL

La configuration de l'analyse de la connexion SSL s'opère sur l'onglet **Configuration du réseau** de la fenêtre de configuration de l'application :

Analyser toutes les connexions SSL : recherche la présence de virus dans tout le trafic qui transite via le protocole SSL.

Confirmer en cas de découverte d'une connexion SSL : demande la confirmation de l'utilisateur à chaque tentative d'établissement d'une connexion SSL.

Ne pas analyser les connexions SSL : absence de recherche de virus dans le trafic transmis via le protocole SSL.

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

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

Pour configurer l'interface du logiciel :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Anti-Virus à l'aide du lien Configuration de la fenêtre principale.
2. Sélectionnez **Apparence** dans le groupe **Service** de l'arborescence des paramètres du logiciel (cf. ill. 70).

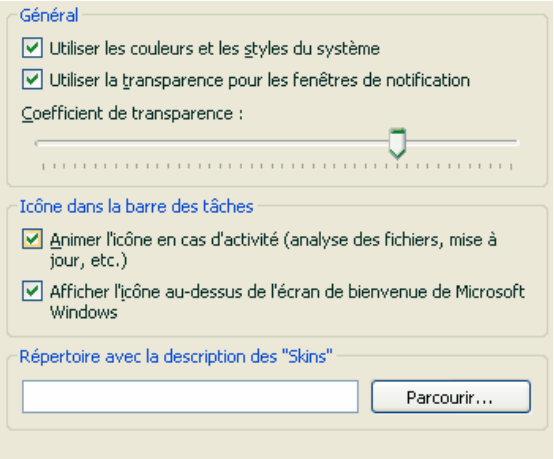


Illustration 70. Configuration de l'interface du programme

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

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

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

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

  L'icône de l'application dans la barre des tâches varie en fonction de l'opération exécutée. 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 apparaît est grisée.

- Degré de transparence des infobulles.

  Toutes les opérations de Kaspersky Anti-Virus au sujet desquelles vous devez être alerté immédiatement ou qui nécessitent une prise de décision rapide sont annoncées sous la forme d'une infobulle qui apparaît au-dessus de l'icône de l'application dans la barre des tâches. Ces infobulles sont transparentes afin de ne pas vous perturber dans votre travail. Le fond de l'infobulle devient solide dès que vous placer le curseur de la souris sur la fenêtre. Il est possible de modifier le degré de transparence de ces infobulles. Pour ce faire, faites glisser le curseur de l'échelle **Coefficient de transparence** jusqu'au niveau requis. Afin de supprimer la transparence des messages, désélectionnez la case **Utiliser la transparence pour les fenêtres de notification**.

  > Cette fonction n'est pas disponible dans les versions installées sous Microsoft Windows 98/NT 4.0/ME.

- Utilisation d'éléments graphiques propres et de la palette des de couleurs dans l'interface du logiciel.

  Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de Kaspersky Anti-Virus peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel, localiser l'interface dans la langue de votre choix. Pour activer votre propre environnement graphique, indiquez le répertoire avec ses paramètres dans le champ **Répertoire avec la description des "Skins"**. Cliquez sur **Parcourir** pour sélectionner le répertoire

Les couleurs et les styles du système sont utilisés par défaut. Si vous souhaitez en utiliser d'autres, désélectionnez la case ☑ **Utiliser les couleurs et les styles du système**. Dans ce cas, le système utilisera les styles que vous aurez indiqués lors de la configuration de l'environnement graphique.

N'oubliez pas que la configuration personnalisée de l'interface de Kaspersky Anti-Virus n'est pas préservée lors du rétablissement des paramètres par défaut ou de la suppression du programme.

14.10. Disque de secours

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

Le disque de secours 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 signatures des menaces.

Afin de créer le disque de secours:

1. Ouvrez la fenêtre principale du logiciel et sélectionnez **Disque de secours** dans la section **Service**.
2. Cliquez sur **Lancement de l'Assistant** afin de lancer la création du disque de secours.

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.

14.10.1. Création d'un disque de secours de restauration

Attention ! Afin de pouvoir créer ce disque de secours, 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 spécial PE Builder.

Afin de créer un disque de secours 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 un 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 secours avant la création du cédérom.

  Si ce n'est pas la première fois que vous créez un disque de secours, 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 secours contient les anciennes signatures des menaces. Afin de garantir la meilleure recherche de virus et la restauration du système, il est conseillé d'actualiser les signatures des menaces et de créer une nouvelle version du disque de secours.
- 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 secours. Attendez la fin du processus. Cela peut durer quelques minutes.

Etape 10. Création d'un fichier ISO

Une fois que PE Builder aura terminé de créer les fichiers du disque de secours, la fenêtre **Création d'un fichier ISO** s'ouvrira.

Le fichier ISO est une image du futur disque de secours 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 11. Enregistrement du disque

Cette fenêtre de l'Assistant vous permet de choisir quand enregistrer les fichiers du disque de secours sur le cédérom : maintenant ou plus tard.

Si vous avez sélectionné l'enregistrement immédiat du disque, indiquez s'il faut nettoyer le contenu du lecteur de cédérom avant de procéder à l'enregistrement. Pour ce faire, cochez la case correspondante. Cette possibilité est accessible uniquement si le graveur de cédérom est compatible avec les cédéroms 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 12. Fin de la création du disque de secours

Cette fenêtre de l'assistant vous informe de la réussite de la création du disque de secours.

14.10.2. Utilisation du disque de secours

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 secours 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 des signatures des virus 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→Programmess→Kaspersky Anti-Virus 6.0→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 signatures de menaces qui étaient d'actualité lors de la création du disque de secours. Pour cette raison, il est conseillé d'actualiser les bases avant de lancer l'analyse.

Pensez également au fait que les bases de signatures de menace 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.

14.11. Utilisation des services complémentaires

Kaspersky Anti-Virus vous propose également les services complémentaires suivants :

- Avertissement de l'utilisateur par courrier électronique en cas d'événements particuliers.
- Autodéfense de Kaspersky Anti-Virus contre la désactivation, la suppression ou la modification des modules et protection de l'accès au logiciel par mot de passe.
- Résolution des problèmes de compatibilité entre Kaspersky Anti-Virus 6.0 et d'autres applications (cf. point **14.11.3**, p. 208).

14.11.1. Notifications relatives aux événements de Kaspersky Anti-Virus

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

Afin d'être au courant de ce qui se passe dans le cadre du fonctionnement de Kaspersky Anti-Virus, vous pouvez activer le service de notification.

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

- Infobulles au-dessus de l'icône du logiciel dans la barre des tâches.
- Notification sonore.
- Messages électroniques.
- Consignation des informations dans le journal des événements.

Pour utiliser ce service :

1. Cochez la case ☑ **Activer les notifications des événements** dans le bloc **Interaction avec l'utilisateur**(cf. ill. 71).

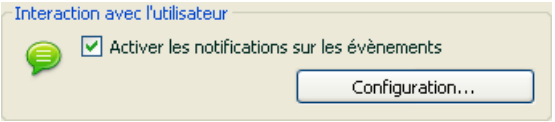


Illustration 71. Activation des notifications

2. Définir le type d'événements de Kaspersky Anti-Virus au sujet desquels vous souhaitez être averti, ainsi que le mode de notification (cf. point 14.11.1.1, p. 202).
3. Configurez les paramètres d'envoi des notifications par courrier électronique si vous avez choisi ce mode (cf. point 14.11.1.2, p. 204).

14.11.1.1. Types de notification et mode d'envoi des notifications

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus.

Evénements critiques. Evénements critiques au sujet desquels il est vivement conseillé d'être averti car ils indiquent un problème dans le fonctionnement du logiciel ou une vulnérabilité dans la protection de l'ordinateur. Par exemple, *signatures des menaces corrompues* ou *expiration de la validité de la licence*.

Refus de fonctionnement. Evénement qui empêche le fonctionnement de l'application. Par exemple, absence de licence ou de signatures des menaces.

Evénements importants. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le fonctionnement du logiciel. Exemple : *protection désactivée* ou *l'analyse antivirus de l'ordinateur a été réalisée il y a longtemps*.

Evénements informatifs. Evénements à caractère purement informatif qui ne contient aucune information cruciale. Exemple : *tous les objets dangereux ont été réparés*.

Afin d'indiquer les événements au sujet desquels vous souhaitez être averti et de quelle manière :

1. Cliquez sur le lien Configuration dans la fenêtre principale du logiciel.
2. Dans la boîte de configuration du logiciel, sélectionnez la section **Service**, cochez la case ☑ **Activer les notifications sur les événements** et passez à la configuration détaillée en cliquant sur **Complémentaire**.

Dans la fenêtre **Configuration des notifications** (cf. ill. 72) , vous pouvez définir les modes d'envoi suivants pour les notifications :

- *Infobulles* au-dessus de l'icône du logiciel dans la barre des tâches contenant les informations relatives à l'événement ;

  Pour utiliser ce mode, cochez la case ☑ dans le schéma **Ecran** en regard de l'événement au sujet duquel vous souhaitez être averti.

- *Notification sonore.*

  Si vous voulez accompagner cette infobulle d'un effet sonore, cochez la case ☑ dans la partie **Son** en regard de l'événement.

- *Notification par courrier* électronique.

  Pour utiliser ce mode, cochez la case ☑ **Message** en regard de l'événement au sujet duquel vous souhaitez être averti et configurez les paramètres d'envoi des notifications (cf. point 14.11.1.2, p. 204).

- *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 **Evènements** et configurez les paramètres du journal des événements (cf. point 14.11.1.3, p. 205).

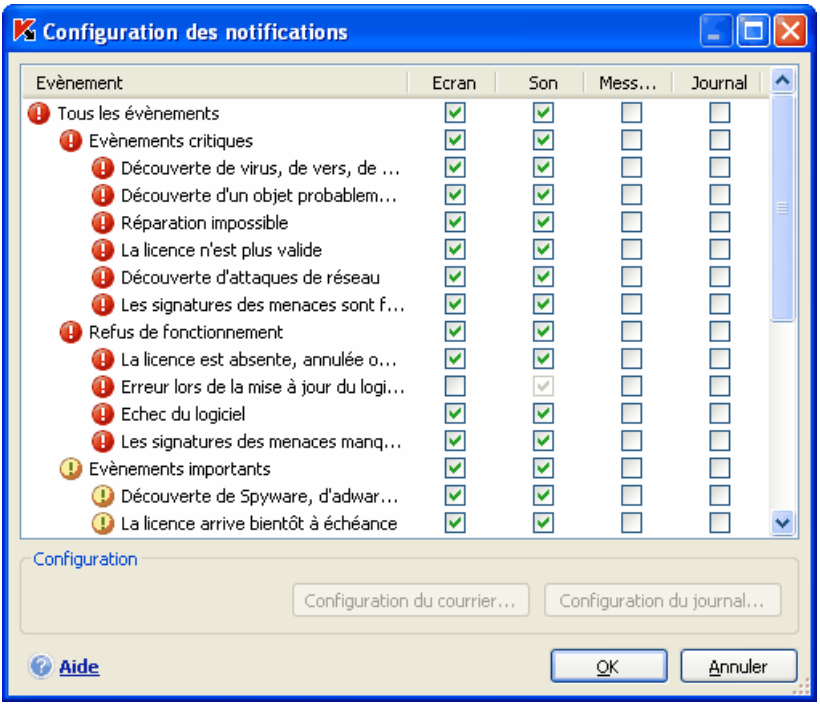


Illustration 72. Evénement survenus pendant le fonctionnement du logiciel et modes de notification choisis.

14.11.1.2. Configuration de l'envoi des notifications par courrier électronique

Après avoir sélectionné les événements (cf. point 14.11.1.1, p. 202)au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications. Pour ce faire :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Service** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Complémentaire** dans le bloc **Interaction avec l'utilisateur** de la partie droite de la fenêtre.
4. Sur l'onglet **Configuration de notifications**, cochez la case ☑ dans la partie **E-mail** pour les événements qui déclencheront l'envoi d'une notification par courrier électronique.

5. Dans la fenêtre qui s'ouvre à l'aide du bouton **Configuration du courrier**, définissez les paramètres suivants pour l'envoi des notifications par courrier:

   - Définissez les paramètres d'expédition de la notification dans le bloc **Envoi de la notification au nom de l'utilisateur**.
   - 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.

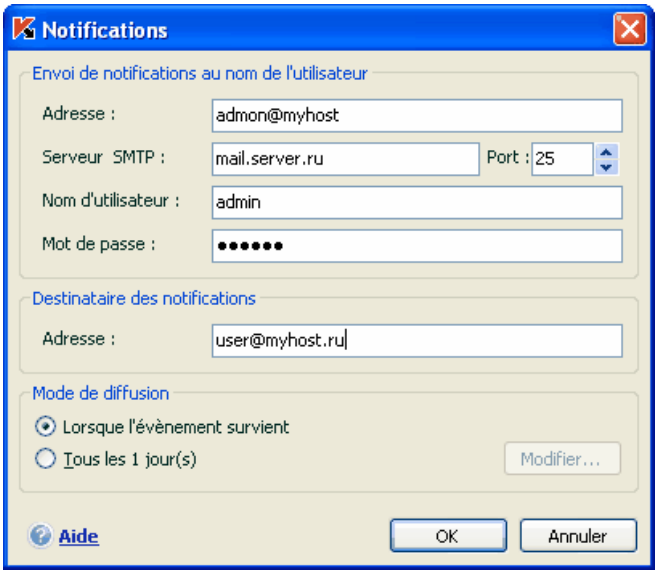


Illustration 73. Configuration de la notification par courrier électronique

14.11.1.3. Configuration du journal des événements

Pour configurer le journal des événements :

1. Cliquez sur le lien Configuration dans la fenêtre principale afin d'ouvrir la fenêtre de configuration de l'application.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Complémentaire** du bloc **Interaction avec l'utilisateur** dans la partie droite de la fenêtre.

Dans la fenêtre **Configuration des notifications**, sélectionnez le type d'événements que vous voulez enregistrer dans le journal et cliquez sur le bouton **Configuration du journal**.

Kaspersky Anti-Virus permet d'enregistrer les informations relatives aux événements survenus pendant l'utilisation de l'application dans le journal général de Microsoft Windows (**Applications**) ou dans le journal séparé des événements de Kaspersky Anti-Virus (**Kaspersky Event Log**).

Sur un ordinateur tournant sous Microsoft Windows 98/ME, il est impossible de consigner les événements dans le journal et sous Microsoft Windows NT 4.0 il est impossible de les consigner dans **Kaspersky Event Log**.

Ces restrictions sont imposées par les particularités de ces systèmes d'exploitation.

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.

14.11.2. 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.

L'autodéfense de l'application n'est pas disponible dans Kaspersky Anti-Virus sur

un ordinateur tournant sous Microsoft Windows 98/ME

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 des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Service** dans l'arborescence des paramètres.
3. Opérez la configuration requise dans le bloc **Autodéfense** (cf. ill. 74) :

   ☑ **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

   Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la barre des tâches en cas de tentative d'exécution des actions citées (si le service de notification n'a pas été désactivé).

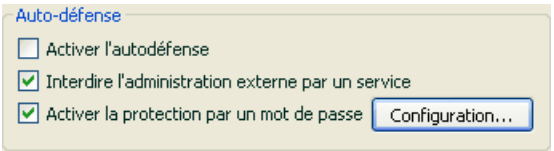


Illustration 74. Configuration de la protection du programme

Afin de limiter l'accès au logiciel à l'aide d'un mot de passe, cochez la case ☑ **Activer la protection par un mot de passe** et dans la fenêtre qui s'ouvre une fois que vous aurez cliqué sur Configuration, précisez le mot de passe et le secteur d'application de celui-ci (cf. ill. 75). 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.

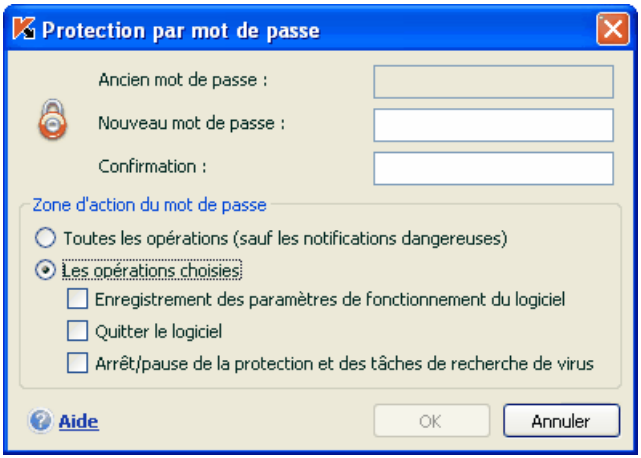


Illustration 75. Configuration de la protection par mot de passe

14.11.3. Résolution des problèmes de compatibilité entre Kaspersky Anti-Virus et d'autres applications

Des conflits peuvent survenir dans certains cas entre Kaspersky Anti-Virus et d'autres applications installées sur l'ordinateur. Cela est dû à la présence de mécanismes d'autodéfense intégrés à ces applications qui réagissent lorsque Kaspersky Anti-Virus tente de s'y introduire. Parmi les programmes réagissant ainsi, citons le module externe Authentica pour Adobe Reader qui se charge de l'analyse de l'accès aux fichiers PDF, Oxygen Phone Manager II, le programme d'administration des téléphones mobiles, et certains types de jeux protégés contre le crackage.

Pour résoudre ce problème, cochez la case **Compatibilité avec les applications auto-protégées** dans la section **Services** de la fenêtre de configuration de l'application. Il nous faut signaler que lorsque cette case est cochée, certaines fonctions de Kaspersky Anti-Virus ne seront plus disponibles (par exemple, l'analyse des macros, l'analyse de l'activité de l'application, l'analyse des scripts, etc.).

La modification de ce paramètre entrera en vigueur après le redémarrage du système d'exploitation.

14.12. Exportation/importation des paramètres de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet d'exporter et d'importer les paramètres de fonctionnement.

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 principale de Kaspersky Anti-Virus.
2. Cliquez sur le lien **Configuration** dans la section **Service**.
3. Cliquez sur le bouton **Exporter** dans le bloc **Profil de configuration.**
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

Pour importer les paramètres du fichier de configuration :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus.
2. Cliquez sur le lien **Configuration** dans la section **Service**.
3. Cliquez sur **Importer** et sélectionnez le fichier contenant les paramètres que vous souhaitez importer dans Kaspersky Anti-Virus.

14.13. Restauration des paramètres par défaut

Vous pouvez toujours revenir aux paramètres recommandés du logiciel. Ces paramètres sont les paramètres optimaux recommandés par les experts de

Kaspersky Lab. La restauration s'opère à l'aide de l'Assistant de configuration initiale du logiciel.

Pour restaurer les paramètres de protection :

1. Sélectionnez la section **Service** et ouvrez la fenêtre des paramètres du logiciel à l'aide du lien Configuration.
2. Cliquez sur le bouton **Par défaut** dans la section **Profil de 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 les listes "blanche" et "noire" des expressions et des adresses utilisées par Anti-Spam, la liste des adresses Internet et des numéros d'accès de confiance utilisée par l'antivirus Internet et Anti-Escroc, les règles d'exclusion pour les composants du programme, les règles de filtrage des paquets et les règles des applications d'Anti-Hacker 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. 34). 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

CHAPITRE 15. 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 signatures des menaces et des modules du programme;
- Appel de l'aide relative à la syntaxe de la ligne de commande;
- Appel de l'aide relative à la syntaxe de la ligne de commande;

La syntaxe de la ligne de commande est la suivante :

```
avp.com <commande> [paramètres]
```

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 clé de licence
START	lancement du composant ou de la tâche
PAUSE	suspension du composant ou de la tâche

RESUME	reprise du fonctionnement du composant ou de la tâche
STOP	arrêt du composant ou de la tâche
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
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 l'application
EXPORT	exportation des paramètres de protection de l'application

Chaque commande possède ses propres paramètres, propres à chaque composant de Kaspersky Anti-Virus.

15.1. Activation de l'application

L'activation de l'activation peut être réalisée de deux manières :

- Via Internet à l'aide d'un code d'activation (commande ACTIVATE);
- Via le fichier de clé de licence (commande ADDKEY).

Syntaxe de la commande :

```
ACTIVATE <code d'activation>
ADDKEY <nom du fichier>
```

Description des paramètres :

<code d'activation>	Code d'activation de l'application fournit à l'achat de celle-ci.
<nom du fichier>	Nom du fichier de clé de licence de l'application avec l'extension **.key*.

Exemple :

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key
```

15.2. Administration des composants de l'application et des tâches

L'administration des composants et des tâches de Kaspersky Anti-Virus au départ de la ligne de commande s'opère à l'aide des commandes suivantes :

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

La tâche ou le composant auquel la commande sera appliquée est définie par son paramètre.

Les commandes STOP et PAUSE sont exécutées uniquement sous saisie du mot de passe de Kaspersky Anti-Virus, défini via l'interface du logiciel.

Syntaxe de la commande :

```
avp.com <commande> <profile|taskid>
avp.com STOP
```

```
PAUSE <profile|taskid> /password=<mot de passe>
```

<profile|taskid> est remplacé par l'une des valeurs suivantes :

RTP	Tous les composants de la protection
FM	Antivirus de fichiers
EM	Antivirus de courrier électronique
WM	Antivirus Internet
BM	Défense proactive
UPDATER	Mise à jour
SCAN_OBJECTS	Tâche "Recherche de virus"
SCAN_MY_COMPUTER	Tâche "Mon poste de travail"
SCAN_CRITICAL_AREAS	Tâche "Secteurs critiques"
SCAN_STARTUP	Tâche "Objets de démarrage"
<nom_de_la_tâche>	Tâche créée par l'utilisateur
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>
```

15.3. 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>]
[<confirmation de l'action>] [<types de fichiers>]
[<exclusions>] [<fichier de configuration>]
[<paramètres du rapport>]
```

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 15.2, page 213). Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface du logiciel.

Description des paramètres.

<objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
<files>	Liste des chemins d'accès aux fichiers et/ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques : • Mettre le nom de l'objet entre guillemets s'il contient un espace; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	objets de la mémoire vive.
/STARTUP	objets de démarrage.
/MAIL	bases de données de messagerie électronique.
/REMDRIVES	tous les disques amovibles.

/FIXDRIVES	tous les disques locaux.
/NETDRIVES	tous les disques de réseau.
/QUARANTINE	objets en quarantaine.
/ALL	Analyse complète de l'ordinateur.
/@:<filelist.lst>	chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i2.**	
/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.

Le paramètre **<confirmation de l'action>** définit les actions qui devront être confirmées par l'utilisateur lors de l'analyse. Si le paramètre n'est pas défini, l'action devra par défaut être confirmée à la fin de l'analyse.	
/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 bases de messagerie.
/e:m	Ne pas analyser les messages électroniques au format plain text.
/e:<mask>	Ne pas analyser les objets en fonction d'un masque
/e:<seconds>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <seconds>.
/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. 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:<settings_file>	Utiliser les valeurs des paramètres définies dans le fichier **<settings_file>**.
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:<report_file>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<report_file>	Consigner tous les événements dans le rapport.

Exemples:

*Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des bases de messagerie et des répertoires **My Documents, Program Files** et du fichier **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Suspendre l'analyse des objets sélectionnés, lancer une nouvelle analyse de l'ordinateur à la fin de laquelle il faudra poursuivre la recherche d'éventuels virus dans les objets sélectionnés :

```
avp.com PAUSE SCAN_OBJECTS
/password=<votre_mot_de_passe>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Analyser les objets dont la liste est reprise dans le fichier **object2scan.txt.** Utiliser le fichier de configuration **scan_setting.txt**. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements.*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

15.4. Mise à jour du logiciel

La commande de mise à jour des modules du logiciel et des signatures des menaces de Kaspersky Anti-Virus possède la syntaxe suivante :

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

Description des paramètres:

[<path/URL>]	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. 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]:<report_file>	**/R:<report_file>** : consigner uniquement les événements importants dans le rapport. **/R[A]:<report_file>** : 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:<settings_file>	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	Mettre a jour les modules du logiciel

Exemples:

Mettre à jour les signatures de menaces, consigner tous les événements dans le rapport :

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Mettre à jour les modules de Kaspersky Anti-Virus en utilisant les paramètres du fichier de configuration **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

15.5. Remise du programme à l'état antérieur à la mise à jour

Syntaxe de la commande:

```
ROLLBACK [/R[A]:<report_file>]
```

/R[A]:<report_file>	**/R:<report_file>** : uniquement consigner les événements importants dans le rapport. **/R[A]:<report_file>** : consigner tous les événements dans le rapport Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt
```

15.6. Exportation des paramètres

Syntaxe de la commande :

```
avp.com EXPORT <profile|taskid> <filename>
```

Description des paramètres:

<profile>	Composant ou tâche dont les paramètres sont exportés. Une des valeurs suivantes peut être utilisées : **RTP** = tous les composants de la protection. **FM** : Antivirus de fichiers. **EM** : antivirus de courrier électronique. **WM** : antivirus Internet. **BM** : défense proactive.
<settings_file>	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*.

Exemples:

```
avp.com EXPORT c:\ settings.cfg
```

15.7. Importation des paramètres

Syntaxe de la commande :

```
avp.com IMPORT <filename> [/password=<mot de passe>]
```

<Filename>	Chemin d'accès au fichier duquel sont importés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu.
<mot de passe>	Mot de passe de Kaspersky Anti-Virus défini via l'interface utilisateur.

Exemple :

```
avp.com IMPORT c:\ settings.dat /password=<mot_de_passe>
```

15.8. Lancement de l'application

Syntaxe de la commande :

```
avp.com
```

15.9. Arrêt de l'application

Syntaxe de la commande :

```
EXIT /password=<mot de passe>
```

<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.

15.10. 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>
```

15.11. 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 16. 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 16.1, p. 224);
- au départ de la ligne de commande (cf. point 16.2, p. 226).

16.1. 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. Déchargez le programme de la mémoire système. Pour ce faire, cliquez avec le bouton droit de la souris sur l'icône du programme dans la barre des tâches et sélectionnez le point **Quitter** dans le menu contextuel.
2. 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 le répertoire et que vous y avez accès.
3. Sélectionnez **Démarrez → Programmes → Kaspersky Anti-Virus 6.0 → 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. Fenêtre d'accueil du programme d'installation

Si vous avez réalisé toutes les tâches nécessaires à la réparation ou à la modification de la composition du programme, la fenêtre d'accueil du programme d'installation de Kaspersky Anti-Virus s'affichera. Cliquez sur **Suivant** pour poursuivre.

Etape 2. Sélection de l'opération

Vous devez définir à cette étape le type d'opération que vous souhaitez exécuter sur le logiciel: vous pouvez soit modifier la composition du logiciel, soit restaurer l'état d'origine des composants installés ou supprimer certains composants ou l'application complète. Pour exécuter l'action que vous voulez, il suffit de cliquer sur le bouton correspondant. La suite de l'Assistant dépend de l'action que vous avez choisie.

La modification de la composition de l'application est similaire à l'installation personnalisée (cf. point Etape 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* : clé de licence ou code d'activation du programme.
- *Signatures des menaces* : toutes les signatures des programmes dangereux, des virus et des autres menaces qui datent de la dernière mise à jour.
- *Objets du dossier de sauvegarde* : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure.
- *Objets de la quarantaine* : objets qui sont peut-être modifiés par des virus ou leur modification. Ces objets contiennent un code semblable au code

d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des signatures des menaces.

- *Paramètres de la protection* : valeurs des paramètres de fonctionnement de 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'écoule entre la suppression d'une version de Kaspersky Anti-Virus et l'installation d'une autre, il n'est pas conseillé d'utiliser la base iSwift de l'installation précédente. En effet, pendant cet intervalle, un programme dangereux peut s'infiltrer et ses actions pourraient ne pas être identifiées à l'aide de cette base, ce qui entraînerait l'infection de l'ordinateur.

Pour exécuter l'action sélectionnée, cliquez sur **Suivant**. La copie des fichiers nécessaires ou la suppression des composants et des données sélectionnés est lancée.

Etape 3. Fin de la réparation, de la modification ou de la suppression du logiciel

La progression de la réparation, de la modification ou de la suppression sera illustrée et vous serez averti dès que l'opération sera terminée.

En règle générale, la suppression requiert le redémarrage de l'ordinateur, indispensable pour tenir compte des modifications dans le système. La boîte de dialogue vous invitant à redémarrer l'ordinateur s'affichera. Cliquez sur **Oui** pour redémarrer immédiatement. Si vous souhaitez redémarrer l'ordinateur manuellement plus tard, cliquez sur **Non**.

16.2. Procédure de suppression de l'application via la ligne de commande

Afin de supprimer Kaspersky Anti-Virus 6.0 for Windows Servers au départ de la ligne de commande, saisissez :

```
msiexec /x <nom_du_paquetage>
```

Cette action lancera l'Assistant d'installation qui vous permettra de supprimer l'application (cf. Chapitre 16, p. 224).

Vous pouvez également utiliser une des commandes suivantes pour la suppression.

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
```

Pour supprimer l'application en mode caché avec redémarrage de l'application, saisissez :

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

CHAPITRE 17. 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 6.0 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 la clé de licence? Kaspersky Anti-Virus fonctionnera-t-il sans elle ?

Kaspersky Anti-Virus peut fonctionner sans clé de 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 clé d'évaluation qui sera valide deux semaines ou un mois. Une fois la durée de validité écoulée, la clé 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. Dans la fenêtre principale du logiciel, cliquez sur Configuration et sélectionnez la section **Protection** dans la boîte de dialogue de configuration.
5. Désélectionnez la case **Exécuter l'application au démarrage de l'ordinateur** et cliquez sur **OK**.
6. Redémarrer le système d'exploitation en mode normal.

Ensuite, contactez le service d'assistance technique via le site Internet de Kaspersky Lab (rubrique **Services → Centre de support → Résoudre un problème**). Décrivez avec le plus de précision possible le problème et les conditions dans lesquelles il survient.

Il faudra joindre à la demande le fichier du tampon complet de la mémoire du système d'exploitation Microsoft Windows. Pour ce faire, suivez ces instructions :

1. Cliquez avec le bouton droit de la souris sur l'icône **Poste de travail** et sélectionnez **Propriétés** dans le menu contextuel qui s'affiche.
2. Dans la fenêtre **Propriétés du système**, sélectionnez l'onglet **Avancé** et dans la section **Démarrage et récupération**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Démarrage et récupération**, sélectionnez **Image mémoire complète** dans la liste déroulante de la section **Ecriture des informations de débogage**.

   Par défaut le fichier de l'image est sauvegardé dans le répertoire système *memory.dmp*. Vous pouvez modifier l'emplacement de sauvegarde en modifiant le nom du répertoire dans le champ correspondant.
4. Reproduisez le problème qui entraîne le gel de Kaspersky Anti-Virus.
5. Assurez-vous que l'image mémoire complète a bien été enregistrée.

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 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 :

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 Microsoft Windows Script Host.

wsf : script Microsoft Windows.

hlp : fichier d'aide au format Win Help.

eml : message électronique de Microsoft Outlook Express.

nws : nouveau message électronique de Microsoft Outlook Express.

msg : message électronique de Microsoft Mail.

plg : message électronique

mbx : extension des messages Microsoft Office Outlook sauvegardés.

doc : document Microsoft Office Word.

dot : modèle de document Microsoft Office Word.

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro.

rtf : document au format Rich Text Format.

shs : fragment de Shell Scrap Object Handler.

dwg : base de données de dessins AutoCAD.

msi : paquet Microsoft Windows Installer.

otm : projet VBA pour Microsoft Office Outlook.

pdf : document Adobe Acrobat.

swf : objet d'un paquet Shockwave Flash.

jpg, jpeg : fichier graphique de conservation de données compressées.

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows. Les fichiers EMS ne sont pas pris en charge par Microsoft Windows 16 bit.

ico : fichier d'icône 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, etc.

*pp** : documents et fichiers de Microsoft Office PowerPoint tels que : *pps* , dia Microsoft Office PowerPoint ; *ppt* , présentation, etc.

*md** : documents et fichiers de Microsoft Office Access tels que : *mda* , groupe de travail de Microsoft Office Access ; mdb, base de données, etc.

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 la classification de la menace à exclure selon l'encyclopédie des virus est indiquée. Dans ce cas, la menace indiquée ne sera pas identifiée dans les objets. L'utilisation de ces menaces sans indication de la classification revient à désactiver la protection en temps réel.
Il est également déconseillé de sélectionner parmi les exclusions le disque virtuel créé sur la base du répertoire du système de fichiers à l'aide de la commande *subst*. Cela n'a pas de sens car pendant l'analyse, le logiciel considère ce disque virtuel comme un répertoire et, par conséquente, l'analyse.

A.3. Masques d'exclusion autorisés 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. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 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 espion. 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 (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 arpès 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 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.

Kaspersky® Internet Security 6.0 **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 (**technologie SmartStealth™**) 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 Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la "météo" des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d'informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner fonctionne directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes 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 fonctionne directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes 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® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile protège les appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le programme assure une analyse antivirus sophistiquée, notamment :

- **Analyse à la demande** de la mémoire de l'appareil nomade, des cartes mémoires, d'un dossier particulier ou d'un fichier particulier. Dès qu'un objet infecté est découvert, il est soit placé en quarantaine ou il est supprimé.
- **Protection en temps réel** : analyse automatique de tous les objets entrant ou modifiés ainsi que des fichiers lors des tentatives d'accès ;
- **Analyse programmée** des informations sauvegardées dans la mémoire de l'appareil nomade;
- **Protection contre les sms et mms** indésirables.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[3] intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et Linux, référentiels de fichiers sous Samba ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition et Microsoft ISA Server 2004 Standard Edition.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

[3] En fonction du type de livraison

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- *Postes de travail* sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et Linux, référentiels de fichiers sous Samba ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition et Microsoft ISA Server 2004 Standard Edition;
- *Ordinateurs de poche* sous Symbian OS, Microsoft Windows CE et Palm OS et téléphones intelligents tournant sous Microsoft Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

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 SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. L'application offre une série de filtres complémentaires de filtrage du courrier indésirable (selon le nom et les types MIME des fichiers en pièce jointe) ainsi qu'une série d'outils permettant de réduire la charge sur le système de messagerie et de prévenir les attaques de pirates informatiques.

Kaspersky® Anti-Virus for Proxy Server

Kaspersky® Anti-Virus for Proxy Server est un logiciel antivirus pour la protection du trafic Internet qui transite via le protocole HTTP via le serveur proxy.

L'application analyse en temps réel le trafic Internet, empêche l'intrusion de code malveillant lors de la visite de pages Internet et analyse les fichiers téléchargés.

Kaspersky® Anti-Virus for MIMESweeper for SMTP

Kaspersky® Anti-Virus for MIMESweeper for SMTP assure une protection antivirus rapide du trafic SMTP sur les serveurs utilisant la solution Clearswift MIMESweeper.

Le programme se présente sous la forme d'un module externe pour MIMESweeper for SMTP développé par Clearswift et analyse et traite en temps réel le trafic de messagerie entrant et sortant.

B.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 *Utilisation*. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus connus ou 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.