

KASPERSKY LAB

Kaspersky[®] Anti-Virus 6.0 SOS

MANUEL DE
L'UTILISATEUR

KASPERSKY® ANTI-VIRUS 6.0 SOS

Manuel de l'utilisateur

© Kaspersky Lab
<http://www.kaspersky.fr/>

Date d'édition: juillet 2007

Sommaire

CHAPITRE 1. MENACES SUR LA SECURITE INFORMATIQUE.....	8
1.1. Sources des menaces.....	8
1.2. Propagation des menaces	9
1.3. Types de menaces	11
1.4. Signes d'une infection	14
1.5. Que faire lorsque les symptômes d'une infection sont présents ?	15
1.6. Préventions des infections de votre ordinateur	16
CHAPITRE 2. KASPERSKY ANTI-VIRUS 6.0 SOS	18
2.1. Nouveautés de Kaspersky Anti-Virus 6.0 SOS.....	18
2.2. Composition de Kaspersky Anti-Virus 6.0 SOS	20
2.2.1. Tâches de recherche de virus.....	20
2.2.2. Services du programme	21
2.3. Configurations matérielle et logicielle	22
2.4. Contenu du pack logiciel	23
CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS 6.0 SOS	25
3.1. Procédure d'installation	26
3.2. Assistant de configuration initiale.....	29
3.2.1. Activation du logiciel	30
3.2.1.1. Sélection du mode d'activation du programme	30
3.2.1.2. Saisie du code d'activation	31
3.2.1.3. Réception de la clé de licence.....	31
3.2.1.4. Sélection du fichier de clé de licence	32
3.2.1.5. Fin de l'activation du logiciel	32
3.2.2. Configuration de la mise à jour.....	32
3.2.3. Programmation de la recherche de virus.....	33
3.2.4. Restriction de l'accès au logiciel.....	34
3.2.5. Fin de l'Assistant de configuration.....	34
3.3. Procédure d'installation de l'application via la ligne de commande	35
3.4. Procédure d'installation via l'éditeur d'objet de stratégie de groupe (Groupe Policy Object).....	35

3.4.1. Installation de l'application.....	36
3.4.2. Mise à jour de la version de l'application	36
3.4.3. Suppression de l'application.....	37
3.5. Mise à niveau de la version 5.0 à la version 6.0	37
CHAPITRE 4. INTERFACE DU LOGICIEL	39
4.1. Icône de la barre des tâches.....	39
4.2. Menu contextuel	40
4.3. Fenêtre principale du logiciel.....	41
4.4. Fenêtre de configuration du logiciel.....	43
CHAPITRE 5. PREMIERE UTILISATION	45
5.1. Recherche d'éventuels virus	45
5.2. Recherche d'éventuels virus dans les secteurs critiques de l'ordinateur	46
5.3. Recherche d'éventuels virus dans les fichiers, les répertoires ou les disques..	47
5.4. Mise à jour du logiciel	48
CHAPITRE 6. ADMINISTRATION DE L'APPLICATION	49
6.1. Désactivation/activation de l'application	49
6.2. Types de programmes malveillants contrôlés.....	50
6.3. Constitution de la zone de confiance	51
6.4. Lancement d'une tâche avec les privilèges d'un utilisateur	56
6.5. Programmation du lancement de tâches et de l'envoi des notifications	58
6.6. Configuration de la productivité.....	60
CHAPITRE 7. RECHERCHE DE VIRUS SUR L'ORDINATEUR.....	62
7.1. Administration des tâches de recherche de virus	63
7.2. Composition de la liste des objets à analyser	63
7.3. Création de tâches liées à la recherche de virus	65
7.4. Configuration des tâches liées à la recherche de virus	66
7.4.1. Sélection du niveau de protection.....	67
7.4.2. Définition du type d'objet analysé.....	68
7.4.3. Restauration des paramètres d'analyse par défaut.....	71
7.4.4. Sélection de l'action exécutée sur les objets	71
7.4.5. Paramètres complémentaires pour la recherche de virus	74
7.4.6. Définition de paramètres d'analyse uniques pour toutes les tâches.....	75
CHAPITRE 8. ESSAI DE KASPERSKY ANTI-VIRUS 6.0 SOS.....	77

8.1. Virus d'essai EICAR et ses modifications.....	77
8.2. Vérification des tâches de recherche de virus.....	79
CHAPITRE 9. MISE A JOUR DU LOGICIEL	81
9.1. Lancement de la mise à jour.....	82
9.2. Annulation de la dernière mise à jour	83
9.3. Création de tâches liées à la mise à jour.....	83
9.4. Configuration de la mise à jour	85
9.4.1. Sélection de la source des mises à jour	85
9.4.2. Sélection du mode et des objets de la mise à jour.....	88
9.4.3. Configuration des paramètres de connexion.....	90
9.4.4. Copie des mises à jour	92
9.4.5. Actions exécutées après la mise à jour du logiciel.....	93
CHAPITRE 10. POSSIBILITES COMPLEMENTAIRES.....	94
10.1. Quarantaine pour les objets potentiellement infectés	95
10.1.1. Manipulation des objets en quarantaine	96
10.1.2. Configuration de la quarantaine	98
10.2. Copie de sauvegarde des objets dangereux	99
10.2.1. Manipulation des copies de sauvegarde	99
10.2.2. Configuration des paramètres du dossier de sauvegarde.....	101
10.3. Utilisation des rapports	101
10.3.1. Configuration des paramètres du rapport.....	103
10.3.2. Onglet <i>Infectés</i>	104
10.3.3. Onglet <i>Evénements</i>	105
10.3.4. Onglet Statistiques.....	106
10.3.5. Onglet <i>Paramètres</i>	107
10.4. Informations générales sur le logiciel.....	108
10.5. Administration des licences.....	109
10.6. Service d'assistance technique aux utilisateurs	111
10.7. Configuration de l'interface de Kaspersky Anti-Virus 6.0 SOS.....	112
10.8. Notifications relatives aux événements de Kaspersky Anti-Virus 6.0 SOS... 114	
10.8.1.1. Types de notification et mode d'envoi des notifications	115
10.8.1.2. Configuration de l'envoi des notifications par courrier électronique. 117	
10.8.1.3. Configuration du journal des événements	118
10.8.2. Restriction de l'accès à l'application.....	119
10.9. Exportation/importation des paramètres de Kaspersky Anti-Virus 6.0 SOS. 120	

10.10. Restauration des paramètres par défaut.....	121
CHAPITRE 11. UTILISATION DU PROGRAMME AU DEPART DE LA LIGNE DE COMMANDE	123
11.1. Activation du logiciel	125
11.2. Gérer les tâches	125
11.3. Analyse antivirus des fichiers.....	127
11.4. Mise à jour du logiciel.....	131
11.5. Remise du programme à l'état antérieur à la mise à jour	133
11.6. Exportation des paramètres.....	133
11.7. Importation des paramètres	134
11.8. Lancement de l'application.....	135
11.9. Arrêt de l'application	135
11.10. Consultation de l'aide	135
11.11. Codes de retour de la ligne de commande	135
CHAPITRE 12. MODIFICATION, REPARATION OU SUPPRESSION DU LOGICIEL	137
12.1. Modification, réparation ou suppression du logiciel à l'aide d'assistant d'installation.....	137
12.2. Procédure de suppression de l'application via la ligne de commande.....	139
CHAPITRE 13. ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT.....	141
13.1. Administration de l'application.....	144
13.1.1. Lancement et arrêt de l'application	145
13.1.2. Configuration de l'application	146
13.1.3. Configuration des paramètres spécifiques	148
13.2. Administration des tâches	149
13.2.1. Lancement et arrêt des tâches.....	150
13.2.2. Création de tâches	151
13.2.2.1. Création d'une tâche locale	151
13.2.2.2. Création d'une tâche de groupe.....	153
13.2.2.3. Création d'une tâche globale.....	154
13.2.3. Configuration des tâches.....	154
13.3. Administration des stratégies	155
13.3.1. Création d'une stratégie	156
13.3.2. Consultation et modification des paramètres de la stratégie	158

CHAPITRE 14. QUESTIONS FREQUEMMENT POSEES.....	160
ANNEXE A. AIDE.....	162
A.1. Liste des objets analysés en fonction de l'extension	162
A.2. Masques autorisés pour l'exclusion de fichiers.....	164
A.3. Masques d'exclusion autorisés en fonction du verdict.....	166
A.4. Description des paramètres du fichier <i>setup.ini</i>	166
ANNEXE B. KASPERSKY LAB	168
B.1. Autres produits antivirus	169
B.2. Coordonnées.....	181
ANNEXE C. CONTRAT DE LICENCE	182

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, financiers et moraux conséquents.

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

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

1.1. Sources des menaces

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

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

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

1.2. Propagation des menaces

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

Internet

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

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

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

de la base de registres système, le vol de données personnelles et l'installation de programmes malveillants.

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

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

Intranet

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

Courrier électronique

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

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, 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 6.0 SOS :

Vers

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

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

Virus

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

Chevaux de Troie

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

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

Adwares

Ce code est intégré, à l'insu de l'utilisateur, dans un logiciel afin d'afficher des messages publicitaires. En règle générale, les adwares sont intégrés à des logiciels distribués gratuitement. La publicité s'affiche dans l'espace de travail. Bien souvent, ces programmes recueillent également des données personnelles sur l'utilisateur qu'ils transmettent à leur auteur, ils modifient divers paramètres du navigateur (page d'accueil et recherche, niveau de sécurité, etc.) et ils créent un trafic sur lequel l'utilisateur n'a aucun contrôle. Tout cela peut entraîner une violation de la politique de sécurité, voire des pertes financières.

Logiciels espion

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

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

Riskwares

Il s'agit d'un programme qui n'a aucune fonction malicieuse mais qui pourrait être exploité par un individu mal intentionné en guise de soutien à

un programme malicieux en raison des failles ou des erreurs qu'il contient. Dans certains cas, la présence de tels programmes sur votre ordinateur expose vos données à un certain risque. Cette catégorie de programme contient par exemple certains utilitaires d'administration à distance, des programmes de permutation automatique de la disposition du clavier, des clients IRC, des serveurs FTP, des utilitaires d'arrêt de processus ou de dissimulation de leur fonctionnement.

Une autre catégorie de programmes présentant un risque potentiel, proche des adwares, spywares et riskwares, contient les programmes qui s'intègrent au navigateur et qui réorientent le trafic. Il vous est certainement déjà arrivé de cliquer de vouloir accéder à un site particulier et de vous retrouver 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 réseaux ou du système attaqué.

Kaspersky Anti-Virus 6.0 SOS identifie et bloque ces différentes menaces en exploitant la méthode réactive qui 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.

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 conseillé de réaliser une analyse complète de l'ordinateur (cf. point 5.1, p. 45).

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

Si vous remarquez que votre ordinateur a un comportement suspect :

1. Ne paniquez pas ! La règle d'or dans ce type de situation est de garder son calme afin d'éviter de supprimer des données importantes.
2. Déconnectez l'ordinateur d'Internet et, le cas échéant, du réseau local.
3. Si le symptôme observé vous empêche de démarrer l'ordinateur depuis le disque dur (un message d'erreur apparaît lorsque vous allumez l'ordinateur), essayez de démarrer en mode Sans échec ou au départ du disque de secours de Microsoft Windows que vous avez créé au moment de l'installation du système d'exploitation.
4. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD/DVD, une carte Flash, etc.
5. Installez Kaspersky Anti-Virus, si cela n'a pas encore été fait.
6. Actualisez les signatures des menaces et les modules de l'application (cf. point 5.4, p. 48) du programme. Dans la mesure du possible, réalisez cette opération depuis l'ordinateur sain d'un ami, d'un cybercafé ou du travail. Il est en effet préférable d'utiliser un autre ordinateur car si le vôtre est bel et bien infecté, sa connexion à Internet permettra plus que probablement au virus d'envoyer des informations importantes à une personne mal intentionnée ou de se propager en envoyant une copie à tous les contacts de votre carnet d'adresses. C'est pour cette même raison qu'il est toujours conseillé de déconnecter votre ordinateur d'Internet si vous soupçonnez une infection. Il est possible également d'obtenir les mises à jour sur une disquette ou sur un disque en s'adressant à Kaspersky Lab ou à l'un de ses distributeurs. Dans ce cas, la mise à jour s'effectue localement.

7. Définissez le niveau de sécurité défini par les experts de Kaspersky Lab.
8. Lancez l'analyse complète de l'ordinateur (cf. point 5.1, p. 45).

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 de réduire sensiblement le risque d'attaques de virus. Toutefois, il ne faut pas oublier que Kaspersky Anti-Virus 6.0 SOS ne garantit pas la protection en temps réel de l'ordinateur.

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 5.4, p. 46) 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).
- 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 5.3, p. 47) (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.*

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 utilisez Internet ou installez un autre programme. Certains d'entre eux sont probablement des riskwares.*

CHAPITRE 2. KASPERSKY ANTI-VIRUS 6.0 SOS

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

Ce qui différencie Kaspersky Anti-Virus 6.0 SOS des produits existants, c'est le fait que l'application est un moyen complémentaire de protection contre les virus qui offre une fonction d'analyse à la demande. Kaspersky Anti-Virus 6.0 SOS peut fonctionner sans risque de conflits avec d'autres logiciels antivirus.

Kaspersky Anti-Virus 6.0 SOS n'offre pas de protection en temps réel contre les virus !

2.1. Nouveautés de Kaspersky Anti-Virus 6.0 SOS

Ce chapitre aborde en détails les nouveautés de Kaspersky Anti-Virus 6.0 SOS.

Nouveautés au niveau de l'analyse des virus

- Modification de la technologie d'analyse des fichiers sur l'ordinateur de l'utilisateur : il est désormais possible de réduire la charge sur le processeur central et les sous-systèmes disque et d'augmenter la vitesse de l'analyse des fichiers. Ce résultat est obtenu grâce au recours à la technologie iChecker™. Ainsi, les fichiers ne sont pas analysés inutilement.
- 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.
- Elargissement de la fonction de notification de l'utilisateur 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, enregistrement dans le journal des événements.

- Possibilité d'administrer centralement à distance le système de protection grâce à l'interface complémentaire d'administration sous Kaspersky Administration Kit.

Nouveautés au niveau de l'interface

- La nouvelle interface de Kaspersky Anti-Virus 6.0 SOS offre un accès simple et convivial à n'importe quelle fonction de l'application. Vous pouvez également modifier l'apparence du logiciel en utilisant vos propres éléments graphiques et la palette de couleurs.
- Vous recevez toutes les informations relatives au fonctionnement de l'application : Kaspersky Anti-Virus 6.0 SOS émet des messages sur l'état de la recherche des virus et des mises à jour et 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

- La procédure de mise à jour a été améliorée : Kaspersky Anti-Virus 6.0 SOS vérifie automatiquement si les fichiers de mise à jour sont présents sur la source de la mise à jour. Si le logiciel découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur.
- 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 s'opère depuis 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 remettre les mises à jour à l'état initial, ce qui permet de revenir à la version antérieure des signatures de menace en cas de corruption des fichiers ou d'erreur de copie des mises à jour.
- Possibilité d'utiliser le service de copie des mises à jour dans un répertoire local en vue de les rendre accessibles aux autres ordinateurs du réseau. Le trafic Internet est ainsi réduit.

2.2. Composition de Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS comprend :

- Des tâches de recherche de virus (cf. point 2.2.1 , p. 20) 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 2.2.2, p. 21) qui garantissent la mise à jour des signatures des menaces et le soutien informatif dans le cadre de l'utilisation du logiciel et qui permettent d'en élargir les fonctions.

2.2.1. Tâches de recherche de virus

Il est particulièrement important de procéder régulièrement à une analyse antivirus de l'ordinateur. Pour ce faire, Kaspersky Anti-Virus 6.0 SOS contient les tâches suivantes axées sur la recherche des virus :

Secteurs critiques

Recherche d'éventuels virus dans tous les secteurs critiques de l'ordinateur. Il s'agit de la mémoire système, des objets utilisés au démarrage du système, des secteurs d'amorçage des disques et des répertoires système *Microsoft Windows* et *system32*. L'objectif poursuivi est d'identifier rapidement les virus actifs dans le système sans devoir lancer une analyse complète de l'ordinateur.

Mon poste de travail

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

Objets de démarrage

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

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

2.2.2. Services du programme

Kaspersky Anti-Virus 6.0 SOS 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 repousser n'importe quelle attaque de pirate, à neutraliser tout virus ou programme malveillant, à intercepter le courrier indésirable, il faut veiller à ce que Kaspersky Anti-Virus 6.0 SOS soit toujours à jour. Le composant *Mise à jour* a été conçu à cette fin. Il assure la mise à jour des signatures des menaces et des modules de Kaspersky Anti-Virus 6.0 SOS utilisés.

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

Rapport

Un rapport est généré pendant l'utilisation pour 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 quelle tâche. 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 6.0 SOS déplace 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.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS par téléphone.

2.3. Configurations matérielle et logicielle

Pour garantir le fonctionnement normal de Kaspersky Anti-Virus 6.0 SOS, 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 SOS 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(SE), Microsoft Windows ME, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Processeur Intel Pentium 300 Mhz ou supérieur.
- 64 Mo de mémoire vive disponible.

Microsoft Windows 2000 Professional (Service Pack 4 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 boîte contient :

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

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

Si vous achetez Kaspersky Anti-Virus en ligne, vous copiez le logiciel depuis le site de Kaspersky Lab (rubrique **Téléchargement** → **Télécharger nos produit**). Les manuels sont disponibles dans la rubrique **Téléchargement** → **Documentation**.

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

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

Lisez attentivement le contrat de licence !

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

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

CHAPITRE 3. INSTALLATION DE KASPERSKY ANTI-VIRUS 6.0 SOS

Kaspersky 6.0 SOS peut être installé avec d'autres logiciels antivirus d'éditeurs tiers ou de Kaspersky Lab. Aucun conflit ne surviendra entre les différents logiciels antivirus. Les seules exceptions sont :

- Kaspersky Anti-Virus 6.0 et 7.0 ;
- Kaspersky Internet Security 6.0 et 7.0 ;
- Kaspersky Anti-Virus 6.0 for Windows Workstations;
- Kaspersky Anti-Virus 6.0 for File Servers.

Kaspersky Anti-Virus 6.0 SOS n'assure pas la protection en temps réel de votre ordinateur et n'est qu'un logiciel antivirus complémentaire !

Kaspersky Anti-Virus 6.0 SOS peut être installé sur un ordinateur de différentes manières :

- Installation locale : installation de l'application sur un ordinateur distinct. Cette installation requiert un accès direct à l'ordinateur en question. L'installation locale peut être réalisée de deux manières :
 - interactive à l'aide de l'assistant d'installation de l'application (cf. point 3.1, p. 26) ; ce mode requiert l'intervention de l'utilisateur au cours de l'installation ;
 - non interactif ; le lancement de l'installation de l'application s'opère via la ligne de commande et applique les paramètres par défaut ; l'intervention de l'utilisateur dans le processus d'installation n'est pas requise (cf. point 3.3, p. 35).
- Installation à distance : installation de l'application sur des ordinateurs du réseau réalisée à distance depuis le poste de travail de l'administrateur à l'aide de :
 - La suite logicielle Kaspersky Administration Kit (cf. « Manuel de déploiement de Kaspersky Administration Kit ») ;
 - Les stratégies de domaines de groupes de Microsoft Windows Server 2000/2003 (cf. point 3.4, p. 35).

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

3.1. Procédure d'installation

Afin d'installer Kaspersky Anti-Virus 6.0 SOS sur votre ordinateur, vous devez exécuter le fichier d'installation (fichier msi) 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-Virus6.0 SOS

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 6.0 SOS. 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 6.0 SOS.

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 6.0 SOS.

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

Etape 3. Examen du contrat de licence

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

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

Etape 4. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le répertoire dans lequel vous souhaitez installer Kaspersky Anti-Virus 6.0 SOS. Il s'agit par défaut de :

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

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

Si vous saisissez le 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. Recherche des programmes pouvant nuire à la bonne installation

Au cours de cette étape, tous les logiciels antivirus chargés sur l'ordinateur sont analysés.

Si un autre logiciel antivirus est découvert, Kaspersky Anti-Virus 6.0 SOS poursuit l'installation. Dans le cas contraire, un message d'avertissement s'affiche pour indiquer que l'application ne garantit pas la protection antivirus complète de l'ordinateur.

Une fois que vous aurez quitté le programme, cliquez sur **Suivant** afin de poursuivre l'installation.

Etape 6. Recherche d'autres logiciels antivirus éventuellement installés

Cette étape constitue la préparation finale pour l'installation du logiciel sur votre ordinateur. Vous pouvez décider d'utiliser les paramètres des signatures des menaces si ceux-ci ont été enregistrés sur l'ordinateur lors de la suppression de la version antérieure de Kaspersky Anti-Virus SOS (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 SOS 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 installez. 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 l'application définis dans la version antérieure que vous aviez sauvegardés, cochez la case **Paramètres de l'application**.

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

Etape 7. Choix du type d'installation

Vous devez décider à ce stade du type d'installation. Trois 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 8

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

Etape 8. 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, le composant de recherche des virus ainsi que le connecteur à l'agent d'administration pour l'administration à distance via Kaspersky Administration Kit seront installés.

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

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

A l'étape suivante, cliquez sur **Installer**.

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 6.0 SOS sur votre ordinateur.

Pour lancer l'Assistant de configuration initiale, cliquez sur **Suivant** (cf. point 3.2, p. 29).

Si le redémarrage de l'ordinateur s'impose pour finaliser l'installation, le message correspondant s'affichera.

3.2. Assistant de configuration initiale

L'Assistant de configuration de Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS. (cf. point 10.10, p. 121)

3.2.1. Activation du logiciel

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

La procédure d'activation du logiciel consiste à installer la clé que Kaspersky Anti-Virus 6.0 SOS utilisera pour confirmer l'existence de droits d'utilisation de l'application et leur durée de validité.

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

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

3.2.1.1. Sélection du mode d'activation du programme

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

- ④ **Activer à l'aide du code d'activation.** Sélectionnez cette option si vous avez acheté une version commerciale de l'application et que vous avez reçu le code d'activation. Vous recevrez, sur la base de ce code, la clé de licence qui vous donnera accès à l'ensemble des fonctions de l'application pendant toute la durée de validité de la licence.
- ④ **Activer la version d'évaluation.** Sélectionnez cette option si vous souhaitez installer une version d'évaluation de l'application avant de décider d'acheter la version commerciale. Vous recevrez une clé de licence gratuite dont la durée de validité sera limitée par la licence associée à la version d'évaluation de l'application:
- ④ **Utiliser votre clé de licence acquise antérieurement non expirée.** Activez l'application à l'aide du fichier de clé de licence pour Kaspersky Anti-Virus 6.0 SOS obtenu précédemment.
- ④ **Activer le logiciel plus tard.** Sélectionnez cette option si vous êtes en attente de votre licence commerciale. L'activation du logiciel sera reportée à plus tard. Ce logiciel Kaspersky Anti-Virus 6.0 SOS 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 9.4.3, p. 90) dans la fenêtre qui s'ouvre à l'aide du bouton **Paramètres LAN**. Pour obtenir de plus amples informations sur la configuration des paramètres de réseau, contactez votre administrateur système ou votre fournisseur d'accès Internet.

Si vous ne disposez pas d'une connexion Internet au moment de réaliser l'installation, vous pouvez réaliser l'activation plus tard (cf. point 10.5, p. 109) au départ de l'interface de l'application ou en vous connectant à Internet depuis un autre ordinateur afin d'obtenir la clé de licence associée au code d'activation après vous être enregistré sur le site Web du service d'assistance technique de Kaspersky Lab.

3.2.1.2. Saisie du code d'activation

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

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

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

3.2.1.3. Réception de la clé de licence

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

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

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

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

3.2.1.4. Sélection du fichier de clé de licence

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




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

3.2.1.5. 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.

3.2.2. Configuration de la mise à jour

La qualité de la recherche des virus sur 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 6.0 SOS vérifie selon la fréquence définie la présence de fichiers de mise à jour sur la source de la mise à jour. L'intervalle peut être réduit en cas d'épidémie de virus ou augmenté lorsque la situation est calme. Si Kaspersky Anti-Virus identifie de nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur.
-  **Toutes les 2 heures** (l'intervalle peut varier en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.
-  **Manuel.** Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules du logiciel qui font partie de l'installation peuvent être dépassés au moment de l'installation. Pour cette raison, nous vous conseillons d'obtenir les mises à jour les plus récentes du logiciel. Il suffit simplement de cliquer sur **Mettre à jour**. Dans ce cas, Kaspersky Anti-Virus 6.0 SOS recevra toutes les mises à jour depuis Internet et les installera sur l'ordinateur.

Si vous souhaitez passer à la configuration des mises à jour (sélectionner les paramètres de réseau, sélectionner la ressource au départ de laquelle la mise à jour sera réalisée, configurer le lancement de la mise à jour au nom d'un compte particulier et activer le service de copie des mises à jour dans un répertoire local), cliquez sur **Configuration**.

3.2.3. 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 6.0 SOS, trois tâches d'analyse sont créées par défaut. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de lancement de la tâche d'analyse :

Analyse des objets de démarrage

Par défaut, l'analyse des objets de démarrage s'opère automatiquement lors du lancement de Kaspersky Anti-Virus 6.0 SOS. Vous pouvez modifier les paramètres de la programmation dans la fenêtre qui s'ouvre à l'aide du bouton **Modifier**.

Analyse des secteurs critiques

Pour lancer automatiquement l'analyse des secteurs critique de l'ordinateur (mémoire système, objets de démarrage, secteurs d'amorçage, répertoires système Microsoft Windows), 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.

3.2.4. Restriction de l'accès au logiciel

Dans la mesure où votre ordinateur peut être utilisé par différentes personnes dont les connaissances en informatique varient et vu que certains programmes malveillants peuvent arrêter l'application, vous avez la possibilité de définir un mot de passe pour limiter l'accès à Kaspersky Anti-Virus 6.0 SOS. Le mot de passe protège le logiciel contre les tentatives d'arrêt non autorisées de l'application ou de modification de ses paramètres.

Afin d'activer cette option, cochez la case **Activer la protection par mot de passe** et saisissez les informations dans les champs **Nouveau mot de passe** et **Confirmation du mot de passe**. Si vous utilisez déjà un mot de passe et que vous souhaitez le modifier, remplissez également le champ **Ancien mot de passe**.

Indiquez ensuite les tâches qui seront concernées :

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

3.2.5. Fin de l'Assistant de configuration

Dans la dernière fenêtre de l'Assistant, cochez le cas échéant la case **Lancer l'application** et cliquez sur le bouton **Terminer**.

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 SOS, 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. 26).

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

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

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

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

L'installation de Kaspersky Anti-Virus en mode non interactif prend en charge la lecture du fichier *setup.ini* contenant les paramètres généraux d'installation de l'application (cf. point A.4, p. 166), du fichier de configuration *install.cfg* (cf. point 11.7, p. 134) ainsi que du fichier de clé de licence. N'oubliez pas que ces fichiers doivent se trouver dans le même répertoire que la distribution de Kaspersky Anti-Virus.

3.4. Procédure d'installation via l'éditeur d'objet de stratégie de groupe (Groupe Policy Object)

Cette possibilité est offerte par les ordinateurs tournant sous Microsoft Windows 2000 et suivant.

L'**Editeur d'objets de stratégie de groupe** vous permet d'installer, d'actualiser et de supprimer Kaspersky Anti-Virus sur les postes de travail de l'entreprise faisant partie du domaine sans devoir utiliser Kaspersky Administration Kit.

3.4.1. Installation de l'application

Pour installer Kaspersky Anti-Virus :

1. Créez un répertoire de réseau partagé sur l'ordinateur faisant office de contrôleur de domaine et placez-y la distribution de Kaspersky Anti-Virus au format *.msi*.

Vous pouvez également ajouter à ce répertoire le fichier *setup.ini* contenant la liste des paramètres d'installation de Kaspersky Anti-Virus (pour obtenir une description complète des paramètres de ce fichier, consultez le point A.4 à la page 166), le fichier de configuration *install.cfg* (cf. point 11.7, p. 134) ainsi que le fichier de clé.

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

Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès au répertoire de réseau partagés contenant la distribution de Kaspersky Anti-Virus (cf. point 1). Dans la boîte de dialogue **Déploiement du programme**, sélectionnez le paramètre **Désigné** puis, cliquez sur **OK**.

La stratégie de groupe sera appliquée à chaque poste de travail après le prochain enregistrement des ordinateurs dans le domaine. Kaspersky Anti-Virus sera ainsi installé sur tous les ordinateurs.

3.4.2. Mise à jour de la version de l'application

Pour actualiser la version de Kaspersky Anti-Virus :

1. Placez la distribution contenant la mise à jour de Kaspersky Anti-Virus au format *msi* dans le répertoire de réseau partagé.

2. Ouvrez l'**Editeur d'objets de stratégie de groupe** et créez un nouveau paquet selon la méthode décrite ci-dessus.
3. Sélectionnez le nouveau paquet dans la liste et utilisez la commande **Propriétés** du menu contextuel. Dans la fenêtre des propriétés du paquet, ouvrez l'onglet **Mises à jour** et indiquez le paquet contenant la distribution de la version précédente de Kaspersky Anti-Virus. Pour installer une version actualisée de Kaspersky Anti-Virus en préservant les paramètres de sécurité, sélectionnez l'option permettant de réaliser l'installation sur le paquet existant.

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

N'oubliez pas que les ordinateurs tournant sous Microsoft Windows 2000 Professional ne prennent pas en charge la mise à jour de Kaspersky Anti-Virus via l'Editeur d'objets de stratégie de groupe.

3.4.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

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

Dans la liste des paquets, sélectionnez le paquet de Kaspersky Anti-Virus, ouvrez le menu contextuel et choisissez la commande **Toutes les tâches/ Supprimer**.

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

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

Si vous avez installé Kaspersky Anti-Virus 5.0 SOS, vous pouvez réaliser la mise à niveau à la version 6.0 SOS.

Une fois que vous aurez lancé le programme d'installation de Kaspersky Anti-Virus 6.0 SOS 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 SOS au départ d'un répertoire de réseau dont l'accès est protégé par un mot de passe, la version 5.0 sera supprimée 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 6.0 SOS 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. 39);
- Le menu contextuel (cf. point 4.2, p. 40);
- La fenêtre principale (cf. point 4.3, p. 41);
- Fenêtre de configuration du logiciel (cf. point 4.4, p. 43).




En plus de l'interface principale du logiciel, il existe des plug-in intégrés dans Microsoft Windows Explorer (cf. point 7.2, p. 63). Celui-ci élargit les possibilités de Microsoft Windows Explorer en lui permettant d'administrer et de configurer Kaspersky Anti-Virus 6.0 SOS directement depuis son interface.

4.1. Icône de la barre des tâches

L'icône de Kaspersky Anti-Virus 6.0 SOS apparaît dans la barre des tâches directement après son installation.

Cette icône est un indicateur du fonctionnement de Kaspersky Anti-Virus 6.0 SOS. Elle illustre diverses tâches fondamentales exécutées par l'application. Si l'icône  apparaît dans la barre des tâches, cela signifie que Kaspersky Anti-Virus 6.0 SOS est activé

L'icône de Kaspersky Anti-Virus 6.0 SOS change en fonction de l'opération exécutée :

	L'analyse d'un fichier est en cours.
	La mise à jour des signatures des menaces et des modules logiciels de Kaspersky Anti-Virus 6.0 SOS est en cours.
	Une erreur s'est produite dans Kaspersky Anti-Virus 6.0 SOS.

L'icône donne également accès aux éléments principaux de l'interface du logiciel : le menu contextuel (cf. point 4.2, p. 40) et la fenêtre principale (cf. point 4.3, p. 41);

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 6.0 SOS à l'onglet **Recherche de virus** (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.

Le menu de Kaspersky Anti-Virus 6.0 SOS contient les éléments suivants :

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

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.



Illustration 1. Menu contextuel

Mise à jour : lance la mise à jour des modules de l'application et des signatures de menaces de Kaspersky Anti-Virus 6.0 SOS et les installe sur l'ordinateur.

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

Configuration : permet d'examiner et de configurer les paramètres de fonctionnement de Kaspersky Anti-Virus 6.0 SOS.

Kaspersky Anti-Virus: ouvre la fenêtre principale de l'application (cf. point 4.3, p. 41).

Quitter : quitte Kaspersky Anti-Virus 6.0 SOS (si ce point du menu est sélectionné, l'application sera déchargée de la mémoire vive de l'ordinateur).

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

4.3. Fenêtre principale du logiciel

La fenêtre principale (cf. ill. 2) de Kaspersky Anti-Virus 6.0 SOS est constituée de deux panneaux :

- Le panneau de gauche est réservé à la *navigation*. Il permet de passer rapidement et simplement à l'exécution de la recherche de virus, de mise à jour et d'accéder aux services du logiciel;
- Le panneau de droite est à caractère *informatif* : il 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.

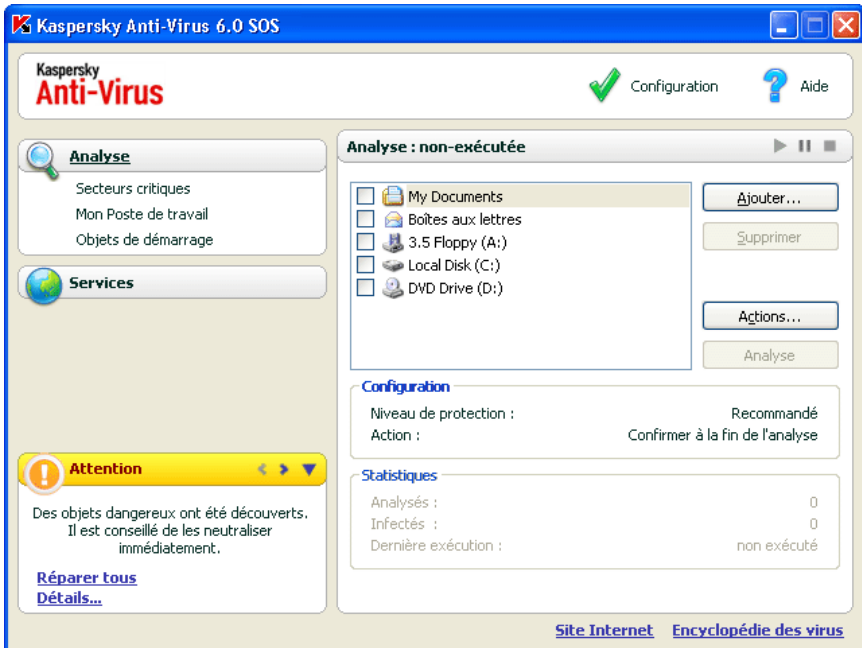
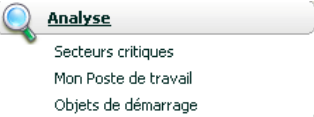

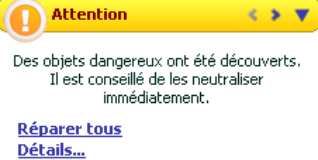


Illustration 2. Fenêtre principale de Kaspersky Anti-Virus 6.0 SOS

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

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

Section du panneau de navigation de la fenêtre principale	Fonction
<p>La section Analyser est prévue pour la recherche d'objets malveillants.</p> 	<p>Cette section contient la liste des objets que vous pouvez soumettre individuellement à l'analyse antivirus.</p> <p>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.</p>

Section du panneau de navigation de la fenêtre principale	Fonction
<p>La section Services contient les fonctions complémentaires de Kaspersky Anti-Virus 6.0 SOS.</p> 	<p>Vous pouvez passer à la mise à jour du logiciel, à la configuration de la copie des mises à jour pour les ordinateurs du réseau, à la consultation des rapports sur la recherche de virus, à la manipulation des objets en quarantaine ou des copies de sauvegarde ou à la fenêtre d'administration des clés de licence.</p>
<p>La section Commentaires et conseils vous accompagne tout au long de l'utilisation de l'application.</p> 	<p>Cette section vous offrira toujours des conseils pour renforcer la protection de l'ordinateur. C'est ici que vous trouverez également les commentaires sur le fonctionnement actuel de l'application et sur ces paramètres. Grâce aux liens repris dans cette section, vous pouvez accéder directement à l'exécution de l'action recommandée dans un cas concret ou en savoir plus sur les informations.</p>

Chaque élément du panneau de navigation est doté d'un menu contextuel spécial. Ainsi, pour 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 et de la mise à jour prévoit un point supplémentaire qui vous permet de personnaliser la tâche sélectionnée.

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

4.4. Fenêtre de configuration du logiciel

La fenêtre de configuration de Kaspersky Anti-Virus 6.0 SOS peut être ouverte depuis la fenêtre principale (cf. point 4.3, p. 41). 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 des tâches liées à la recherche de virus, à la mise à jour ainsi qu'à la configuration des services du logiciel;
- La partie droite reprend une énumération des paramètres 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 de 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.

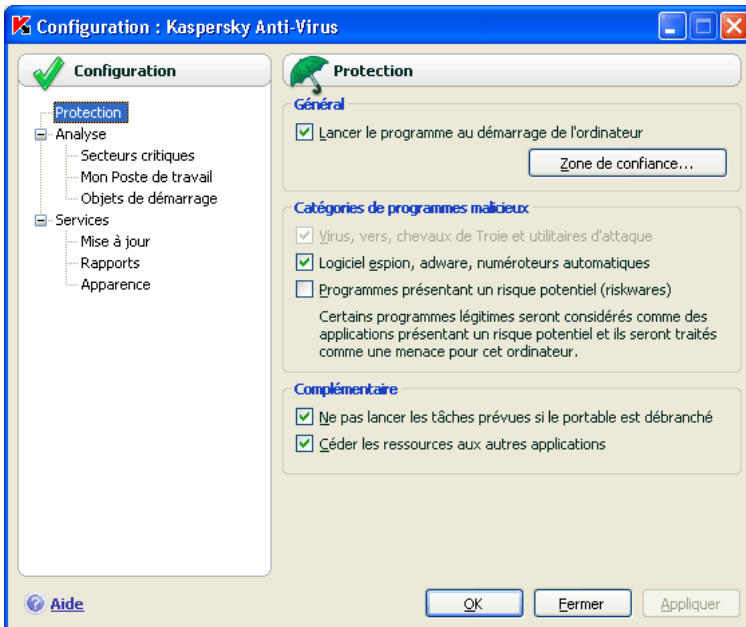


Illustration 3. Fenêtre de configuration de Kaspersky Anti-Virus 6.0 SOS

CHAPITRE 5. PREMIERE UTILISATION

Une des principales tâches des experts de Kaspersky Lab dans le cadre du développement de Kaspersky Anti-Virus 6.0 SOS 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. 29). Cet Assistant démarre à la fin de l'installation du logiciel. En suivant les indications de l'Assistant, vous pourrez activer le programme, configurer la mise à jour et le lancement de la recherche de virus, limiter l'accès au programme grâce à un mot de passe etc.

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

- 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 5.4, p. 48).
- Analyser l'ordinateur (cf. point 5.1, p. 45).

5.1. Recherche d'éventuels virus

Dès que l'installation est terminée, un message spécial vous signale que l'analyse du serveur n'a pas encore été réalisée et qu'il est conseillé de la lancer immédiatement.

Kaspersky Anti-Virus 6.0 SOS possède une tâche de recherche de virus sur l'ordinateur. Elle se trouve dans la section **Analyser** de la fenêtre principale du logiciel.

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

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

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

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

5.2. 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 peuvent être 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 **Analyser** de la fenêtre principale du logiciel.

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

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

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

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

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

Il arrive parfois que vous deviez absolument rechercher la présence d'éventuels virus non pas dans tout l'ordinateur mais uniquement dans un objet particulier comme l'un des disques durs où sont enregistrés les logiciels et les jeux, une base de données de messagerie ramenée de l'ordinateur de votre bureau, une archive envoyée par courrier électronique, etc. Vous pouvez sélectionner l'objet à analyser à l'aide des méthodes traditionnelles du système d'exploitation Microsoft Windows (via l'**Assistant** ou sur le **Bureau**, etc.)

Pour lancer l'analyse d'un objet :

Placez la souris sur l'objet, ouvrez le menu contextuel de Microsoft Windows d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 4).

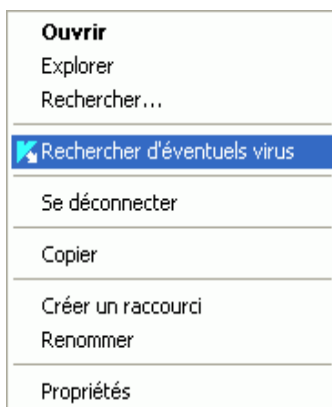


Illustration 4. Recherche d'éventuels virus dans un objet sélectionné à l'aide des outils Windows

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.

5.4. Mise à jour du logiciel

Kaspersky Lab met à jour les signatures des menaces et les modules de Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS nécessite une connexion Internet

Kaspersky Anti-Virus 6.0 SOS vérifie automatiquement par défaut la présence des mises à jour sur les serveurs de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Anti-Virus 6.0 SOS les télécharge et les installe en arrière plan.

Pour procéder à la mise à jour manuelle de Kaspersky Anti-Virus 6.0 SOS :

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

Cette action entraînera la mise à jour de Kaspersky Anti-Virus 6.0 SOS. Tous les détails du processus sont illustrés dans une fenêtre spéciale.

CHAPITRE 6. ADMINISTRATION DE L'APPLICATION

Kaspersky Anti-Virus 6.0 SOS peut être soumis à une administration complexe :

- Désactivation/activation de l'application (cf. point 6.1, p. 49).
- Sélection des logiciels contrôlés contre lesquels Kaspersky Anti-Virus 6.0 SOS vous protégera (cf. point 6.2, p. 50).
- Constitution de la liste des exclusions pour la protection (cf. point 6.3, p. 51).
- Création de tâches personnalisées de recherche de virus et de mise à jour (cf. point 6.4, p. 56).
- Configuration du lancement des tâches à l'heure qui vous convient (cf. point 6.5, p. 58).
- Configuration des paramètres de performance (cf. point 6.6, p. 60) de la protection de l'ordinateur.

6.1. Désactivation/activation de l'application

Par défaut, Kaspersky Anti-Virus 6.0 SOS est lancé au démarrage du système.

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Anti-Virus 6.0 SOS, sélectionnez le point **Quitter** dans le menu contextuel (cf. point 4.2, p. 40) du programme. Celui-ci sera déchargé de la mémoire vive.

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

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

6.2. Types de programmes malveillants contrôlés

Kaspersky Anti-Virus 6.0 SOS recherche divers types de programmes malveillants. . Quels que soient les paramètres définis, l'application protégera toujours l'ordinateur contre les types de programmes malveillants les plus dangereux tels que les virus, les chevaux de Troie et les utilitaires d'attaque. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une plus protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

Afin de sélectionner les types de programmes malveillants contre lesquels Kaspersky Anti-Virus 6.0 SOS vous protégera, passez à la section **Protection**, de la fenêtre de configuration du logiciel (cf. point 4.4, p. 43).

Les types de menaces (cf. point 1.1, p. 8) 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 6.0 SOS contrôle toujours les programmes malveillants de cette catégorie.
- Logiciel espion, Adwares, numéroteurs automatiques.** Ce groupe recouvre tous les riskwares qui peuvent gêner l'utilisateur ou lui causer 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 lors de la recherche d'éventuels virus sur votre ordinateur.

Lorsque tous les groupes sont sélectionnés, Kaspersky Anti-Virus 6.0 SOS garantit l'analyse antivirus maximale de votre ordinateur. Si le deuxième et le troisième groupe sont désélectionnés, le logiciel recherche 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 vous conseillent de ne pas désactiver le contrôle des deuxième et troisième groupes. Lors Kaspersky Anti-Virus 6.0 SOS 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. 51).

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 6.0 SOS. En d'autres termes, il s'agit des éléments exclus de l'analyse 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.

Il est possible d'exclure des fichiers d'un certain format, des fichiers selon un masque, certains secteurs (par exemple, un répertoire ou un programme), des processus ou des objets en fonction d'un verdict (état attribué à l'objet par 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 l'application et passez à la section **Protection**.
2. Cliquez sur **Zone de confiance** dans le bloc **Général**.
3. Dans la boîte de dialogue (cf. ill. 5) qui apparaît, configurez les règles d'exclusion pour les objets.

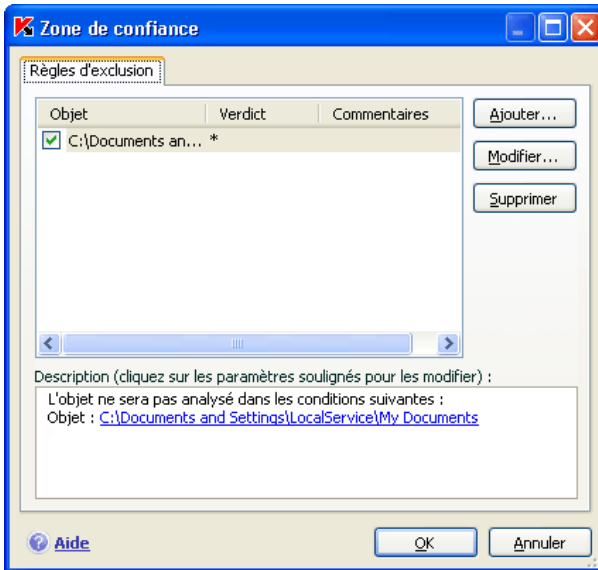


Illustration 5. Constitution de la zone de confiance

La règle d'exclusion est un ensemble de paramètres qui détermine si un objet quelconque sera analysé ou non par Kaspersky Anti-Virus 6.0 SOS.

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

La classification est l'état que Kaspersky Anti-Virus 6.0 SOS 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 ils 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 Internet Security, consultez l'encyclopédie des virus à l'adresse www.viruslist.com/fr). De tels programmes peuvent être bloqués après l'analyse. Dans la mesure où certains d'entre eux sont très populaires auprès des utilisateurs, il est possible de les

exclure de l'analyse. Pour ce faire, il faut ajouter le nom ou le masque de la menace en fonction de la classification de l'Encyclopédie des virus à la zone de confiance. Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'un système d'accès à distance qui permet de travailler sur un ordinateur distant. Kaspersky Internet Security 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 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. 6), 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.
 - Verdict** : exclusion de l'analyse d'un objet en fonction d'un état attribué selon le classement de l'encyclopédie des virus.

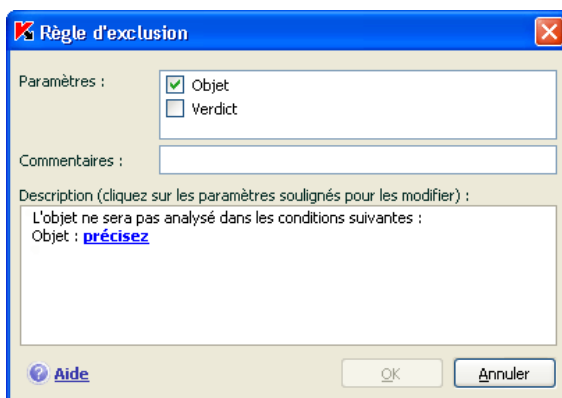


Illustration 6. Création d'une règle d'exclusion

Si vous cochez simultanément les deux cases, vous créez 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 **Verdict**, 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 **Verdict**, 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. 164). Afin que l'objet indiqué (fichier, masque de fichiers, répertoire) soit ignoré partout pendant l'analyse, cochez la case **Sous-répertoires compris**. Si vous avez défini le fichier **C:\Program Files\winword.exe** comme une exclusion et que vous avez coché la case d'analyse des sous-répertoire, le fichier **winword.exe** situé dans n'importe quel sous-répertoire de **C:\Program Files** sera ignoré.
 - Pour la **Verdict** indiquez le nom complet de l'exclusion telle qu'elle est reprise dans l'encyclopédie des virus ou selon un masque (cf. point A.3, p. 166).

Pour certaines classifications, il est possible de définir dans le champ **Paramètres complémentaires** des conditions supplémentaires pour l'application de la règle.

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

1. Cliquez sur Ajouter à la liste de confiance dans la fenêtre de notification (cf. ill. 7).
2. Dans la boîte de dialogue qui s'affiche, vérifiez si tous les paramètres vous conviennent. Les champs reprenant le nom de l'objet et le type de menace attribué sont remplis automatiquement sur la base des renseignements qui figurent dans la notification. Afin de créer une règle, cliquez sur **OK**.

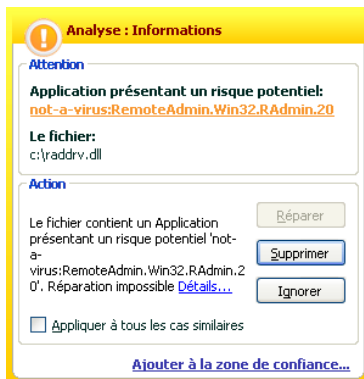


Illustration 7. Notification sur la découverte d'un objet dangereux

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

1. Sélectionnez dans le rapport l'objet que vous souhaitez ajouter aux exclusions.
2. Ouvrez le menu contextuel et sélectionnez le point **Ajouter à la zone de confiance** (cf. ill. 8).

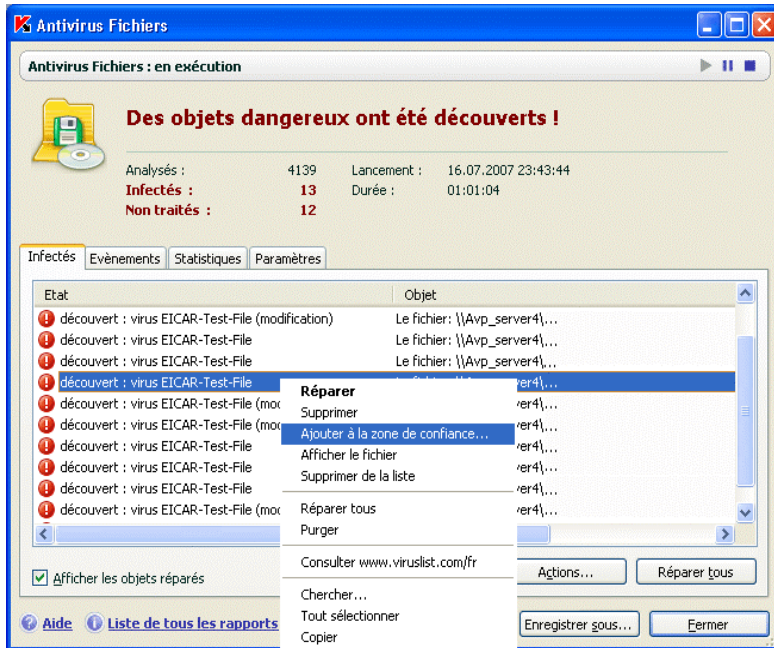


Illustration 8. Création d'une règle d'exclusion au départ du rapport

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**.

6.4. Lancement d'une tâche avec les privilèges d'un utilisateur

Kaspersky Anti-Virus 6.0 SOS 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.

Cette option n'est pas disponible sous Microsoft Windows 98/ME.

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

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

1. Sélectionnez le nom de la tâche dans la section **Analyser** (pour la recherche de virus) ou **Service** (pour la mise à jour ou la copie des mises à jour) de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.
2. Cliquez sur le bouton **Configuration** dans la boîte de dialogue de configuration de la tâche et passez à l'onglet **Complémentaire** dans la fenêtre qui s'affiche (cf. ill. 9).

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

N'oubliez pas que la mise à jour programmée sera exécutée selon les privilèges du compte utilisateur en session si les privilèges ne sont pas définis. Si aucun utilisateur n'a ouvert une session à ce moment, si la configuration du lancement de la mise à jour sous un compte particulier et si la mise à jour a été programmée, alors elle sera exécutée avec les privilèges du compte SYSTEM.

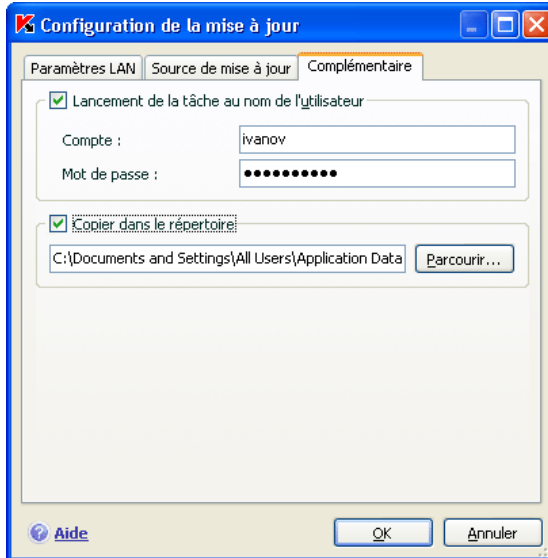


Illustration 9. Configuration du lancement de la mise à jour au nom d'un autre utilisateur

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

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

L'exécution des tâches de recherche de virus définies lors de l'installation est désactivée par défaut. La seule exception est la tâche d'analyse des objets de démarrage qui est exécutée chaque fois que Kaspersky Anti-Virus est lancé. S'agissant des mises à jour, elles sont exécutées automatiquement par défaut au fur et à mesure que les mises à jour sont publiées sur les serveurs de Kaspersky Lab.

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

Afin d'activer le lancement programmer d'une tâche, cochez la case en regard de la condition de lancement de la tâche dans le bloc **Mode d'exécution**. Vous pouvez modifier les conditions de lancement de l'analyse dans la fenêtre **Programmation** (cf. ill. 10) en cliquant sur **Modifier...**

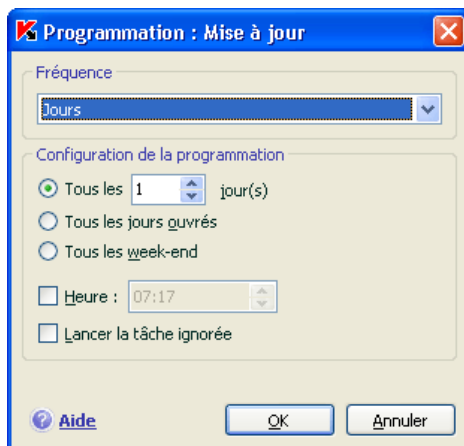


Illustration 10. Programmation de l'exécution de la tâche

L'élément le plus important à définir, c'est l'intervalle selon lequel l'événement aura lieu (exécution de la tâche ou envoi des notifications). Pour ce faire, sélectionnez l'option souhaitée dans le groupe **Fréquence** (cf. ill. 10). Il faudra ensuite définir les paramètres de planification pour l'option choisie dans le bloc **Configuration de la programmation**. Vous avez le choix entre les options suivantes :

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

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

Jour. L'exécution de la tâche ou l'envoi de notifications a lieu tous les quelques jours. Définissez la valeur de l'intervalle dans les paramètres de programmation :

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

- Sélectionnez **Tous les jours ouvrés** si vous souhaitez exécuter l'action tous les jours du lundi au vendredi.
- Sélectionnez **Tous les week-ends** si vous voulez que la tâche soit lancée uniquement les samedi et dimanche.

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

- ④ **Semaines.** L'exécution de la tâche ou l'envoi de notifications a lieu certains jours de la semaine. Si vous avez choisi cette fréquence, il vous faudra cocher les jours d'exécution de la tâche dans les paramètres de la programmation. Précisez l'heure dans le champ **Heure**.
- ④ **Mois.** L'exécution de la tâche ou l'envoi de notifications a lieu une fois par mois à l'heure indiquée.
- ④ **Au moment défini.** L'exécution de la tâche ou l'envoi de notifications a lieu au jour et à l'heure indiqué.
- ④ **Au lancement de l'application.** L'exécution de la tâche ou l'envoi de notification a lieu à chaque démarrage de Kaspersky Anti-Virus. Vous pouvez également définir l'intervalle de temps après le lancement de l'application qui doit s'écouler avant l'exécution de la tâche.
- ④ **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).

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

6.6. Configuration de la productivité

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 5.4, p. 48) ou lancer l'analyse antivirus manuellement (cf. point 5.1, p. 45). 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 augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, le programme arrête par défaut la recherche des virus et libère des ressources pour l'application de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Afin que la recherche de virus ne dépende 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

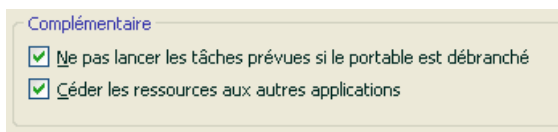


Illustration 11. Configuration de la productivité

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. ill. 10).

CHAPITRE 7. RECHERCHE DE VIRUS SUR L'ORDINATEUR

Kaspersky Anti-Virus 6.0 SOS 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.

Kaspersky Anti-Virus 6.0 SOS propose par défaut les tâches de recherche de virus suivantes :

Secteurs critiques

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

Mon poste de travail

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

Objets de démarrage

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

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres (cf. point 7.4, p. 66) et même programmer le lancement de la tâche (cf. point 6.5, p. 58).

Il est possible également de créer des tâches personnalisées (cf. point 7.3, p. 65) 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 trouvent 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 6.0 SOS 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.

7.1. Administration des tâches de recherche de virus

Les tâches liées à la recherche de virus peuvent être lancées manuellement ou automatiquement selon un horaire défini (cf. point 6.5, p. 58).

Afin de lancer la tâche de recherche de virus manuellement :

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

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

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

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

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

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

7.2. 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. 12).

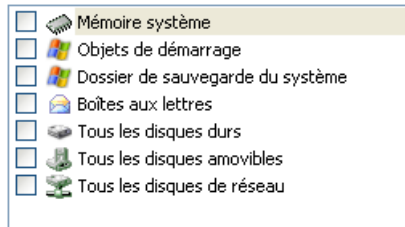


Illustration 12. Liste des objets à analyser

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

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

Pour le confort de l'utilisateur, il est possible d'ajouter aux zones d'analyse des catégories telles que les boîtes aux lettres de l'utilisateur, la mémoire système, les objets de démarrage, le dossier de sauvegarde du système d'exploitation et les objets situés dans le dossier de quarantaine de Kaspersky Anti-Virus 6.0 SOS.

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

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

Afin de lancer l'analyse, cliquez sur **Analyser** ou sélectionnez **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. 13). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.



Illustration 13. Analyse d'un objet au départ du menu contextuel de Microsoft Windows

7.3. 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 7.2, p. 63), indiquer les paramètres d'exécution de la tâche (cf. point 7.4, p. 66) et, le cas échéant, programmer (cf. point 6.5, p. 58) le lancement automatique.

Afin de renommer la tâche créée :

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

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

Pour supprimer une tâche créée :

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

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

Attention !

Vous pouvez uniquement renommer les tâches que vous avez créées.

7.4. Configuration des tâches liées à la recherche de virus

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

Afin de passer à la configuration des paramètres des tâches :

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

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

- sélectionner le niveau de protection pour l'exécution de la tâche (cf. point 7.4.1, p. 67);
- passer à la configuration détaillée du niveau :
 - indiquer les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 7.4.2, p. 68);
 - configurer le lancement des tâches au nom d'un autre compte utilisateur (cf. point 6.4, p. 56);

- définir les paramètres complémentaires de l'analyse (cf. point 7.4.5, p. 74);
- restaurer les paramètres d'analyse utilisés par défaut (cf. point 7.4.3, p. 71);
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou potentiellement infecté (cf. point 7.4.4, p. 71);
- programmer le lancement automatique de la tâche (cf. point 6.5, p. 58).

De plus, vous pouvez définir des paramètres uniques de lancement pour toutes les tâches (cf. point 7.4.6, p. 75).

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

7.4.1. Sélection du niveau de protection

Chaque tâche liée à la recherche de virus analyse les objets selon un des trois niveaux suivants (cf. ill. 14):

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.

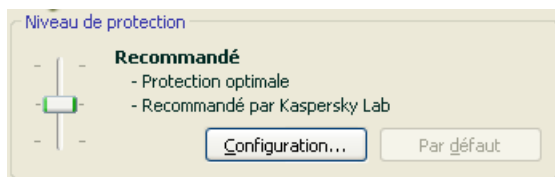


Illustration 14. Sélection du niveau de protection pour la recherche de virus

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

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

Pour modifier le niveau de protection :

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

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

Pour modifier les paramètres du niveau de protection actuel :



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

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

7.4.2. 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. 15). Choisissez l'une des trois options :


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

Informations.

Il existe 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. 162).

Conseil.

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

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

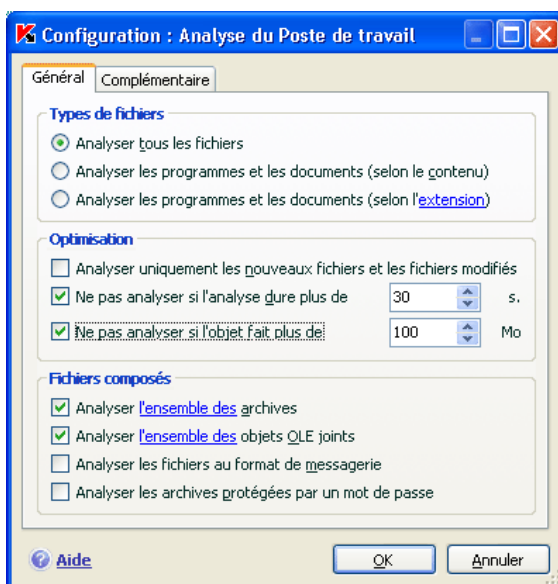


Illustration 15. Configuration des paramètres de l'analyse

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

- 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 6.0 SOS (par exemple : ICE, TAR, JAR, LHA) 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. Si la case est cochée, Kaspersky Anti-Virus 6.0 SOS décompose le fichier au format de messagerie et recherche la présence de virus dans chacun des composants du message (corps, pièce jointe). Si la case n'est pas sélectionnée, le fichier au format de messagerie est considéré comme un objet unique.

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

- Kaspersky Anti-Virus 6.0 SOS 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.

7.4.3. 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 de protection 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**.

7.4.4. 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. Cela signifie que le code du fichier contient probablement 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 suspects sont placés en quarantaine.

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

sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration de la tâche. Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 16).

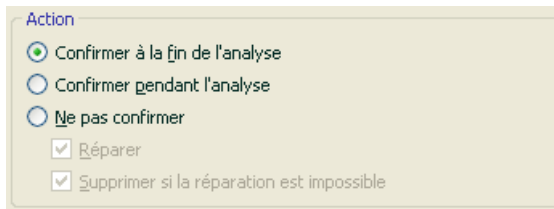


Illustration 16. Sélection de l'action à réaliser sur l'objet dangereux

Action choisie	Conséquence en cas de découverte d'un objet infecté/potentiellement infecté
<input checked="" type="radio"/> 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.
<input checked="" type="radio"/> Confirmer pendant l'analyse	Le programme affiche un message d'avertissement qui reprend les informations relatives au code malveillant source de l'infection (potentielle) et propose l'une des actions suivantes.

<input checked="" type="radio"/> Ne pas confirmer	<p>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.</p>
<input checked="" type="radio"/> Ne pas confirmer <input checked="" type="checkbox"/> Réparer	<p>Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la tentative échoue, l'objet est placé en quarantaine (cf. point 10.1, p. 95). Les informations relatives à cette situation sont consignées dans le rapport (cf. point 10.3, p. 101). Il est possible de tenter de réparer cet objet ultérieurement.</p>
<input checked="" type="radio"/> Ne pas confirmer <input checked="" type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer si la réparation est impossible	<p>Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la réparation de l'objet échoue, il sera supprimé.</p>
<input checked="" type="radio"/> Ne pas confirmer <input type="checkbox"/> Réparer <input checked="" type="checkbox"/> Supprimer	<p>Le programme supprimera automatiquement l'objet.</p>

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus 6.0 SOS crée une copie de sauvegarde avant de tenter de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde (cf. point 10.2, p. 99) au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

7.4.5. 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. 17):

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

Admettons que vous ayez une archive qui a été analysée par le programme et qui est saine. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez changé le contenu de l'archive (ex. : ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases des signatures des menaces, l'archive sera analysée à nouveau.

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 6.0 SOS (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

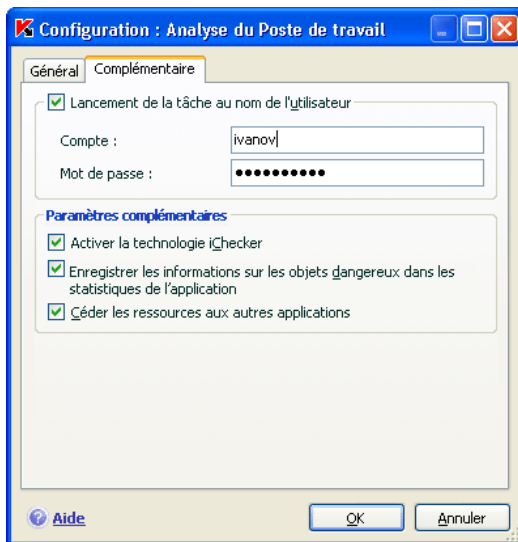


Illustration 17. Configuration complémentaire de l'analyse

- Enregistrer les informations sur les objets dangereux dans les statistiques de l'application:** enregistre les informations sur la découverte d'objets dangereux dans les statistiques globales de l'application et affiche la liste des menaces dangereuses sur l'onglet Infectés de la fenêtre du rapport (cf. point 10.3.2, p. 104). Si la case n'est pas cochée, les informations relatives aux objets dangereux ne seront pas reprises dans le rapport et par conséquent, il sera impossible de traiter ces objets.
- Céder les ressources aux autres applications :** interrompt la recherche de virus si les ressources du processeur sont occupées par d'autres applications.

7.4.6. 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 7.4.1, p. 67), réalisez la configuration complémentaire du niveau et indiquez l'action qui sera réalisée sur les objets (cf. point 7.4.4, p. 71).
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 8. ESSAI DE KASPERSKY ANTI-VIRUS 6.0 SOS

Une fois que vous aurez installé et configuré Kaspersky Anti-Virus 6.0 SOS, 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.

8.1. Virus d'essai EICAR et ses modifications

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

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. Lors de la recherche des virus Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS 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 « virus »	Le fichier contient le virus d'essai. Réparation	L'application identifie l'objet comme un objet malveillant qui ne

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

Préfixe	Etat du virus d'essai	Actions lors du traitement de l'objet par l'application
	impossible.	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 6.0 SOS 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.

8.2. 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 8.1, p. 77) ainsi que les versions modifiées du virus d'essai.
2. Créez une nouvelle tâche de recherche de virus (cf. point 7.3, p. 65) et en guise d'objet à analyser, sélectionnez le dossier contenant la sélection de virus d'essais (cf. point 7.2, p. 63).
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 7.1, p. 63) 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 :



Ainsi, en choisissant diverses actions, vous pouvez vérifier les réactions de Kaspersky Anti-Virus 6.0 SOS 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 9. MISE A JOUR DU LOGICIEL

Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillant apparaissent. Il est donc primordial de s'assurer que vous utilisez les versions des signatures des menaces les plus récentes.

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

- **Signature des menaces**

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

Les versions antérieures des logiciels antivirus de Kaspersky Lab prenaient en charge l'utilisation de différentes bases de signatures des menaces : *standard* ou *étendues*. Elles se différençaient par le type d'objets dangereux contre lesquels elles assuraient une protection. Avec Kaspersky Anti-Virus6.0 SOS, il n'est plus nécessaire de se soucier du choix des bases de signatures des menaces adéquates. Nos logiciels utilisent désormais les signatures des menaces qui offrent une protection non seulement contre divers types de programmes malveillants et d'objets présentant un risque potentiel.

- **Modules de l'application**

En plus des signatures des menaces connues, vous pouvez actualiser les modules logiciels de Kaspersky Anti-Virus 6.0 SOS. 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 6.0 SOS. Afin de pouvoir télécharger ces bases , votre ordinateur doit absolument être connecté à Internet.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Labs (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 95 797 87 00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 pour obtenir l'adresse d'un partenaire de Kaspersky Labs qui pourra vous donner les mises à jour sur disquette ou sur CD-ROM dans un fichier zip.

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 des mises à jour. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Lorsque Kaspersky Anti-Virus 6.0 SOS 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 de la source des mises à jour. Si les signatures et les composants installés sur votre ordinateur sont toujours d'actualité, un message relatif à l'actualité des signatures et des modules 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 6.0 SOS 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 9.2, p. 83) 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.

9.1. 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 9.4.1, p. 85).

Vous pouvez lancer la mise à jour du logiciel depuis :

- le menu contextuel (cf. point 4.2, p. 40);
- la fenêtre principale du logiciel (cf. point 4.3, p. 41).

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

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

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

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

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

N'oubliez pas que la copie des mises à jour dans une source locale aura lieu en même temps que l'exécution de la mise à jour, pour autant que ce service ait été activé (cf. point 9.4.4, p. 92).

9.2. Annulation de la dernière mise à jour

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Anti-Virus 6.0 SOS commence par créer une copie de sauvegarde de la version actuelle des signatures des menaces avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau la version antérieure des signatures après une mise à jour ratée.

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

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

9.3. Création de tâches liées à la mise à jour

Une tâche de mise à jour a été intégrée à Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS sur un ordinateur portable que vous utilisez à la maison et au bureau. A la maison, la mise à jour est téléchargée depuis les serveurs de Kaspersky Lab tandis qu'au

bureau, vous utilisez un répertoire local contenant les mises à jour à installer. Afin de ne pas devoir modifier les paramètres de mise à jour à chaque fois, vous pouvez créer deux règles 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 programme n'accepte qu'un maximum de deux tâches créées par l'utilisateur.

La nouvelle tâche applique tous les paramètres 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.

Après la création des tâches, vous devrez procéder aux configurations suivantes: indiquer la source de la mise à jour (cf. p.9.4.1, p. 85), définir les paramètres de connexion (cf. p.9.4.3, p. 90) et, le cas échéant activer le lancement avec les privilèges (cf. p.6.4, p. 56) et configurer la programmation (cf. p.6.5, p. 58).

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 que vous avez créées.

9.4. 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 9.4.1, p. 85);
- le mode de lancement de la mise à jour du logiciel et les éléments mis à jour (cf. point 9.4.2, p. 88);
- la fréquence d'exécution de la mise à jour si le lancement automatique a été configuré (cf. point 6.4, p. 56);
- le nom du compte utilisateur sous lequel la mise à jour va être réalisée (cf. point 9.4.4, p. 92) ;
- la nécessité ou non de copier les mises à jour récupérées dans un répertoire local (cf. point 9.4.4; p. 92);
- les actions à réaliser après la mise à jour du logiciel.

Tous ces paramètres sont abordés en détails ci-après.

9.4.1. Sélection de la source des mises à jour

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

Vous pouvez choisir une des sources suivantes :

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

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Labs (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 95 797 87 00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 pour obtenir l'adresse d'un

partenaire de Kaspersky Labs qui pourra vous donner les mises à jour sur disquette ou sur CD-ROM dans un fichier zip.

Attention !

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

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

La sélection de la source de la mise à jour s'opère dans l'onglet **Source de mise à jour** (cf. ill. 18).

Par défaut la mise à jour s'opère depuis les serveurs de mise à jour de Kaspersky Lab. Cette liste n'est pas modifiable. Lors de la mise à jour, Kaspersky Anti-Virus 6.0 SOS consulte cette liste, contacte le premier serveur de la liste et tente de télécharger les mises à jour. Lorsque l'adresse sélectionnée ne répond pas, le logiciel choisit le serveur suivant et tente à nouveau de télécharger les bases antivirus.

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

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

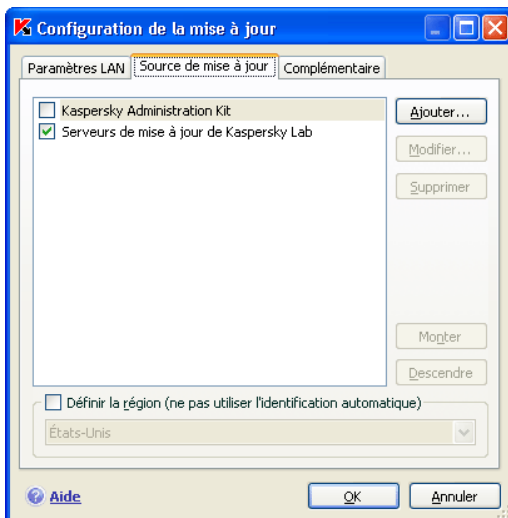


Illustration 18. Sélection de la source de la mise à jour

Attention !

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

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

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

Kaspersky Anti-Virus 6.0 SOS 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.

9.4.2. 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. 19) désignent les objets qui seront actualisés :

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

Les signatures des menaces sont actualisées à chaque fois tandis que les modules de l'application, les pilotes de réseau et les bases d'attaques de réseau sont actualisées uniquement lorsque le mode correspondant est activé.



Illustration 19. Sélection des objets de la mise à jour


Pour copier et installer les mises à jour des bases de nouvelles attaques de réseau et les pilotes de réseau 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. 20) désigne la manière dont la mise à jour sera lancée. Choisissez l'un des modes suivants dans le bloc **Mode de lancement** :

 **Automatique.** Kaspersky Anti-Virus 6.0 SOS vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source. 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 6.0 SOS tentera de réaliser la mise à jour chaque fois que la connexion sera établie ou selon un intervalle défini lors de la mise à jour antérieure. Les mises à jour réalisées au départ d'une source locales ont lieu à l'intervalle défini lors de la mise à jour précédente. Cela permet de régler automatiquement la fréquence des mises à jour en cas d'épidémie de virus ou d'autres situations dangereuses. Le logiciel recevra en temps opportuns les versions les plus récentes des signatures des menaces, des modules de l'application, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

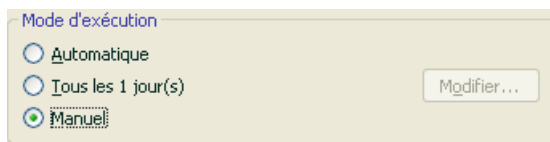




Illustration 20. Sélection du mode de lancement de la mise à jour

 **Toutes les 2 heures.** La mise à jour du logiciel est réalisée selon un horaire défini. Si vous souhaitez activer ce mode, la mise à jour sera réalisée par défaut toutes les deux heures. Pour composer un autre horaire, cliquez sur **Modifier** à côté du nom du mode et réalisez les modifications souhaitées dans la boîte de dialogue qui s'ouvre (pour de plus amples renseignements, consultez le point 6.5 à la page 58).

 **Manuel.** Vous lancez vous-même la procédure de mise à jour du logiciel. Kaspersky Anti-Virus 6.0 SOS vous avertira de la nécessité de réaliser la mise à jour (si le service de notification est activé) :

- Tout d'abord, une infobulle apparaît au-dessus de l'icône de l'application dans la barre des tâches (cf. point 10.8, p. 114);

- Ensuite, 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. 41).

9.4.3. 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. 21).

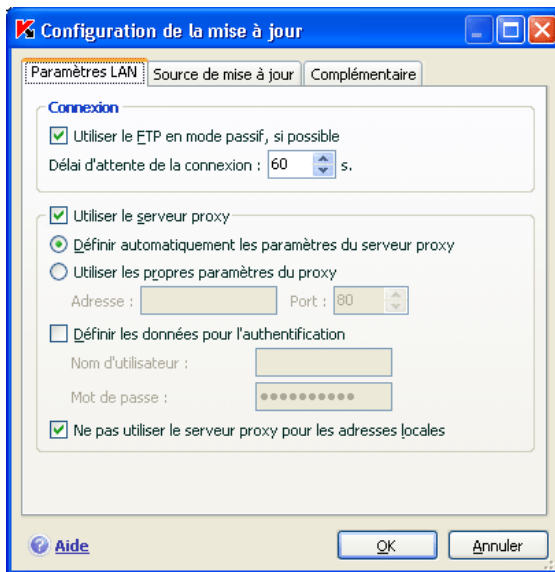


Illustration 21. Configuration des paramètres de réseau de la mise à jour

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 désélectionner 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 qu'il faudra utiliser pour la mise à jour :
 - Définir automatiquement les paramètres du serveur proxy** : utilise le serveur proxy indiqué dans les paramètres de connexion de Microsoft Internet Explorer.
 - Utiliser les propres paramètres du proxy** : utilise un serveur proxy différent de celui indiqué dans les paramètres de connexion du navigateur. Saisissez l'adresse IP ou le nom symbolique dans le champ **Adresse** et dans le champ **Port**, le port du serveur proxy.
- indiquez si l'authentification est requise sur le serveur proxy. *L'authentification* est une procédure de vérification des données d'enregistrement de l'utilisateur afin de contrôler l'accès.

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

Si la case n'est pas cochée ou si les données ne sont pas définies, le système procédera à une tentative d'utilisation NTML en utilisant le compte utilisateur au nom duquel la mise à jour est lancée cf. point 6.4, p. 56).

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

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

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.

9.4.4. Copie des mises à jour

Le service de copie des mises à jour permet d'optimiser 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

Pour activer la copie des mises à jour, cochez la case **Copier dans le répertoire** de l'onglet **Complémentaire** (cf. ill. 22) et dans le champ situé en dessous, indiquez le chemin d'accès au dossier partagé dans lequel les mises à jour seront sauvegardées. Le chemin d'accès peut être saisi manuellement ou dans la fenêtre qui s'ouvre dès que vous aurez cliqué sur **Parcourir**. Si la case est cochée, les nouvelles mises à jour seront copiées automatiquement dans ce répertoire.

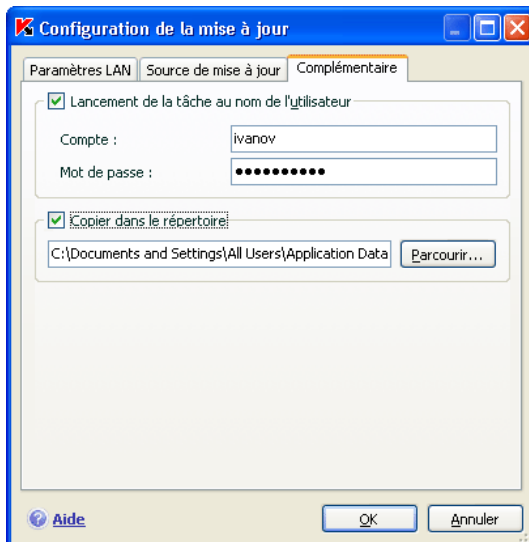


Illustration 22. Configuration du service de copie des mises à jour

N'oubliez pas que Kaspersky Anti-Virus 6.0 SOS 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.

9.4.5. Actions exécutées après la mise à jour du logiciel

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

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

Pourquoi ces objets et pas d'autres ?

La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infectés (cf. point 10.1, p. 95). Il se peut que la version actualisée des signatures des menaces de Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS propose une tâche d'analyse des objets de démarrage (cf. Chapitre 7, p. 62). 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. 58).

CHAPITRE 10. POSSIBILITES COMPLEMENTAIRES

En plus de protéger vos données, le logiciel propose des services complémentaires qui élargissent les possibilités de Kaspersky Anti-Virus 6.0 SOS.

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 6.0 SOS (cf. point 10.2, p. 99). 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 10.1, p. 95).

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 6.0 SOS (cf. point 10.6, p. 111). 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 6.0 SOS (cf. point 10.8, p. 114). Il peut s'agir d'événements à caractère informatif ou d'erreurs qui nécessitent une réaction immédiate et dont il faut avoir conscience.
- 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 10.5, p. 109).

Le logiciel propose également une aide (cf. point 10.4, p. 108) détaillée et des rapports complets (cf. point 10.3, p. 101) sur l'exécution de toutes les tâches liées à la recherche de virus.

Vous pouvez également modifier l'aspect extérieur de Kaspersky Anti-Virus 6.0 SOS et configurer les paramètres de l'interface actuelle (cf. point 10.7, p. 112).

Examinons en détails ces différents services.

10.1. 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 6.0 SOS 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 6.0 SOS le classe comme un objet potentiellement infecté.

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

L'objet potentiellement infecté peut-être identifié et mis en quarantaine lors de la recherche de virus.

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.

10.1.1. 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 6.0 SOS ;
- 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. 23) :

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

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

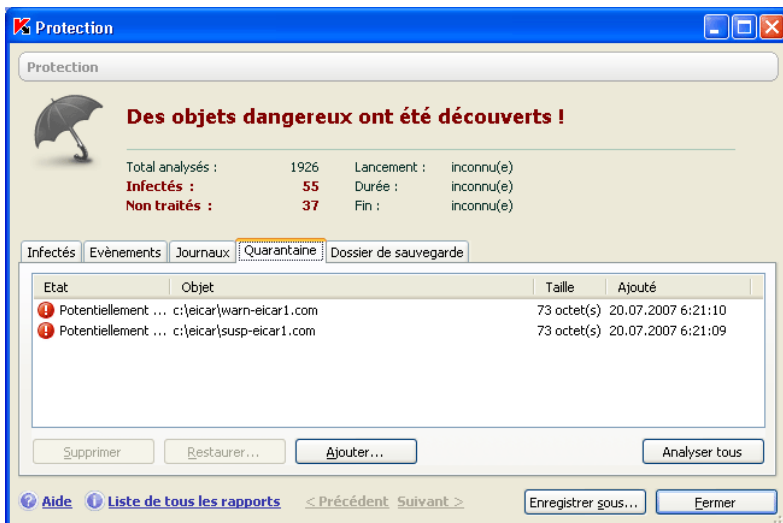


Illustration 23. Liste des objets en quarantaine

- 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**.

10.1.2. 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 (cf. point 9.4.4, p. 92).

Attention !

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

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

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

Pour ce faire :

1. Ouvrez la fenêtre des paramètres de Kaspersky Anti-Virus 6.0 SOS en cliquant sur **Configuration** dans la fenêtre principale.
2. Sélectionnez **Rapports** dans l'arborescence.
3. Définissez dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. ill. 24) le délai de conservation au terme duquel les objets seront automatiquement supprimés.



Illustration 24. Configuration de la conservation des objets en quarantaine

10.2. 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.

10.2.1. Manipulation des copies de sauvegarde

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

- Le nombre de copies de sauvegarde créées par Kaspersky Anti-Virus 6.0 SOS ;
- 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. 25) reprend la liste des copies de sauvegarde. Les informations suivantes sont fournies pour chaque copie : nom complet de l'objet avec indication du chemin d'accès à son emplacement d'origine, l'état de l'objet attribué suite à l'analyse et sa taille.

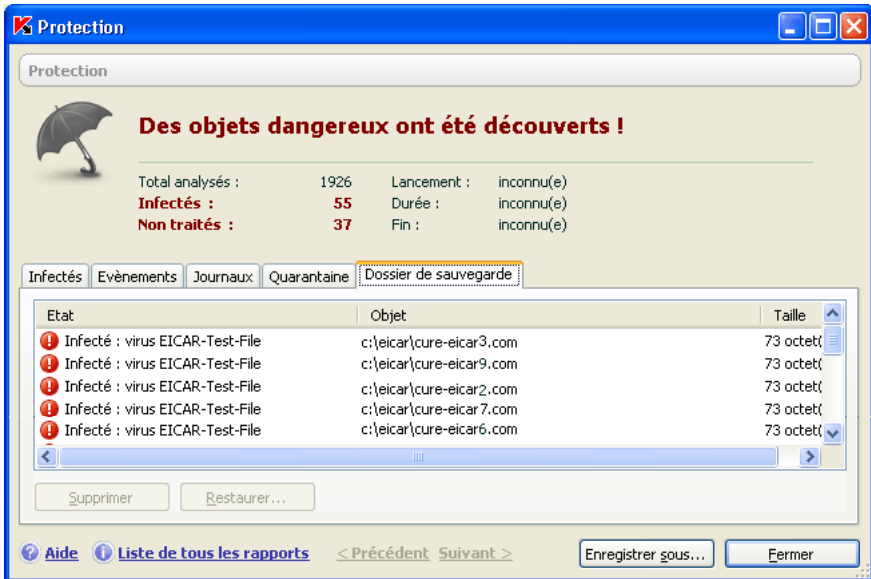


Illustration 25. Copies de sauvegarde des objets supprimés ou réparés

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 effet entraîner l'infection de votre ordinateur.

Il est conseillé d'examiner fréquemment le contenu du dossier et de le nettoyer à l'aide du bouton **Supprimer**. Vous pouvez également configurer le logiciel afin qu'il supprime les copies les plus anciennes du répertoire (cf. point 10.2.2, p. 101).

10.2.2. 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 6.0 SOS en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Rapports** dans l'arborescence.
3. Définissez le délai de conservation des copies de sauvegarde dans le bloc **Quarantaine & Dossier de sauvegarde** (cf. ill. 24) dans la partie droite de la fenêtre.

10.3. Utilisation des rapports

L'exécution de chaque tâche liée à la recherche de virus et à la mise à jour est consignée dans un rapport. Le total des rapports composés par le logiciel en ce moment ainsi que leur taille totale (en octets) sont repris dans les **Rapports** de la section **Services** de la fenêtre principale du logiciel. Ces informations sont reprises dans le bloc **Rapports**.

Pour consulter les rapports :

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

La fenêtre s'ouvre sur l'onglet **Rapports** (cf. ill. 26). Vous y verrez les derniers rapports les tâches antivirus lancées au cours de cette session de Kaspersky Anti-Virus 6.0 SOS. Le résultat du fonctionnement est affiché en regard de chaque 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**.

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

sélectionnez le nom de la tâche dans l'onglet **Rapports** et cliquez sur **Détails**.



Illustration 26. Rapports sur le fonctionnement d'une tâche de recherche de virus

Cette action entraîne l'ouverture d'une fenêtre contenant des informations détaillées sur le fonctionnement de la tâche sélectionnée. Les statistiques sont reprises dans la partie supérieure de la fenêtre tandis que les détails apparaissent sur divers onglets de la partie centrale:

- L'onglet **Infectés** contient la liste des objets dangereux découverts par le logiciel.
- **Evénements** illustre les événements survenus pendant l'exécution de la tâche.
- L'onglet **Statistiques** reprend les statistiques détaillées de tous les objets analysés.
- L'onglet **Paramètres** reprend les paramètres qui définissent le fonctionnement, de la recherche de virus ou de la mise à jour des signatures des menaces.

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 adresser 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 de la tâche dont vous souhaitez consulter le rapport; 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 lancer 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 objet de la liste ou à une sélection d'objets.

Supprimer de la liste : supprime les informations relatives 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 6.0 SOS 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.

10.3.1. 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 6.0 SOS 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. 27), 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.

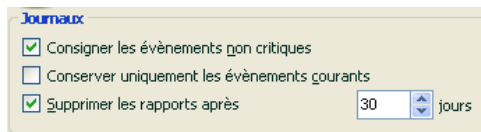


Illustration 27. Configuration des paramètres de constitution des rapports

10.3.2. Onglet *Infectés*

Cet onglet (cf. ill. 28) contient la liste des objets dangereux découverts par Kaspersky Anti-Virus 6.0 SOS. 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**.

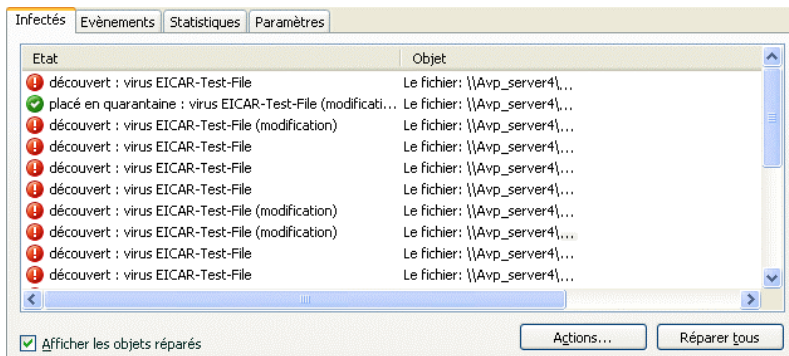


Illustration 28. Liste des objets dangereux découverts

Le traitement des objets dangereux découverts par Kaspersky Anti-Virus 6.0 SOS 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.

10.3.3. Onglet *Evénements*

Cet onglet (cf. ill. 29) reprend la liste de tous les événements importants survenus, lors de l'exécution d'une tâche liée à la recherche de virus ou de la mise à jour des signatures des menaces.

Les événements prévus sont :

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

Evénements informatifs. Événements 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.

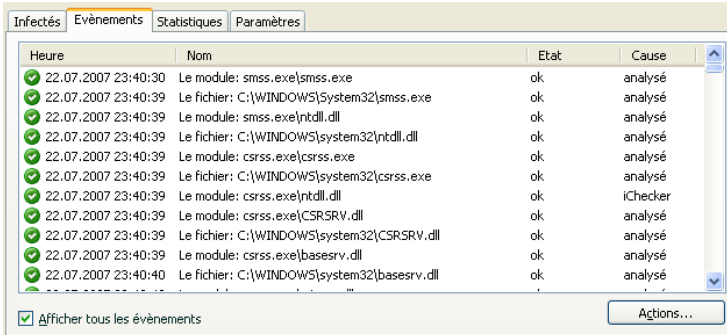


Illustration 29. Evénements survenus pendant

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

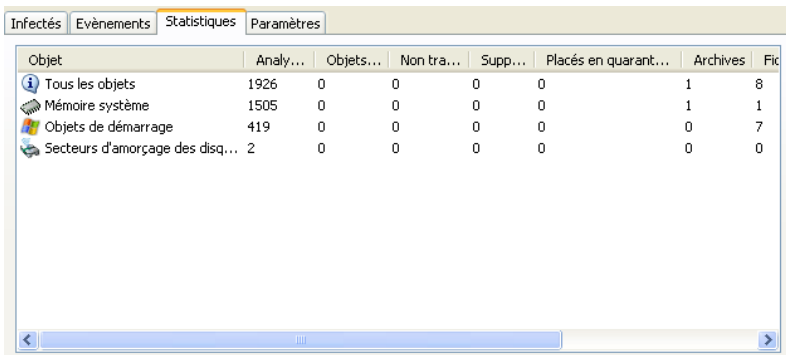
- Le nom de l'événement;
- Le nom de l'objet pour lequel cet événement a été consigné;
- L'heure à laquelle l'événement est survenu;
- La taille du fichier téléchargé.

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.

10.3.4. Onglet Statistiques

Cet onglet reprend les statistiques détaillées du fonctionnement de l'exécution des tâches liées à la recherche de virus (cf. ill. 30). Vous pouvez voir :

- Le nombre d'objets soumis à l'analyse 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.



Objet	Analy...	Objets...	Non tra...	Supp...	Placés en quarant...	Archives	Fic
Tous les objets	1926	0	0	0	0	1	8
Mémoire système	1505	0	0	0	0	1	1
Objets de démarrage	419	0	0	0	0	0	7
Secteurs d'amorçage des disq...	2	0	0	0	0	0	0

Illustration 30. Statistique du composant

10.3.5. Onglet *Paramètres*

Cet onglet (cf. ill. 31) présente tous les paramètres qui définissent l'exécution des tâches liées à la recherche de virus ou à la mise à jour. Vous pouvez voir le niveau de protection défini pour la recherche de virus, les actions exécutées sur les objets dangereux, les paramètres appliqués à la mise à jour, etc. Pour passer à la configuration des paramètres, cliquez sur Modifier les paramètres.

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

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

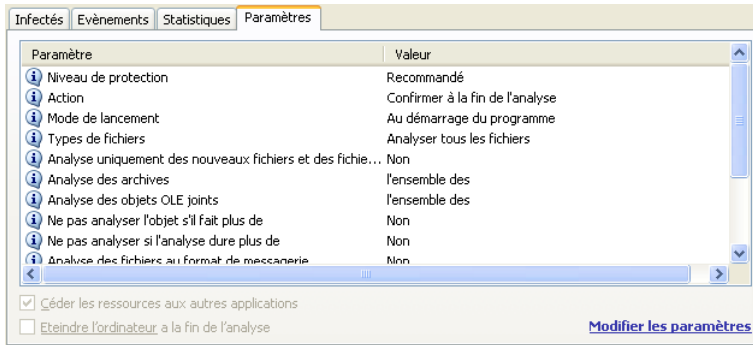


Illustration 31. Paramètres de fonctionnement du composant

- 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.

10.4. Informations générales sur le logiciel

La section **Services** de la fenêtre principale affiche des informations générales sur le logiciel (cf. ill. 32).

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 6.0 SOS.

Toutes ces informations sont nécessaires lors des contacts avec le service d'Assistance technique de Kaspersky Lab (cf. point 10.6, p. 111).



Illustration 32. Informations relatives au logiciel, à la licence et au système sur lequel il est installé

10.5. Administration des licences

Kaspersky Anti-Virus 6.0 SOS fonctionne grâce à une *licence*. Elle vous est donnée lors de l'achat du logiciel et vous donne le droit d'utiliser celui-ci dès le jour de l'activation de la clé.

Sans la clé de licence et sans activation de la version d'évaluation, Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS 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 mettre à jour les signatures des menaces. Vous pourrez toujours analyser votre ordinateur à l'aide de la recherche de virus, 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 votre ordinateur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la licence d'utilisation de Kaspersky Anti-Virus 6.0 SOS. Deux semaines avant la date d'expiration, le programme vous avertira. Au cours des deux semaines suivantes, le programme affichera à chaque démarrage le message de circonstance.

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

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

ou:

Achetez une nouvelle clé de licence ou un code d'activation directement chez Kaspersky Lab en cliquant sur le lien Activer dans la fenêtre des clés de licence (cf. ill. Illustration 33). Remplissez le formulaire qui s'affiche dans notre site. Dès que le paiement aura été reçu, un message contenant un lien sera envoyé à l'adresse électronique indiquée dans le formulaire de commande. Ce lien vous permettra de télécharger la clé de licence ou d'obtenir le code d'activation de l'application.

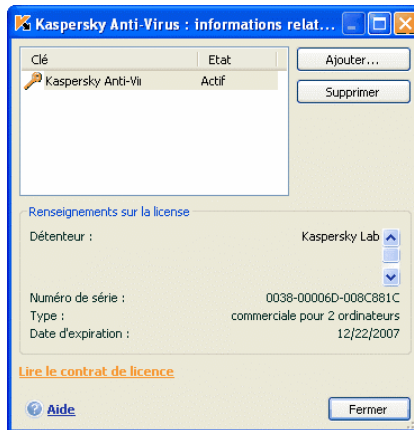


Illustration 33. Informations relatives à la licence

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. Illustration 33) 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 3.2.1, p. 30).. 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](#).

10.6. Service d'assistance technique aux utilisateurs

Kaspersky Anti-Virus 6.0 SOS 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. 34) dans la section **Services**.



Illustration 34. Informations relatives à l'assistance technique

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

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

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

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

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

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

10.7. Configuration de l'interface de Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS 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 6.0 SOS à l'aide du lien [Configuration](#) de la fenêtre principale.
2. Sélectionnez **Apparence** dans le groupe **Services** de l'arborescence des paramètres du logiciel (cf. ill. 35).

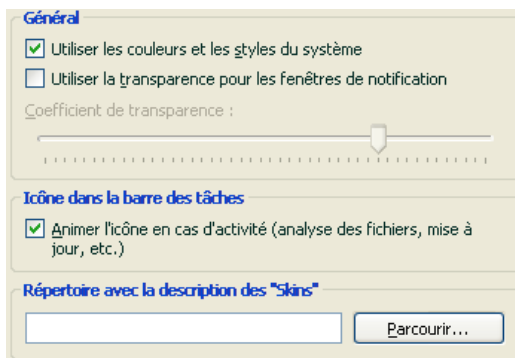


Illustration 35. Configuration de l'interface du programme

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

- 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 l'application sur votre ordinateur : si l'application tourne, l'icône sera grise.

- Degré de transparence des infobulles.

Toutes les opérations de Kaspersky Anti-Virus 6.0 SOS 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 placez 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 option n'est pas disponible pour les versions installées sous Windows NT 4.0.

- 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 6.0 SOS peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel, localiser l'interface dans la langue de votre choix. Pour activer votre propre environnement graphique, indiquez le répertoire avec ses paramètres dans le champ **Répertoire avec la description des "Skins"**. Cliquez sur **Parcourir...** pour sélectionner le répertoire

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

N'oubliez pas que la modification des paramètres de l'interface de Kaspersky Anti-Virus 6.0 SOS n'est pas préservée lors du rétablissement des paramètres par défaut ou de la suppression du programme.

10.8. Notifications relatives aux événements de Kaspersky Anti-Virus 6.0 SOS

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus 6.0 SOS. 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 6.0 SOS, 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. Ouvrez la fenêtre de configuration de l'application à l'aide du lien Paramètres de la fenêtre principale. Sélectionnez le point **Service** dans l'arborescence des paramètres.

2. Cochez la case **Activer les notifications sur les événements** dans le bloc **Interaction avec l'utilisateur**(cf. ill. 36).

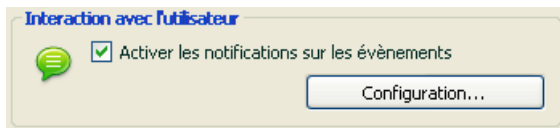


Illustration 36. Activation des notifications

3. Définir le type d'événements de Kaspersky Anti-Virus 6.0 SOS au sujet desquels vous souhaitez être averti, ainsi que le mode de notification (cf. point 10.8.1.1, p. 115).
4. Configurez les paramètres d'envoi des notifications par courrier électronique si vous avez choisi ce mode (cf. point 10.8.1.2, p. 117).

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

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus 6.0 SOS.

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

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

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

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

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

1. Cliquez sur le lien Configuration dans la fenêtre principale du logiciel.
2. Dans la boîte de configuration du logiciel, sélectionnez la section **Services**, cochez la case **Activer les notifications sur les**

événements et passez à la configuration détaillée en cliquant sur **Configuration...** .

Dans la fenêtre **Configuration des notifications** (cf. ill. 37) qui s'ouvre, vous pouvez définir les modes d'envoi suivants pour les notifications :

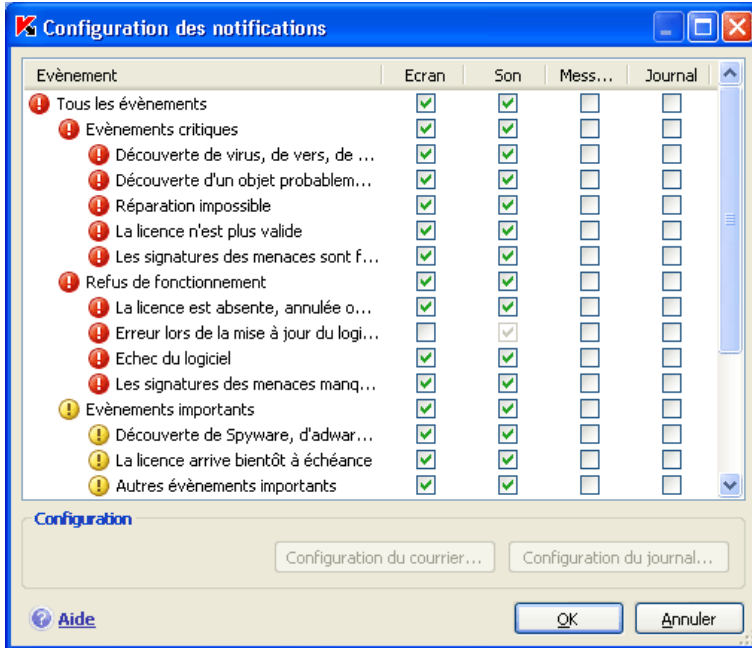


Illustration 37. Evènement survenu pendant le fonctionnement du logiciel et modes de notification choisis.

- *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 10.8.1.2, p. 117).

- 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 **Evènement** et configurez les paramètres du journal des événements (cf. point 10.8.1.3, p. 118).

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

Après avoir sélectionné les événements (cf. point 10.8.1.1, p. 115) au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications. Pour ce faire :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Complémentaire** dans le bloc **Interaction avec l'utilisateur** de la partie droite de la fenêtre.
4. Sur l'onglet **Configuration des 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.

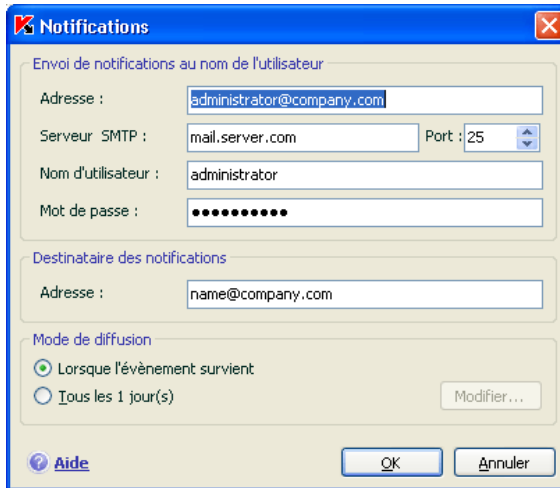


Illustration 38. Configuration de la notification par courrier électronique

10.8.1.3. Configuration du journal des événements

Pour configurer le journal des événements :

1. Cliquez sur le lien Configuration dans la fenêtre principale afin d'ouvrir la fenêtre de configuration de l'application.
2. Sélectionnez le point **Services** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration...** 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 6.0 SOS 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 6.0 SOS (**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**.

10.8.2. Restriction de l'accès à l'application

Kaspersky Anti-Virus 6.0 SOS 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 de protection contre les interactions distantes ainsi que la protection de l'accès via un mot de passe.

Afin de restreindre l'accès à l'application :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point Services dans l'arborescence des paramètres.
3. Dans le groupe **Autodéfense** (cf. ill. 39), cochez la **Interdire l'administration externe du service**. Dans ce cas, toutes les tentatives d'administration à distance des services de l'application seront bloquées :

Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la barre des tâches en cas de tentative d'administration externe de l'application (pour autant que le service de notification n'a pas été annulé par l'utilisateur).

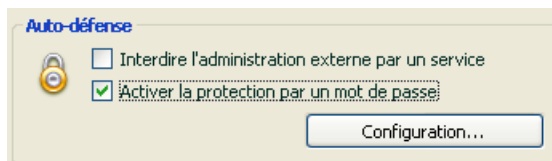


Illustration 39. Configuration de la protection du programme

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. 40). 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 6.0 SOS.
- 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.

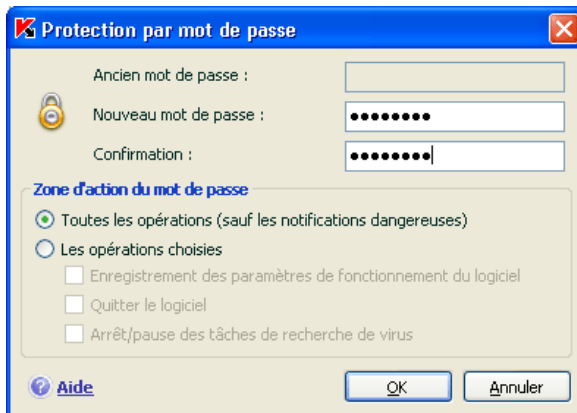


Illustration 40. Configuration de la protection par mot de passe

10.9. Exportation/importation des paramètres de Kaspersky Anti-Virus 6.0 SOS

Kaspersky Anti-Virus 6.0 SOS vous permet d'exporter et d'importer ses 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 6.0 SOS.
2. Cliquez sur le lien **Configuration** dans la section **Services**.
3. Cliquez sur le bouton **Exporter** dans le bloc **Administration de la configuration**.
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

Pour importer les paramètres du fichier de configuration :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus 6.0 SOS.
2. Cliquez sur le lien **Configuration** dans la section **Services**.
3. Cliquez sur **Importer** et sélectionnez le fichier contenant les paramètres que vous souhaitez importer dans Kaspersky Anti-Virus 6.0 SOS.

10.10. Restauration des paramètres par défaut

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

Pour restaurer les paramètres de protection :

1. Sélectionnez la section **Services** et ouvrez la fenêtre des paramètres du logiciel à l'aide du lien **Configuration**.
2. Cliquez sur le bouton **Restaurer** dans la section **Administration de la configuration**.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et de quels composants que vous souhaitez conserver en plus de la restauration du niveau de protection recommandé.

Par défaut, tous les paramètres uniques présentés dans la liste seront conservés (la case correspondante n'est pas sélectionnée). Si certains paramètres n'ont pas besoin d'être conservés, cochez la case située en regard de ceux-ci.

Une fois la configuration terminée, cliquez sur **Suivant**. Cela lancera l'Assistant de configuration initiale du logiciel (cf. point 3.2, p. 29). Suivez les instructions affichées.

Lorsque vous aurez quitté l'Assistant, toutes les tâches 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 11. UTILISATION DU PROGRAMME AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Anti-Virus 6.0 SOS à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- lancement, arrêt, suspension et reprise de l'exécution des tâches liées à la recherche de virus;
- obtention d'informations relatives aux tâches et à leur statistiques;
- Analyse des objets sélectionnés;
- Mise à jour des signatures des menaces et des modules du programme;
- Appel de l'aide relative à la syntaxe de la ligne de commande;
- Appel de l'aide relative à la syntaxe de la ligne de commande;

La syntaxe de la ligne de commande est la suivante :

avp.com <commande> [paramètres]

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

Où <commande> peut être remplacé par :

ADDKEY	Activation de l'application à l'aide du fichier de la clé (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
ACTIVATE	Activation de l'application via Internet à l'aide du code d'activation
START	lancement de la tâche
PAUSE	Suspension de la tâche (l'exécution de la commande

	est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
RESUME	reprise du fonctionnement du composant ou de la tâche
STOP	arrêt de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
STATUS	affichage de l'état actuel de la tâche
STATISTICS	affichage des statistiques de la tâche
HELP	aide sur la syntaxe de la commande ou la liste des commandes.
SCAN	Analyse antivirus des objets
UPDATE	Lancement de la mise à jour du programme
ROLLBACK	Annulation de la dernière mise à jour réalisée (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application).
EXIT	Quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mode passe défini via l'interface du programme)
IMPORT	importation des paramètres de protection de Kaspersky Anti-Virus 6.0 SOS (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
EXPORT	exportation des paramètres de protection de Kaspersky Anti-Virus 6.0 SOS

Chaque commande possède ses propres paramètres.

11.1. Activation du logiciel

L'application peut être activée de deux manières :

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

Syntaxe de la commande :

```
ACTIVATE <code_d'activation>
ADDKEY <nom_du_fichier>
/password=<votre_mot_de_passe>
```

Description des paramètres:

<nom_du_fichier>	Nom nom du fichier de clé de l'activation avec l'extension *.key.
<code_d'activation>	Code d'activation de l'application fourni à l'achat
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application.

N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.

Exemple :

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA11A1.key /password=<votre mot de passe>
```

11.2. Gérer les tâches

Syntaxe de la commande :

```
avp.com <commande> <nom_de_la_tâche>
avp.com STOP|PAUSE <nom_de_la_tâche>
/password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

Description des paramètres:

<p><commande></p>	<p>L'administration des tâches de Kaspersky Anti-Virus via la ligne de commande s'opère à l'aide de la sélection de commande suivante :</p> <p>START : lancement de la tâche.</p> <p>STOP : arrêt de la tâche.</p> <p>PAUSE : suspension de la tâche.</p> <p>RESUME : reprise de la tâche.</p> <p>STATUS : affichage de l'état actuel de la tâche.</p> <p>STATUS : affichage des statistiques actuelles de la tâche.</p> <p>La commande PAUSE ou STOP ne pourra être exécutée sans la saisie du mot de passe.</p>
<p><profil nom_de_la_tâche></p>	<p>Le paramètre <nom_de_la_tâche> peut prendre comme valeur le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour créée par l'utilisateur.</p> <p>Les valeurs suivantes sont prévues pour les tâches prédéfinies :</p> <p>UPDATER : mise à jour ;</p> <p>RetranslationCfg : copie de la mise à jour dans une source locale ;</p> <p>Rollback : remise à l'état antérieur à la mise à jour ;</p> <p>SCAN_OBJECTS : tâche d'analyse d'un objet particulier (fichier, répertoire ou disque) ;</p> <p>SCAN_MY_COMPUTER : analyse complète de l'ordinateur ;</p> <p>SCAN_CRITICAL_AREAS : tâche d'analyse des secteurs critiques ;</p> <p>SCAN_STARTUP : tâche d'analyse des objets de démarrage ;</p> <p>SCAN_QUARANTINE : tâche d'analyse des</p>

	objets en quarantaine..
<votre mot de passe>	mot de passe de Kaspersky Anti-Virus défini dans l'interface de l'application.
/R[A]:<fichier_de_rapport>	<p>R:<fichier_de_rapport> : consigne uniquement les événements importants dans le rapport.</p> <p>/RA:<fichier_de_rapport> : consigne tous les événements dans le rapport.</p> <p>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.</p>
Les tâches lancées via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.	

Exemple :

Pour arrêter la tâche d'analyse du poste de travail via la ligne de commande, saisissez :

```
avp.com STOP SCAN_MY_COMPUTER
/password=<votre_mot_de_passe>.
```

11.3. Analyse antivirus des fichiers

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types
de fichiers>] [<exclusions>] [<fichier de
configuration>] [<paramètres du rapport>>]
[<paramètres complémentaires>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans Kaspersky Anti-Virus 6.0 SOS en lançant la tâche requise via la ligne de commande (cf. point 11.1, page 125). 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>	<p>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.</p> <p>Remarques :</p> <ul style="list-style-type: none"> • Mettre le nom de l'objet entre guillemets s'il contient un espace; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/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>	<p>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.</p> <p>La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace</p>

<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur /i8 .	
/i0	aucune action n'est exécutée, seules les informations sont consignées dans le rapport.
/i1	réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx) (cette action est exécutée par défaut).
/i3	réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	supprimer les objets infectés; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.
Le paramètre <types de fichiers> définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
/fa	Analyser tous les fichiers.

<p>Le paramètre <exclusions> définit les objets exclus de l'analyse.</p> <p>Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.</p>	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque
-e:<seconds>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <seconds> .
-es:<size>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre <size> .
<p>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.</p> <p>Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus.</p> <p>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 6.0 SOS qui seront utilisées.</p>	
/C:<settings_file>	Utiliser les valeurs des paramètres définies dans le fichier de configuration <settings_file> .
<p>Le paramètre <paramètres du rapport> définit le format du rapport sur les résultats de l'analyse.</p> <p>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.</p>	
/R:<report_file>	Consigner uniquement les événements importants dans le fichier indiqué.

<code>/RA:<report_file></code>	Consigner tous les événements dans le rapport.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
<code>/iChecker=<on off></code>	Activer/désactiver l'utilisation de la technologie iChecker.

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 /@:object2scan.txt
/C:scan_settings.txt /RA:scan.log
```

11.4. Mise à jour du logiciel

La commande de mise à jour des modules du logiciel et des signatures des menaces de Kaspersky Anti-Virus 6.0 SOS possède la syntaxe suivante :

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

Description des paramètres:

<code><path/URL></code>	<p>Serveur HTTP, serveur FTP pour 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.</p>
<code>/R[A]:<report_file></code>	<p><code>/R:<report_file></code> : consigner uniquement les événements importants dans le rapport.</p> <p><code>/R[A]:<report_file></code> : consigner tous les événements dans le rapport.</p> <p>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.</p>
<code>/C:<settings_file></code>	<p>Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de l'application lors de la mise à jour.</p> <p>Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application.</p> <p>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 6.0 SOS qui seront utilisées.</p>
<code>/APP</code>	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 6.0 SOS en utilisant les paramètres du fichier de configuration **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

11.5. Remise du programme à l'état antérieur à la mise à jour

Syntaxe de la commande:

```
ROLLBACK [/R[A]:<report_file>] [/password=<mot de
passe>]
```

/R[A]:<report_file>	<p>/R:<report_file> : uniquement consigner les événements importants dans le rapport.</p> <p>/R[A]:<report_file> : consigner tous les événements dans le rapport</p> <p>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.</p>
<mot de passe>	Mot de passe pour Kaspersky Anti-Virus 6.0 SOS défini via l'interface de l'application.

N'oubliez pas que cette commande ne peut être exécutée sans la saisie préalable du mot de passe.

Exemple :

```
avp.com ROLLBACK /RA:rollback. txt /password=<votre mot de
passe>
```

11.6. Exportation des paramètres

Syntaxe de la commande :

```
avp.com EXPORT <profile> <filename>
```

Description des paramètres:

<profile>	<p>Tâche dont les paramètres sont exportés.</p> <p>Le paramètre <profile> peut prendre n'importe quelle des valeurs indiquées au point 11.2 à la page 125.</p>
------------------------	---

<filename>	<p>Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Anti-Virus 6.0 SOS. Vous pouvez indiquer un chemin relatif ou absolu.</p> <p>Le fichier de configuration est enregistré au format binaire (<i>dat</i>), si aucun autre format n'est indiqué ou défini, et peut servir au transfert des paramètres sur d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension <i>txt</i>. N'oubliez pas que l'importation de paramètres depuis un fichier texte n'est pas prise en charge, ce fichier peut être utilisé uniquement pour consulter les paramètres principaux de fonctionnement de l'application.</p>
-------------------------	---

Exemples:

```
avp.com EXPORT c:\ settings.dat
```

11.7. Importation des paramètres

Syntaxe de la commande :

```
avp.com IMPORT <nom_du_fichier> [/password=<mot de
passe>]
```

<nom_du_fichier>	<p>Chemin d'accès au fichier duquel sont importés les paramètres de Kaspersky Anti-Virus 6.0 SOS. Vous pouvez indiquer un chemin relatif ou absolu.</p> <p>L'importation des paramètres de protection est possible uniquement depuis un fichier au format binaire.</p>
<mot de passe>	<p>Mot de passe de Kaspersky Anti-Virus 6.0 SOS défini dans l'interface de l'application.</p>

Cette commande ne peut être exécutée sans la saisie du mot de passe.

Exemples:

```
avp.com IMPORT c:\ settings.dat /password=<votre mot de
passe>
```

11.8. Lancement de l'application

Syntaxe de la commande :

```
avp.com
```

11.9. Arrêt de l'application

Syntaxe de la commande :

```
EXIT /password=<mot de passe>
```

<mot de passe>	Mot de passe Kaspersky Anti-Virus 6.0 SOS défini via l'interface de l'application.
-----------------------------	--

Cette commande ne pourra être exécutée sans la saisie du mot de passe.

11.10. 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>
```

11.11. 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 12. 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 12.1, p. 137) ;
- au départ de la ligne de commande (cf. point 12.2, p. 139)
- via Kaspersky Administration Kit (cf. "Guide de déploiement de Kaspersky Administration Kit")
- via les stratégies de domaine de groupe de Microsoft Windows Server 2000/2003 (cf. point 3.4.3, p. 37).

12.1. 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 sont inutiles. Vous pouvez par exemple installer ou supprimer le connecteur à l'agent d'administration de Kaspersky Administration Kit.

Pour passer à la restauration de l'état d'origine du logiciel ou à l'installation de composants de Kaspersky Anti-Virus qui n'avaient pas été installés à l'origine ainsi que pour supprimer l'application :

1. Introduisez le cédérom d'installation dans le lecteur pour autant que vous ayez installé le logiciel à l'aide de ce cédérom. Si vous aviez procédé à l'installation au départ d'une autre source (dossier partagé, répertoire du disque dur, etc.), assurez que le fichier d'installation se trouve toujours dans cette source et que vous y avez accès.

2. Sélectionnez **Démarrez → Programmes → Kaspersky Anti-Virus 6.0 SOS → 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 6.0 SOS 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 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 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 6.0 SOS, sélectionnez l'option  **Supprimer l'application complète**. Pour sauvegarder les données, vous devrez sélectionner l'option  **Enregistrer les objets de l'application** et précisez quels objets exactement :

- *Informations relatives à l'activation* : fichier de la clé indispensable au fonctionnement de l'application.
- *Signatures des menaces* : toutes les signatures des programmes dangereux, des virus et des autres menaces qui datent de la dernière mise à jour.
- *Objets du dossier de sauvegarde* : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure.

- *Objets de la quarantaine* : objets qui sont peut-être modifiés par des virus ou leur modification. Ces objets contiennent un code semblable au code d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des signatures des menaces.
- *Paramètres de fonctionnement de l'application* : valeurs des paramètres de fonctionnement du logiciel.

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**.

12.2. Procédure de suppression de l'application via la ligne de commande

Pour supprimer Kaspersky Anti-Virus 6.0 SOS 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. point Chapitre 12, page 137)..

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

```
msiexec /x <nom_du_paquetage> /qn
```

Pour supprimer l'application en mode non interactif avec redémarrage de l'ordinateur, saisissez :

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

Si un mot de passe contre la suppression avait été défini lors de l'installation, il faudra absolument saisir ce mot de passe sans quoi la suppression ne pourra avoir lieu.

Pour supprimer l'application avec définition d'un mot de passe confirmant le privilège de suppression de l'application, saisissez :

```
msiexec /x <nom_du_paquetage> KLUNINSTPASSWD=***** :  
supprime l'application en mode interactif ;  
msiexec /x <nom_du_paquetage> KLUNINSTPASSWD=*****  
/qn : supprime l'application en mode non interactif
```

CHAPITRE 13. ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit est un système qui permet d'exécuter, de manière centralisée, les principales tâches d'administration de la sécurité des ordinateurs du réseau d'une entreprise. Il repose sur les applications faisant partie de la suite Kaspersky Business Optimal et Kaspersky Corporate Suite.

Kaspersky Anti-Virus 6.0 SOS est un des logiciels de Kaspersky Lab qui peut être administré directement via l'interface, via la ligne de commande (cette méthode est décrite ci-dessus dans la documentation) ou via Kaspersky Administration Kit (pour autant que l'ordinateur soit inclus dans le système d'administration centralisée à distance).

Il est possible de procéder à l'administration à distance de l'application via l'interface de Kaspersky Administration Kit. Pour ce faire :

- Déployez le *Serveur d'administration* dans le réseau, installez la *Console d'administration* sur le poste de travail de l'administrateur (pour de plus amples informations, consultez le manuel de déploiement de Kaspersky Administration Kit 6.0).
- Installez Kaspersky Anti-Virus 6.0 SOS et l'*Agent d'administration* (faisant partie de Kaspersky Administration Kit) sur les ordinateurs du réseau. Pour de plus amples informations sur l'installation à distance de Kaspersky Anti-Virus 6.0 SOS sur les ordinateurs du réseau, consultez le Manuel de déploiement de Kaspersky Administration Kit».

Faites attentions aux particularités suivantes lors de l'utilisation de Kaspersky Anti-Virus 6.0 SOS via Kaspersky Administration Kit !

Si la version 5.0 de Kaspersky Anti-Virus est installée sur le réseau, il faudra remplir les conditions suivantes avant de procéder à la mise à jour vers la version 6.0 via Kaspersky Administration Kit :

- Arrêtez la version antérieure de l'application (l'arrêt peut s'opérer à distance via Kaspersky Administration Kit);
- Avant de lancer l'installation, quittez toutes les applications ;
- Installez la version 6.0 de l'application.

Avant d'actualiser la version du module externe d'administration de Kaspersky Anti-Virus via Kaspersky Administration Kit, quittez la console d'administration.

L'administration de l'application via Kaspersky Administration Kit s'opère grâce à la console d'administration (cf. ill. Illustration 41). Cette console se présente sous la forme d'une **interface** standard **intégrée au MMC**. Grâce à elle, l'administrateur peut exécuter les tâches suivantes :

- Installation à distance de Kaspersky Anti-Virus 6.0 SOS et de *l'Agent d'administration* sur les ordinateurs du réseau ;
- Configuration à distance de Kaspersky Anti-Virus 6.0 SOS sur les ordinateurs du réseau ;
- Mise à jour des signatures des menaces et des modules de Kaspersky Anti-Virus 6.0 SOS ;
- Administration des licences d'utilisation de Kaspersky Anti-Virus 6.0 SOS sur les ordinateurs du réseau ;
- Consultation des informations relatives à l'activité de l'application sur les ordinateurs client.

Kaspersky Anti-Virus 6.0 SOS ne garantit pas la protection en temps réel de l'ordinateur. C'est la raison pour laquelle un ordinateur doté de Kaspersky Anti-Virus 6.0 SOS apparaît sous l'état **Critique.**

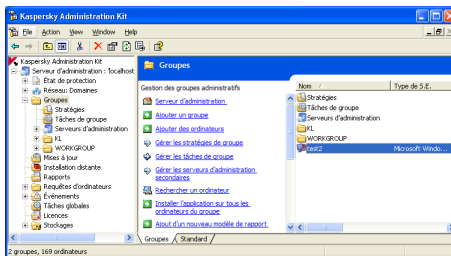


Illustration 41. Console d'administration de Kaspersky Administration Kit¹

En cas d'utilisation de Kaspersky Administration Kit, l'administration s'opère selon les paramètres des stratégies, les paramètres des tâches et les paramètres de l'application définis par l'administrateur.

Les paramètres de l'application regroupent les paramètres de fonctionnement de l'application, y compris les paramètres globaux de la tâche, les paramètres du dossier de sauvegarde et de la quarantaine, les paramètres de constitution des rapports, etc.

Une **Tâche** est une action exécutée par l'application. Les tâches de Kaspersky Anti-Virus 6.0 SOS sont réparties selon divers types (recherche de virus, mise à jour de l'application, remise à l'état antérieur à la mise à jour, installation de la clé de licence). A chaque tâche correspond un groupe de paramètres que le programme applique à l'exécution de la tâche. Il s'agit des *paramètres de la tâche*.

Parmi les particularités de l'administration centralisée, citons la répartition des ordinateurs distants en groupe et l'administration des paramètres via la création et la définition de stratégies de groupe.

La **stratégie** est un ensemble de paramètres de fonctionnement de l'application pour les ordinateurs des groupes du réseau logique ainsi qu'un ensemble de restrictions sur la redéfinition des paramètres lors de la configuration de l'application et des tâches sur un ordinateur client distant.

La stratégie intègre la configuration complète de toutes les fonctions de l'application. Elle porte sur les paramètres de l'application et les paramètres de tous les types de tâche, à l'exception des tâches spécifiques.

¹ L'apparence de la fenêtre principale de Kaspersky Administration Kit peut varier en fonction du système d'exploitation de l'ordinateur.

13.1. Administration de l'application

Kaspersky Administration Kit permet de gérer à distance le lancement et l'arrêt de Kaspersky Anti-Virus 6.0 SOS sur chaque ordinateur client, de même que la configuration des paramètres généraux de fonctionnement de l'application tels que l'activation ou la désactivation de la protection, la configuration du dossier de sauvegarde et de la quarantaine et la composition des rapports.

Pour administrer les paramètres de l'application :

1. Dans le dossier **Groupes** (cf. ill. Illustration 41), sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.
2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez modifier les paramètres de l'application. Utilisez la commande **Applications** du menu contextuel ou l'élément correspondant du menu **Actions**.
3. L'onglet **Applications** (cf. ill. Illustration 42) de la fenêtre des propriétés de l'ordinateur client reprend la liste complète de tous les logiciels Kaspersky Lab installés sur l'ordinateur client. Sélectionnez **Kaspersky Anti-Virus 6.0 SOS**.

En bas de la liste des applications, vous verrez un ensemble de boutons qui vous permettront de :

- Consulter la liste des événements survenus dans l'application au niveau de l'ordinateur client et enregistrées sur le Serveur d'administration ;
- Consulter les statistiques actuelles sur l'activité de l'application ;
- Configurer l'application (cf. point 13.1.2, page 146).

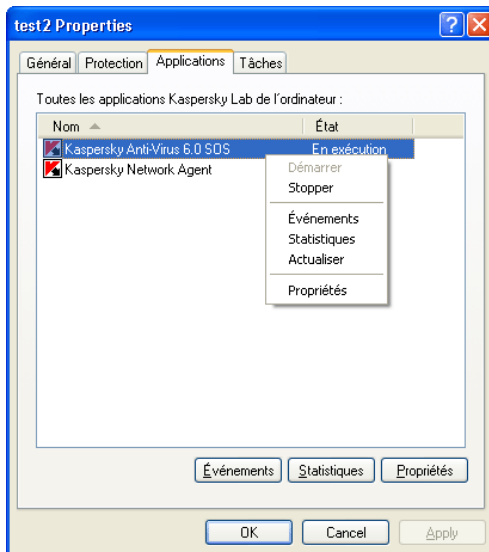


Illustration 42. Liste des applications Kaspersky Lab

13.1.1. Lancement et arrêt de l'application

Le lancement ou l'arrêt de Kaspersky Anti-Virus 6.0 SOS sur l'ordinateur client distant s'opère grâce à la commande du menu contextuel de la fenêtre des propriétés de l'ordinateur (cf. ill. Illustration 42).

Un résultat identique peut être obtenu grâce aux boutons **Lancer/Arrêter** de l'onglet **Général** (cf. ill. Illustration 43) dans la fenêtre de configuration de l'application.

La partie supérieure de la fenêtre indique le nom de l'application installée, la version, la date d'installation, le statut (application lancée ou arrêtée sur l'ordinateur local) et l'état des signatures de menaces.

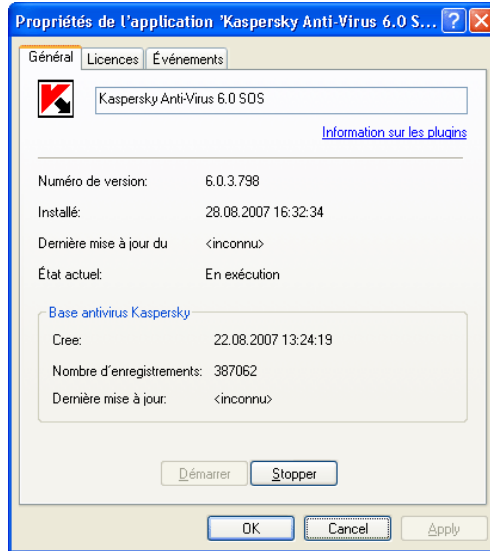


Illustration 43. Configuration de Kaspersky Anti-Virus 6.0 SOS.
Onglet **Général**

13.1.2. Configuration de l'application

Afin de consulter ou de modifier les paramètres de l'application :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Applications** (cf. ill. Illustration 42).
2. Sélectionnez **Kaspersky Anti-Virus 6.0 SOS** puis, cliquez sur le bouton **Propriétés**. La boîte de dialogue de configuration de l'application s'affichera (cf. ill. Illustration 44).

Ces onglets (à l'exception de l'onglet **Paramètres**) sont des onglets standard pour Kaspersky Administration Kit 6.0. Ils sont présentés en détail dans le manuel de l'administrateur de Kaspersky Administration Kit.

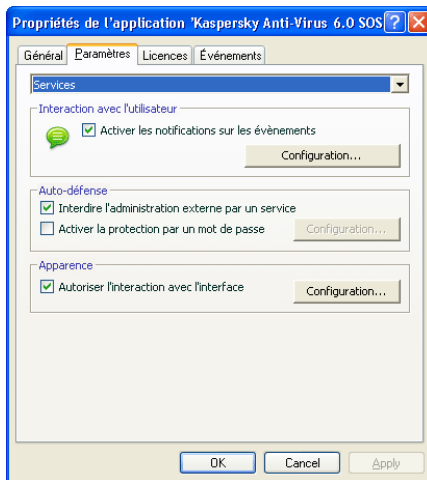


Illustration 44. Configuration de Kaspersky Anti-Virus.
Onglet **Paramètres**

Si une stratégie interdisant la modification de certains paramètres a été créée (cf. point 13.3, p. 155), la modification de la configuration de l'application sera impossible.

Vous pouvez, sur l'onglet **Paramètres**, définir les paramètres généraux et de service pour la protection assurée par Kaspersky Anti-Virus 6.0 SOS, les paramètres du dossier de sauvegarde et de la quarantaine, les paramètres de composition des rapports ainsi que les paramètres du réseau. Il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure :

Protection

Il est possible de :

- Configurer le lancement automatique de l'application au démarrage de l'ordinateur (cf. point 6.1, page 49).
- Constituer la liste des exclusions de l'analyse (cf. point 6.3, page 51).
- Sélectionner les catégories de programmes malveillants qui seront contrôlés par l'application (cf. point 6.2, p. 50);
- Configurer les performances de Kaspersky Anti-Virus 6.0 SOS.

Services

La configuration des services comporte:

- La configuration de la réception des notifications des événements survenus pendant l'utilisation de l'application (cf. point 10.8 , p. 114).
- La configuration de l'apparence de l'application sur l'ordinateur distant est une configuration particulière de Kaspersky Anti-Virus 6.0 SOS en cas d'administration via Kaspersky Administration Kit (cf. 10.8.2 point, p. 119);
- La configuration des paramètres de compatibilités entre Kaspersky Anti-Virus 6.0 SOS et d'autres applications (cf. point 13.1.3, p. 148).

Rapports

Cette fenêtre permet de configurer la composition des rapports statistiques sur le fonctionnement de l'application (cf. point 10.3.1, p. 103), ainsi que l'heure de placement des fichiers dans le dossier de sauvegarde (cf. point 10.1.2, p. 98) ou en quarantaine (cf. point 10.2.2 , p. 101).

13.1.3. Configuration des paramètres spécifiques

Si vous administrez Kaspersky Anti-Virus 6.0 SOS via Kaspersky Administration Kit, vous pouvez activer ou désactiver l'interaction entre l'application et l'utilisateur ainsi que modifier les informations relatives à l'assistance technique. Pour ce faire :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Applications** (cf. ill. Illustration 42). Sélectionnez **Kaspersky Anti-Virus 6.0 SOS** puis, cliquez sur le bouton **Propriétés**. La fenêtre de configuration de l'application s'ouvre.
2. Passez à l'onglet **Paramètres** (cf. ill. Illustration 44) et dans la liste déroulante de la partie supérieure, sélectionnez **Services**.

L'activation ou la désactivation du mode de fonctionnement interactif de Kaspersky Anti-Virus sur l'ordinateur distant s'opère au départ de l'onglet **Service** dans le groupe **Apparence** : affichage de l'icône de Kaspersky Anti-Virus 6.0 SOS dans la barre des tâches et notifications des événements survenus pendant l'utilisation de l'application (par exemple, découverte d'un objet dangereux).

Si la case **Autoriser l'interaction avec l'utilisateur** est cochée, l'utilisateur qui travaille sur l'ordinateur distant verra l'icône de l'application, les infobulles et il

pourra décider de l'action à prendre après chaque événement. Annulez la sélection de cette case pour désactiver le mode interactif.

Vous pouvez adapter les informations relatives à l'assistance techniques présentées sous le point **Assistance technique** de la rubrique **Service** au départ de l'onglet **Informations personnalisées pour l'assistance technique** de la fenêtre qui s'ouvre à l'aide du bouton **Configuration** (cf. ill. 34).

Il suffit de modifier le texte du champ supérieur. Dans le champ inférieur, modifiez la liste des liens qui apparaissent dans le groupe **Assistance technique en ligne** du point **Assistance technique** dans la rubrique **Services**.

Les boutons **Ajouter...**, **Modifier...** et **Supprimer...** vous permettent de modifier le contenu de la liste. Kaspersky Anti-Virus 6.0 SOS ajoute le nouveau lien en tête de liste. Il est possible de modifier l'ordre de la liste grâce au bouton **Monter/Descendre**.

Si aucune information n'est reprise dans la fenêtre, alors les informations proposées par défaut sur l'assistance technique ne seront pas modifiées.

13.2. Administration des tâches

Cette rubrique est consacrée à l'administration de tâches pour Kaspersky Anti-Virus 6.0 SOS. Pour obtenir de plus amples informations sur l'administration des tâches via Kaspersky Administration Kit 6.0, veuillez consulter le manuel de l'administrateur de ce logiciel.

Un ensemble de tâches système est créé pour chaque ordinateur du réseau lors de l'installation. Cette liste (cf. ill. Illustration 45) comprend certaines tâches en rapport avec la recherche de virus (Analyser mon poste de travail, analyse des objets de démarrage, analyse des secteurs critiques) ainsi que les tâches de mise à jour (mise à jour des signatures des menaces et des modules de l'application, retour à l'état antérieur à la mise à jour et la copie des mises à jour).

Vous pouvez administrer le lancement des tâches système et en configurer les paramètres. Il est toutefois impossible de les supprimer.

De plus, vous pouvez créer vos propres tâches, par exemple des tâches de recherche de virus, de mise à jour de l'application, d'annulation de la mise à jour ou d'installation des clés de licence (cf. point 13.2.2, p. 151).

Afin de consulter la liste des tâches créées pour l'ordinateur client :

1. Dans le dossier **Groupes** (cf. ill. Illustration 41), sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.

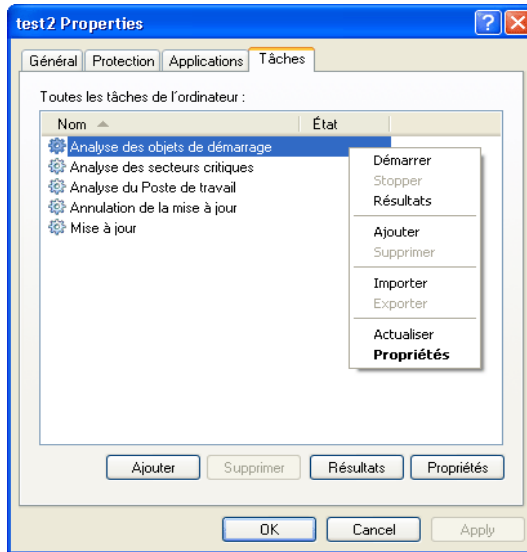


Illustration 45. Liste des tâches de Kaspersky Anti-Virus 6.0 SOS

2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez créer la tâche locale. Utilisez la commande **Tâches** du menu contextuel ou l'élément correspondant du menu **Actions**. Cette action entraîne l'ouverture de la fenêtre des propriétés de l'ordinateur client.
3. Toutes les tâches créées pour cet ordinateur client figure sur l'onglet **Tâches** (cf. Illustration 45)

13.2.1. Lancement et arrêt des tâches

Le lancement d'une tâche sur l'ordinateur est possible uniquement si l'application correspondante est lancée (cf. point 13.1.1, p. 145). En cas d'arrêt de l'application, l'exécution des tâches en cours sera interrompue.

Le lancement et l'arrêt des tâches s'opèrent soit automatiquement (selon l'horaire défini), soit manuellement (à l'aide de la commande du menu contextuel) ou depuis la fenêtre d'examen des paramètres de la tâche. Vous pouvez suspendre l'exécution d'une tâche puis la reprendre.

Afin de lancer /arrêter/interrompre/repandre manuellement une tâche :

Sélectionnez la tâche voulue, ouvrez le menu contextuel et sélectionnez **Démarrer/Stopper/Suspendre/Repandre** ou utilisez les éléments équivalents du menu **Actions**.

Les mêmes actions peuvent être réalisées au départ de la fenêtre de configuration de la tâche, dans l'onglet **Général** (cf. ill. Illustration 46) à l'aide des boutons identiques.

13.2.2. Création de tâches

Si vous utilisez Kaspersky Anti-Virus 6.0 SOS via Kaspersky Administration Kit, vous pouvez créer :

- Des tâches locales : définies pour un ordinateur client distinct.
- Des tâches de groupe : pour un groupe d'ordinateurs client.
- Des tâches globales : définies pour un ensemble d'ordinateurs clients issus de groupes du réseau local.

Vous pouvez modifier les paramètres des tâches, observer leur exécution, copier et déplacer les tâches d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Actions**.

13.2.2.1. Création d'une tâche locale

Afin de créer une tâche pour un ordinateur client particulier, procédez comme suit :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet Tâches (cf. ill. Illustration 45).
2. Cliquez sur Ajouter... pour ajouter une nouvelle tâche. Cette action entraîne l'ouverture de la boîte de dialogue de création d'une nouvelle tâche. Son interface se présente sous la forme d'un Assistant Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons Préc. et Suivant. Pour quitter l'Assistant, cliquez sur Terminer. Pour arrêter le programme à n'importe quel stade, cliquez sur Annuler.

Etape 1. Saisie des données générales sur la tâche

La première fenêtre de l'Assistant est une fenêtre d'introduction : il faut saisir ici le nom de la tâche (champ **Nom**).

Etape 2. Sélection de l'application et du type de tâche

Au cours de cette étape, vous devez préciser l'application pour laquelle vous créez la tâche, à savoir Kaspersky Anti-Virus 6.0 SOS. Il faut également sélectionner le type de tâche. Les tâches suivantes peuvent être créées pour Kaspersky Anti-Virus 6.0 SOS :

- *Recherche de virus* : recherche de virus dans les secteurs définis par l'utilisateur.
- *Mise à jour* : réception et installation des mises à jour pour l'application.
- *Remise à l'état antérieur à la mise à jour* : annulation de la dernière mise à jour effectuée.
- *Installation de la clé de licence* : ajout d'une nouvelle clé de licence d'utilisation de l'application.

Etape 3. Configuration des paramètres du type de tâche sélectionné

Le contenu des fenêtres suivantes varie en fonction du type de tâche sélectionné à l'étape précédente.

RECHERCHE DE VIRUS

Dans la fenêtre de configuration de la recherche de virus, il faut préciser l'action qui sera exécutée par Kaspersky Anti-Virus 6.0 SOS lors de la détection d'un objet dangereux (cf. point 7.4.4, p. 71) et dresser la liste des objets à analyser (cf. point 7.2, p. 63).

MISE A JOUR

Pour la mise à jour des signatures des menaces et des modules de l'application, il faut indiquer la source utilisée pour le téléchargement des fichiers de mise à jour (cf. point 9.4.1, p. 85). Les mises à jour sont téléchargées par défaut du serveur de mise à jour de l'application Kaspersky Administration Kit.

REMISE A L'ETAT ANTERIEUR A LA MISE A JOUR

La tâche liée à l'annulation de la dernière mise à jour effectuée ne dispose pas de paramètres particuliers.

INSTALLATION DE LA CLE DE LICENCE

Afin d'ajouter une clé de licence, cliquez sur **Parcourir** pour indiquer le chemin d'accès au fichier de clé. Pour que la nouvelle clé soit considérée comme une clé de réserve, cochez la case **Ajouter en tant que clé de réserve**. La clé de licence de réserve prendra la place de la clé actuelle dès que cette dernière sera arrivée à échéance.

Les informations relatives à la clé ajoutée (numéro de licence, type de licence et durée de validité) sont reprises dans le champ inférieur.

Etape 4. Configuration du lancement d'une tâche au nom d'un autre compte

Cette étape vous permet de configurer le lancement de la tâche au nom d'un autre compte jouissant de privilèges d'accès suffisant à l'objet à analyser ou à la source de la mise à jour (pour de plus amples informations, consultez le point 6.4 à la page 56).

Etape 5. Programmation de la tâche

Une fois que vous aurez configuré la tâche, vous aurez la possibilité de programmer son lancement automatique.

Pour ce faire, sélectionnez la fréquence de lancement dans le menu déroulant et précisez les paramètres de la programmation dans la partie inférieure.

Etape 6. Fin de la création d'une tâche

La dernière fenêtre de l'Assistant vous informe de la réussite de la création de la tâche.

13.2.2.2. Création d'une tâche de groupe

Afin de créer une tâche de groupe pour Kaspersky Anti-Virus 6.0 SOS, procédez comme suit :

1. Sélectionnez le groupe pour lequel vous souhaitez créer la tâche dans l'arborescence de la console.
2. Sélectionnez le répertoire **Tâches de groupe** (cf. ill. Illustration 41) qui en fait partie, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Actions**. Cette action entraîne l'ouverture de l'Assistant de création de tâches semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 13.2.2.1 à la page 151). Suivez les instructions affichées.

Une fois que vous aurez quitté l'Assistant, la tâche sera ajoutée au dossier **Tâches de groupe** du groupe correspondant et de tous les groupes repris dans ce groupe et reprise dans le panneau des résultats.

13.2.2.3. Création d'une tâche globale

Afin de créer une tâche globale pour Kaspersky Anti-Virus 6.0 SOS, procédez comme suit :

1. Sélectionnez le nœud **Tâches globales** (cf. ill. Illustration 41) dans l'arborescence, affichez le menu contextuel et sélectionnez le point **Créer→Tâche** ou choisissez l'élément équivalent du menu **Actions**.
2. Cette action entraîne l'ouverture de l'Assistant de création de tâches semblable à celui utilisé pour la création d'une tâche locale (pour de plus amples informations, consultez le point 13.2.2.1 à la page 151). La seule différence se situe au niveau de l'existence d'une étape permettant de dresser la liste des ordinateurs clients du réseau logique pour lesquels vous créez la tâche globale.
3. Sélectionnez les ordinateurs du réseau logique sur lesquels la tâche sera exécutée. Vous pouvez sélectionner des ordinateurs issus de différents dossiers ou sélectionner directement le dossier entier (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit 6.0).

Les tâches globales sont exécutées uniquement sur le groupe d'ordinateurs sélectionnés. La tâche d'installation à distance définie pour les ordinateurs d'un groupe ne sera pas appliquée aux nouveaux ordinateurs clients qui seraient ajoutés à ce groupe. Il faudra donc créer une nouvelle tâche ou modifier comme il se doit les paramètres de la tâche existante.

A la fin de la création de la tâche, la nouvelle tâche globale sera reprise dans le nœud **Tâches globales** de l'arborescence de la console et apparaîtra dans le panneau des résultats.

13.2.3. Configuration des tâches

Afin de consulter ou de modifier les paramètres des tâches de l'ordinateur client :

1. Ouvrez la fenêtre des propriétés de l'ordinateur client à l'onglet **Tâches** (cf. ill. Illustration 45).
2. Sélectionnez la tâche dans la liste puis cliquez sur **Propriétés**. La boîte de dialogue de configuration des tâches s'affichera (cf. ill. Illustration 46).

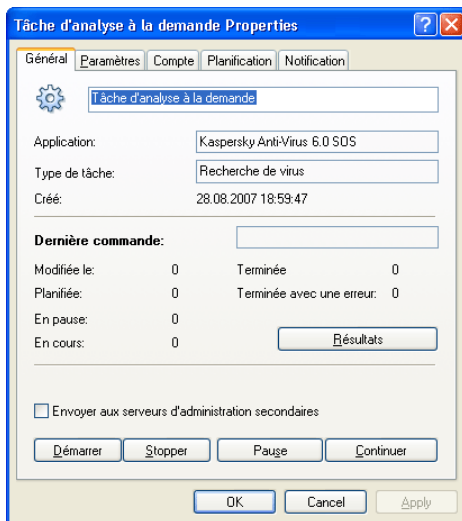


Illustration 46. Configuration des tâches

Ces onglets (à l'exception de l'onglet **Paramètres**) sont des onglets standard pour Kaspersky Administration Kit 6.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit. L'onglet **Paramètres** contient les paramètres propres à Kaspersky Anti-Virus 6.0 SOS. Le contenu de cet onglet varie en fonction du type de tâche sélectionnée.

La configuration des tâches de l'application via Kaspersky Administration Kit est identique à la configuration via l'interface locale de Kaspersky Anti-Virus 6.0 SOS. La seule différence réside au niveau des paramètres définis individuellement pour chaque utilisateur tel que l'horaire d'exécution des tâches. Pour obtenir de plus amples informations sur la configuration des tâches, consultez les points Chapitre 7 - Chapitre 9 aux pages 62 - 120 de ce manuel.

Si une stratégie interdisant la modification de certains paramètres a été créée (cf. point 13.3, p. 155), la modification de la configuration de la tâche sera impossible.

13.3. Administration des stratégies



La définition de stratégie est un moyen permettant d'appliquer une configuration des tâches et de l'application identique à tous les ordinateurs client faisant partie d'un groupe du réseau logique.

Cette rubrique est consacrée à la création et à la configuration de politiques pour Kaspersky Anti-Virus 6.0 SOS. Pour obtenir de plus amples informations sur l'administration des stratégies via Kaspersky Administration Kit 6.0, veuillez consulter le manuel de l'administrateur de ce logiciel.

13.3.1. Création d'une stratégie

Afin de créer une stratégie pour Kaspersky Anti-Virus 6.0 SOS, procédez comme suit :

1. Dans le dossier **Groupes** (cf. ill. Illustration 41) de l'arborescence de la console, sélectionnez le groupe d'ordinateur pour lequel vous souhaitez créer la stratégie.
2. Sélectionnez le dossier **Stratégies** appartenant au groupe sélectionné, ouvrez le menu contextuel et cliquez sur **Créer** → **Stratégie**.
L'interface du programme de création des stratégies se présente sous la forme d'un Assistant Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Préc.** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Lors de la configuration des stratégies, vous pouvez décider de bloquer totalement ou partiellement la modification de ses paramètres dans les stratégies des groupes intégrés, dans les tâches et les applications. Il suffit simplement de cliquer sur . Pour les paramètres qui ne peuvent pas être modifiés, l'icône doit ressembler à .

Etape 1. Saisie des données générales sur la stratégie

Les premières fenêtres de l'Assistant sont des fenêtres d'introduction. Il faut à ce stade définir le nom de la stratégie (champ **Nom**) et sélectionner l'application **Kaspersky Anti-Virus 6.0 SOS** dans la liste déroulante **Nom de l'application**.

Etape 2. Sélection de l'état de la stratégie

Cette fenêtre vous permet de définir le statut de la stratégie à l'aide des cases adéquates : stratégie active ou stratégie inactive.

Plusieurs stratégies peuvent être créées dans le groupe pour une application mais il ne peut y avoir qu'une seule politique active.

Etape 3. Sélection et configuration de l'application

Cette étape vous permet d'activer ou de désactiver l'application et définir ses paramètres dans la stratégie.

L'application est activée par défaut. Pour désactiver l'application, désélectionnez la case **Protection**. Si vous souhaitez procéder à une configuration détaillée de l'application, sélectionnez **Protection** et cliquez sur **Configuration**.

Etape 4. Configuration des paramètres de la recherche de virus

Cette étape correspond à la configuration des paramètres utilisés par les tâches de recherche de virus.

Sélectionnez, dans le bloc **Niveau de protection** un des trois niveaux proposés (cf. point 7.4.1, p. 67). Pour procéder à une configuration détaillée du niveau sélectionné, cliquez sur **Configuration**. Afin de restaurer les paramètres du niveau **Recommandé**, cliquez sur **Par défaut**.

Dans le groupe **Action**, indiquez l'action qui sera exécutée par Kaspersky Anti-Virus lors de la découverte d'un objet dangereux (cf. point 7.4.4, p. 71).

Etape 5. Configuration de la mise à jour

Cette étape correspond à la configuration de la mise à jour de Kaspersky Anti-Virus 6.0 SOS.

Dans le bloc **Paramètres de la mise à jour**, indiquez l'élément à actualiser (cf. point 9.4.2, p. 88). Dans la fenêtre qui s'ouvre après avoir cliqué sur **Configuration**, définissez les paramètres de l'intranet (cf. point 9.4.3, p. 90) et désignez la source de la mise à jour (cf. 9.4.1, p. 85).

Dans le groupe **Actions après la mise à jour**, activez ou désactivez l'analyse de la quarantaine après la réception de la dernière mise à jour (cf. 9.4.4, p. 92).


Etape 6. Application des stratégies

Cette étape vous permet de sélectionner le mode de diffusion des stratégies sur les ordinateurs client du groupe (pour de plus amples informations, consultez le manuel de l'administrateur de Kaspersky Administration Kit).

Etape 7. Fin de la création d'une stratégie

La dernière fenêtre de l'Assistant vous informe sur la réussite de la création de la stratégie.

Lorsque vous quittez l'Assistant de création de stratégie pour l'application sélectionnée, le dossier **Stratégies** (cf. ill. Illustration 41) sera ajouté au groupe correspondant et repris dans le panneau des résultats.

Vous pouvez modifier les paramètres de la stratégie créée et limiter la possibilité de modification des paramètres à l'aide du bouton  pour chaque groupe de paramètres. L'utilisateur sur l'ordinateur client ne pourra pas modifier les paramètres marqués de cette manière. La stratégie sera diffusée sur les ordinateurs client lors de la première synchronisation des clients avec le serveur.

Vous pouvez copier et déplacer les stratégies d'un groupe à l'autre, les supprimer à l'aide des commandes standard **Copier/Coller**, **Couper/Coller** et **Supprimer** ou des éléments similaires du menu **Actions**.

13.3.2. Consultation et modification des paramètres de la stratégie

A cette étape, vous pouvez introduire des modifications dans la stratégie, interdire la modification de certains paramètres des stratégies des sous-groupes, de l'application et des tâches.

Afin de consulter et de modifier les paramètres d'une stratégie :

1. Dans le dossier **Groupes** de l'arborescence de la console, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez modifier les paramètres de la stratégie.
2. Sélectionnez le dossier **Stratégies** faisant partie de ce groupe (cf. ill. Illustration 41). Toutes les stratégies définies pour ce groupe seront reprises dans le panneau des résultats.
3. Sélectionnez dans la liste la stratégie pour l'application **Kaspersky Anti-Virus 6.0 SOS** (le nom de l'application est indiqué dans le champ **Application**).
4. Sélectionnez l'élément **Propriétés** dans le menu contextuel de la stratégie sélectionnée. Cette action entraîne l'ouverture de la fenêtre de configuration de la stratégie pour Kaspersky Anti-Virus 6.0 SOS (cf. ill. Illustration 47).

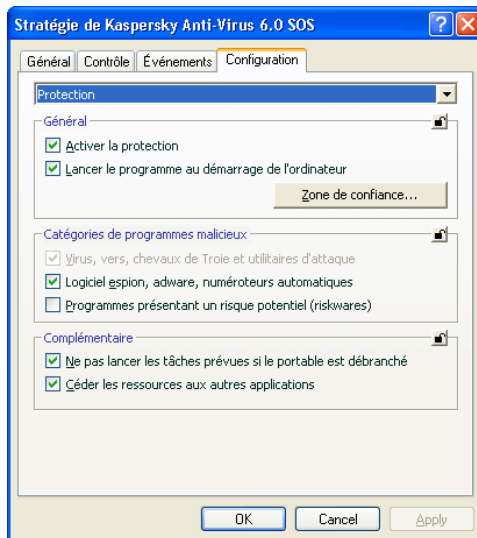


Illustration 47. Configuration de la stratégie

Ces onglets (à l'exception de l'onglet **Paramètres**) sont des onglets standard pour Kaspersky Administration Kit 6.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit.

L'onglet **Configuration** reprend les paramètres de la stratégie pour Kaspersky Anti-Virus 6.0 SOS. Les paramètres de la stratégie reprennent les paramètres de l'application (cf. point 13.1.2, p. 146) et les paramètres des tâches (cf. point 13.2.3, p. 154).

Pour configurer les paramètres, il suffit de sélectionner la valeur souhaitée dans la liste déroulante de la partie supérieure.

CHAPITRE 14. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquentes des utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Internet Security. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : *Kaspersky Anti-Virus 6.0 SOS peut-il être utilisé simultanément avec les logiciels d'autres éditeurs ?*

Oui, tout à fait. Kaspersky Anti-Virus 6.0 SOS ne génère aucun conflit avec les logiciels antivirus d'autres éditeurs.

Question : *Kaspersky Anti-Virus 6.0 SOS n'analyse pas le fichier une deuxième fois. Pourquoi ?*

En effet, Kaspersky Anti-Virus 6.0 SOS ne procédera pas à une nouvelle analyse d'un fichier si ce dernier n'a pas été modifié depuis la dernière analyse.

Et cela, grâce à la nouvelle iChecker. Ces technologies reposent sur l'utilisation d'une base de données des sommes de contrôle des objets.

Question : *a quoi sert le fichier de clé? Kaspersky Anti-Virus 6.0 fonctionnera-t-il sans elle ?*

Kaspersky Anti-Virus 6.0 SOS peut fonctionner sans clé, 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 6.0 SOS, 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 Internet Security, 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 6.0 SOS 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 6.0 SOS.
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 6.0 SOS.
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 6.0 SOS et elle définit également les paramètres du fichier setup.ini, utilisé lors de l'installation de l'application en mode caché

A.1. Liste des objets analysés en fonction de l'extension

Si vous avez coché la case  **Analyser les programmes et les documents (selon l'extension)**, Antivirus Fichiers ou la tâche de recherche de virus réalisera une analyse minutieuse des fichiers portant l'extension suivante. Ces fichiers seront également analysés par l'Antivirus Courrier si vous avez activé le filtrage 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 Microsoft Windows Script Host.
wsf : script Microsoft Windows.
hlp : fichier d'aide au format Win Help.
eml : message électronique de Microsoft Outlook Express.
nws : nouveau message électronique de Microsoft Outlook Express.
msg : message électronique de Microsoft Mail.
plg : message électronique
mbx : extension des messages Microsoft Office Outlook sauvegardés.
*doc** : document Microsoft Office Word, par exemple: *doc* – document Microsoft Office Word, *docx* – document Microsoft Office Word 2007 compatible avec XML, *docm* – document Microsoft Office Word 2007 compatible avec les macros.
*dot** : modèle de document Microsoft Office Word, например, *dot* – modèle de document Microsoft Office Word, *dotx* – modèle de document Microsoft Office Word 2007, *dotm* – modèle de document Microsoft Office Word 2007 compatible avec les macros.
fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro.
rtf : document au format Rich Text Format.
shs : fragment de Shell Scrap Object Handler.
dwg : base de données de dessins AutoCAD.
msi : paquet Microsoft Windows Installer.
otm : projet VBA pour Microsoft Office Outlook.
pdf : document Adobe Acrobat.
swf : objet d'un paquet Shockwave Flash.
jpg, jpeg, png : fichier graphique de conservation de données compressées.

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows. Les fichiers EMS ne sont pas pris en charge par Microsoft Windows 16 bit.

ico : fichier d'icône de l'objet

ov? : fichiers exécutable MS DOC

*xl** : documents et fichiers de Microsoft Office Excel tels que : *xla*, extension Microsoft Excel ; *xlc*, schéma ; *xlt*, modèle de document, *xlsx* – feuille de calcul Microsoft Office Excel 2007, *xlsm* – feuille de calcul Microsoft Office Excel 2007 compatible avec les macros, *xlsb* – feuille de calcul Microsoft Office Excel 2007 au format binaire (non xml), *xltm* – modèle Microsoft Office Excel 2007, *xlsm* – modèle Microsoft Office Excel 2007 compatible avec les macros, *xlam* – modèle externe Microsoft Office Excel 2007 compatible avec les macros.

*pp** : documents et fichiers de Microsoft Office PowerPoint tels que : *pps*, dia Microsoft Office PowerPoint ; *ppt*, présentation, *pptx* – présentation Microsoft Office PowerPoint 2007, *pptm* – présentation Microsoft Office PowerPoint 2007 compatible avec les macros, *potx* – modèle de présentation Microsoft Office PowerPoint 2007, *potm* – modèle de présentation Microsoft Office PowerPoint 2007 compatible avec les macros, *ppsx* – diaporama Microsoft Office PowerPoint 2007, *ppsm* – diaporama Microsoft Office PowerPoint 2007 compatible avec les macros, *ppam* – module externe Microsoft Office PowerPoint 2007 compatible avec les macros.

*md** : documents et fichiers de Microsoft Office Access tels que : *mda*, groupe de travail de Microsoft Office Access ; *mdb*, base de données, etc.

sldx : diaporama Office PowerPoint 2007.

sldm : diaporama Office PowerPoint 2007 compatible avec les macros.

thmx : thème Microsoft Office 2007.

N'oubliez pas que le format du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

A.2. Masques autorisés pour l'exclusion de fichiers

Voici des exemples de masques que vous utilisez lors de la constitution de la liste d'exclusions des fichiers :

- Masques sans chemin vers les fichiers :
 - ***.exe** : tous les fichiers *.exe

- ***.exe?** tous les fichiers *.ex? où " ? " représente n'importe quel caractère
- **test** : tous les fichiers portant le nom *test*
- Masque avec chemin d'accès absolu aux fichiers :
 - **C:\dir\.*** ou **C:\dir* C:\dir** : tous les fichiers du répertoire *C:\dir*
 - **C:\dir*.exe** : tous les fichiers *.exe du répertoire *C:\dir*
 - **C:\dir*.ex?** tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère unique
 - **C:\dir\test** : uniquement le fichier *C:\dir\test*

Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case **Sous-répertoires compris**.

- Masque avec chemin d'accès relatifs aux fichiers :
 - **dir\.*** ou **dir*** ou **dir** : tous les fichiers dans tous les répertoires *dir*
 - **dir\test** : tous les fichiers *test* dans les répertoires *dir*
 - **dir*.exe** : tous les fichiers *.exe dans tous les répertoires *dir*
 - **dir*.ex?** tous les fichiers *.ex? dans tous les répertoires *dir* où " ? " peut représenter n'importe quel caractère unique

Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case **Sous-répertoires compris**.

Conseil.

L'utilisation du masque *.* ou * est autorisée uniquement lorsque le verdict de la menace à exclure est indiqué. Dans ce cas, la menace indiquée ne sera pas identifiée dans les objets. L'utilisation de ces menaces sans indication du verdict 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 conséquent, l'analyse.

A.3. Masques d'exclusion autorisés en fonction du verdict

Pour ajouter des menaces d'un verdict particulier (conforme au classement 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 .

A.4. Description des paramètres du fichier *setup.ini*

Le fichier *setup.ini* situé dans le répertoire de fichier d'installation de Kaspersky Anti-Virus intervient lors de l'installation de l'application en mode caché via la ligne de commande (cf. point 3.3 à la page 35) ou via l'éditeur d'objet de stratégie de groupe (cf. point 3.4, p. 35). Il contient les paramètres suivants :

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

InstallDir=<chemin d'accès au répertoire d'installation de l'application >.

Reboot=yes|no – détermine s'il faut redémarrer ou non l'ordinateur à la fin de l'installation de l'application (le redémarrage n'a pas lieu par défaut).

[Tasks] : activation des tâches de Kaspersky Anti-Virus. Si aucune tâche n'est sélectionnée, toutes les tâches seront activées après l'installation. Si une tâche est activée, les autres tâches ne le seront pas.

ScanMyComputer=yes|no : tâche d'analyse complète de l'ordinateur.

ScanStartup=yes|no : tâche d'analyse des objets de démarrage.

ScanCritical=yes|no : tâche d'analyse des secteurs critiques.

Updater=yes|no : tâche de mise à jour des signatures de menace et des modules de l'application.

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

ANNEXE B. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automatisation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nos bases sont actualisées toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la "météo" des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d'informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de :

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers.** Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive.** Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.

- **Le contrôle des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique.** Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.
- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers** : n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles

est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont :

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel** : tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;

- **Protection contre les sms et mms indésirables .**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;

- *Génération de rapports détaillés ;*
- *Mise à jour automatique des bases de l'application.*

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable. ;*
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*

- *Analyse du courrier électronique et du trafic Internet en temps réel ;*
- *Blocage des fenêtres pop up et des bannières publicitaires pendant la navigation sur Internet ;*
- *Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;*
- *Outils de création d'un disque de démarrage capable de restaurer le système après une attaque de virus ;*
- *Système développé de rapports sur l'état de la protection ;*
- *Mise à jour automatique des bases ;*
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits ;*
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables (technologie Intel® Centrino® Duo pour ordinateurs portables) ;*
- *Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™).*

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet ;*
- *Utilisation de la technologie iSwift pour éviter les analyses répétées dans le cadre du réseau ;*
- *Répartition de la charge entre les processeurs du serveur ;*
- *Isolement des objets suspects du poste de travail dans un répertoire spécial ;*
- *Annulation des modifications malveillantes dans le système ;*

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus* contre les programmes malveillants ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases.*

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs* contre les virus, les chevaux de Troie et les vers ;
- *Protection des serveurs de messagerie* Sendmail, Qmail, Postfix et Exim ;
- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Prévention des épidémies de virus et des diffusions massives* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Utilisation sécurisée des réseaux sans fil* Wi-Fi ;
- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes dans le système* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;
- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Utilisation de la technologie iSwift* pour éviter les analyses répétées dans le cadre du réseau ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™) ;
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino,

Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Filtrage des messages non sollicités ;*
- *Analyse des messages et des pièces jointes du courrier entrant et sortant ;*
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange y compris les dossiers partagés ;*
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino ;*
- *Filtrage des messages en fonction du type de pièce jointe ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration du logiciel ;*
- *Prévention des épidémies de virus ;*
- *Surveillance de l'état du système de protection à l'aide de notifications ;*
- *Système de rapports sur l'activité de l'application ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Mise à jour automatique des bases.*

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.

- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Analyse du trafic Internet (HTTP/FTP) en temps réel ;*
- *Filtrage du trafic Internet selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration ;*
- *Système de rapports sur le fonctionnement de l'application ;*
- *Compatibilité avec les serveurs proxy matériels ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Mise à jour automatique des bases.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

B.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") Kaspersky Anti-Virus Second Opinion Solution CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI LE LOGICIEL N'ETAIT PAS DANS SON EMBALLAGE PUISQU'AYANT ETE ACQUIS EN FORMAT ELECTRONIQUE, 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 LE LOGICIEL A ETE ACQUIS AVEC SON MEDIA PHYSIQUE FOURNI DANS SON EMBALLAGE D'ORIGINE, EN OUVRANT LE PAQUET 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*.

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.

Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé pour protéger un réseau et sur plus d'un ordinateur. Ce logiciel est une application anti-virus complémentaire qui ne fournit pas de protection en temps réel. Ce logiciel n'est pas prévu pour être utilisé comme l'unique protection anti-virale d'un ordinateur.

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.

Le logiciel protège l'ordinateur contre les virus dont les signatures sont contenues dans les bases anti-virales disponibles sur les serveurs de mises à jour de Kaspersky Lab.

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.

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.

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.

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.

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.

Assistance technique.

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

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.

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.

Limites de Garantie.

- (i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.
- (ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.
- (iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.
- (iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.
- (v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.
- (vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions,

garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

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.

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 utiliser 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 dès son installation. La période est visible dans l'interface graphique windows du logiciel.