KASPERSKY LAB

Kaspersky Anti-Virus® 5.0 for Windows Workstations

Manuel de l'administrateur

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

Manuel de l'administrateur

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

http://www.kaspersky.fr/

Date d'édition: juillet 2006

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (ci-après Kaspersky Anti-Virus également) vise à protéger les postes de travail contre les virus et les programmes malveillants qui nuisent au fonctionnement normal des logiciels et aux données sauvegardées dans le système de fichiers des ordinateurs.

Le logiciel offre les fonctions suivantes :

- **Protection contre les virus et les programmes malveillants** : identification et élimination des programmes malveillants sur votre ordinateur. Le logiciel peut fonctionner dans l'un des deux modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :
    - **La protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
    - **L'analyse à la demande** permet de rechercher la présence éventuelle de virus sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut être lancée manuellement ou automatiquement selon un horaire défini.
- **Restauration des capacités opérationnelles après une attaque de virus**. Les fonctions d'analyse et de réparation selon les critères recommandés par les experts de Kaspersky Lab vous permettent de découvrir l'ensemble des virus qui ont infecté vos données.
- **Analyse et réparation du courrier entrant et sortant.** Le courrier entrant et sortant est analysé et les réparations nécessaires sont effectuées en temps réel[1]. De plus, il est possible de procéder à l'analyse

[1] L'analyse porte sur tout le courrier reçu et envoyé via Microsoft Office Outlook quels que soient les protocoles utilisés, de même que sur tout le courrier reçu et envoyé par n'importe quel client de messagerie compatible avec les protocoles SMTP et POP3.

à la demande[2] des bases de messagerie électronique des clients de messagerie et de réaliser les réparations qui s'imposent.

- **Protection de l'ordinateur contre les attaques de réseau** : analyse de toutes les données transmises via le réseau (local ou Internet) afin de déceler des attaques de réseau. Si une attaque est identifiée, elle est repoussée et l'ordinateur attaquant est bloqué. Le programme prend également en charge le mode furtif dans le cadre duquel l'ordinateur accepte uniquement les données des connexions lancées par l'utilisateur.

- **Mise à jour des bases antivirus, des bases d'attaque de réseau et des modules de l'application** : enrichissement des bases antivirus et des bases d'attaques de réseau avec les informations relatives aux nouveaux virus et aux attaques. Elle contiennent également les moyens de réparer les objets infectés et les mises à jour des modules de l'application (pour autant que cette option n'ait pas été désactivée). Les mises à jour sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab sélectionnés par l'utilisateur ou installées depuis un répertoire local ou de réseau

- **Présentation de recommandations sur la configuration du logiciel et sur son utilisation** : les conseils des experts de Kaspersky Lab et les recommandations relatives aux configurations qui correspondent à la protection optimale sont présents à toutes les étapes de l'utilisation de Kaspersky Anti-Virus.

  La fenêtre principale de Kaspersky Anti-Virus® affiche des recommandations sur l'exécution de telle ou telle tâche et sur les raisons qui les justifient en cas de découverte d'objets dangereux, lorsque le contenu des bases antivirus est fortement dépassé ou lorsqu'il est grand temps de réaliser l'analyse complète de l'ordinateur.

  Nous nous sommes efforcés de configurer ce logiciel de la meilleure manière possible en intégrant notre riche expérience dans la lutte contre les virus et en tenant compte des nombreux commentaires d'utilisateurs envoyés au Service d'assistance technique. Les paramètres de protection antivirus recommandés par nos experts sont appliqués dès l'installation et le lancement du logiciel.

- **Utilisation de divers profils de configuration** : création et exploitation de fichiers de configuration spéciaux, *les profils*, où sont enregistrés les

[2] Kaspersky Anti-Virus peut procéder à l'analyse antivirus des bases de messagerie électronique de n'importe quel client mais ne peut réparer que les bases de Microsoft Office Outlook et Microsoft Outlook Express.

paramètres du logiciel. Grâce à la définition des paramètres et à leur enregistrement dans les profils, vous pouvez modifier facilement la configuration de Kaspersky Anti-Virus. Vous pouvez par exemple configurer le logiciel pour qu'il fonctionne uniquement en protection en temps réel, pour qu'il exécute les tâches liées à l'analyse à la demande ou pour utiliser ces configurations uniquement lorsque cela est nécessaire. A tout moment, vous pourrez revenir aux paramètres recommandés.

- **Utilisation de deux modes de fonctionnement** : le logiciel peut être utilisé en mode *utilisateur* ou en mode *administrateur*. En mode utilisateur, seules les fonctions principales de Kaspersky Anti-Virus sont accessibles et il est impossible de configurer l'application ou de désactiver la protection antivirus. L'administration complète de l'application est possible en mode administrateur.
- **Placement des objets en quarantaine**. Il est possible de déplacer les objets potentiellement infectés par un virus ou l'une de ses variantes dans un répertoire particulier sécurisé. Vous pouvez ensuite réparer, supprimer ou restaurer le fichier incriminé dans son répertoire d'origine ou l'envoyer aux experts de Kaspersky Lab en vue d'un examen approfondi. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.
- **Création de copies de sauvegarde des objets** : création de copie de "réserve" des objets dans un dossier de sauvegarde spécial avant leur suppression ou leur réparation. Ces copies sont créées au cas où il serait nécessaire de restaurer l'objet original (s'il contenait des données importantes) ou afin de reproduire le scénario de l'infection. Les copies sont converties dans un format spécial et ne représentent aucun danger.
- **Création d'un rapport**. Tous les résultats de l'activité de Kaspersky® Anti-Virus sont consignés dans un rapport. Le rapport détaillé sur les résultats de l'analyse reprend des statistiques générales relatives aux objets analysés, la configuration en vigueur pour l'exécution de la tâche et préserve la chronologie de l'analyse et du traitement de chaque objet. Un rapport est également créé à la fin de la mise à jour et pour la protection en temps réel.
- **Administration centralisée de l'application** : administration à distance de l'application à l'aide du système d'administration centralisé Kaspersky Administration Kit 5.0.

Certaines fonctions de Kaspersky Anti-Virus sont accessibles via la ligne de commande (cf. Chapitre 9, p. 194).

1.1. Nouveautés de la version 5.0

Les éléments suivants distinguent la version 5.0 de Kaspersky Anti-Virus for Windows Workstations des versions 4.x :

- *Exploitation de technologies d'accélération de l'analyse antivirus : IChecker™ et iStreams™*. Kaspersky Anti-Virus ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une nette augmentation de la rapidité d'exécution de l'application.
- *Analyse et réparation du courrier* envoyé et reçu par n'importe quel client de messagerie via les protocoles SMTP et POP3. Dans la version antérieure, la protection du courrier était applicable uniquement à Microsoft Office Outlook.
- *Réparation des archives infectées*. Kaspersky Anti-Virus est capable de réparer les archives infectées au format *zip, arj, cab* et *rar*. La version antérieure du logiciel était capable uniquement d'identifier les fichiers infectés dans les archives et de réparer les objets infectés dans les archives zip.

  

  Kaspersky Anti-Virus analyse les archives multivolume aux formats indiqués ainsi que les archives auto-extractibles, mais il ne les répare pas.
- *Accélération de la mise à jour* grâce à la possibilité de choisir le serveur de mise à jour de Kaspersky Lab le plus proche géographiquement de l'utilisateur. Il est désormais possible de reprendre le téléchargement là où il a été interrompu en cas de déconnexion.
- *Protection contre les attaques de réseau*. Cette version de Kaspersky Anti-Virus protège votre ordinateur contre les attaques de réseau et les attaques de pirates informatiques les plus répandues à l'heure actuelle.
- *Interface simplifiée*. L'attribution de chacune des fonctions particulières de la protection antivirus à un module de programme distinct caractéristique de la version antérieure a été abandonnée au profit d'une application unifiée. Cette démarche se traduit par une simplification de l'utilisation et de l'administration des fonctions les plus critiques de Kaspersky Anti-Virus.
- *Compatibilité améliorée entre Kaspersky Anti-Virus et les logiciels antivirus d'autres éditeurs*. Pendant l'installation du programme, vous pouvez décider de ne pas utiliser la protection du système de fichiers, du

courrier, du réseau ou des scripts exécutés si cette protection est garantie par un autre logiciel déjà installé sur votre ordinateur.

- *Paramètres recommandés et conseils des experts*. Cette version du logiciel est distribuée avec un ensemble de paramètres d'analyse à la demande prédéfinis par les experts de Kaspersky Lab, ce qui simplifie l'utilisation. Dans la majorité des cas, il n'est pas nécessaire de configurer le logiciel avant de l'utiliser. En cas de sélection du niveau de protection le plus faible, le logiciel affiche le message adéquat et propose différentes options pour renforcer la protection.

- *Administration de l'utilisation du logiciel à l'aide de profils*. Il est désormais possible de conserver les paramètres du logiciel dans un fichier spécial en vue de les utiliser ultérieurement. Si la configuration recommandée de Kaspersky Anti-Virus ne vous convient pas, modifiez-la en fonction de vos besoins et enregistrez-la dans un *profil*.

- *Prolongation de la licence d'utilisation du logiciel*. Kaspersky Anti-Virus 5.0 vous permet d'activer les clés de licence afin de pouvoir utiliser le logiciel plus longtemps.

- *Envoi d'objets à Kaspersky Lab pour étude approfondie*. Il est désormais possible d'envoyer à Kaspersky Lab en vue d'un examen approfondi les objets potentiellement infectés découverts par Kaspersky® Anti-Virus ainsi que les objets que vous soupçonnez être infectés.

- *Interdiction de la suppression des bases de messagerie infectées*. Désormais, les bases de messagerie infectées ne sont plus supprimées à l'aide de Kaspersky Anti-Virus. Vous pouvez toutefois toujours les supprimer indépendamment.

- *Possibilité de créer une liste reprenant les processus de confiance*. L'activité de fichiers des processus de confiance n'est pas contrôlée par Kaspersky Anti-Virus en mode de protection en temps réel.

- *Protection de l'accès à l'administration des paramètres de Kaspersky Anti-Virus par mot de passe*. Vous pouvez définir le mot de passe qui sera requis pour passer du mode utilisateur au mode administrateur. En mode utilisateur, il est impossible de modifier les paramètres, de désactiver la protection ou de décharger Kaspersky Anti-Virus de la mémoire de l'ordinateur.

1.2. Configurations matérielle et logicielle requises

Afin de garantir le fonctionnement normal de Kaspersky Anti-Virus for Windows Workstations, il convient d'utiliser un matériel conforme aux configurations suivantes :

Configuration générale :

- 50 Mo disponibles sur le disque dur ;
- Lecteur de CD-ROM (pour l'installation de Kaspersky Anti-Virus au départ d'un CD) ;
- Microsoft Internet Explorer version 5.5 ou suivante (pour la mise à jour des bases antivirus et des modules du programme via Internet).

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

- Processeur Intel Pentium de 300 Mhz minimum ;
- 64 Mo de RAM.

Microsoft Windows 2000 Professional (Service Pack 2 ou suivant), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 ou suivant):

- Processeur Intel Pentium de 300 Mhz minimum ;
- 128 Mo de RAM.

1.3. Contenu du pack logiciel

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

Le pack logiciel en boite contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés; la clé de licence 365 jours est inclue et présente sur le CDROM, séparément ou incluse dans le fichier exécutable.
- Le manuel de l'utilisateur avec le contrat de licence utilisateur imprimé à la fin de ce manuel.

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

- le fichier d'installation contenant votre clé de licence d'un an,
- votre clé de licence un an seule (utile dans le cas où vous auriez déjà installé une version avec une clé d'essai),
- la version électronique de ce manuel (format Adobe PDF).

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

1.4. Services réservés aux utilisateurs enregistrés

Kaspersky Lab offre à ses utilisateurs légalement enregistrés une gamme élargie de prestations leur permettant d'augmenter l'efficacité d'utilisation du logiciel Kaspersky Anti-Virus.

Le service d'assistance technique ne répond ni aux questions portant sur le fonctionnement et l'utilisation des systèmes d'exploitation, ni à celles sur le fonctionnement des différentes technologies.

1.5. Notations conventionnelles

Le texte de la documentation se distingue par divers éléments de mise en forme en fonction de son affectation sémantique. Le tableau ci-après illustre les conventions typographiques utilisées dans ce manuel.

Mise en forme	Fonction sémantique
Caractères gras	Nom du menu, des options du menu, des fenêtres, des éléments des boîtes de dialogue, etc.
 Remarque.	Informations complémentaires.
 Attention !	Informations auxquelles il est recommandé d'accorder une attention particulière.

Mise en forme	Fonction sémantique
 *Pour exécuter une action,* 1. Etape 1. 2. …	Description de la succession des étapes que l'utilisateur doit suivre ou des actions possibles.
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du logiciel

CHAPITRE 2. INSTALLATION ET DESINSTALLATION DE L'APPLICATION

Il existe deux modes d'installation de Kaspersky Anti-Virus 5.0 for Windows Workstations : locale ou à distance (via le système d'administration centralisée de Kaspersky Administration Kit). Ce manuel traite de l'installation locale de Kaspersky Anti-Virus. Pour obtenir de plus amples informations sur l'installation à distance, consultez le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

2.1. Installation de l'application

Avant d'installer Kaspersky Anti-Virus sur l'ordinateur, il est conseillé de quitter toutes les applications ouvertes.

Afin d'installer l'application, lancez le fichier *setup.exe* repris dans la distribution .

L'installation réalisée au départ d'un fichier d'installation téléchargé depuis Internet est parfaitement identique à l'installation de l'application depuis le cédérom.

Le programme d'installation se compose d'une succession de boîtes de dialogue. 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.
- **Fermer** conclut l'installation du logiciel sur l'ordinateur.
- Vous trouverez ci-après une description détaillée, étape par étape, de l'installation de l'application.

Etape 1. Vérification de la version du système d'exploitation installé sur votre ordinateur

Avant de pouvoir lancer l'installation de Kaspersky Anti-Virus, le système doit vérifier la conformité du système d'exploitation ainsi que la présence des Services Packs requis.

Si l'une des exigences n'est pas remplie, le message de circonstance apparaît. Nous vous conseillons d'installer les versions et les services packs requis à l'aide de **Windows Update** (ou d'un autre moyen) avant de procéder à l'installation de Kaspersky Anti-Virus.

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

Dès l'exécution du fichier exécutable une fenêtre d'accueil reprenant les informations sur le lancement de l'installation de Kaspersky Anti-Virus apparaît.

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

Etape 3. Lecture du contrat de licence

La boîte de dialogue **Contrat de licence** contient le texte du contrat de licence. Lisez le texte du contrat de licence et si vous en acceptez les conditions, cliquez sur **J'accepte**. Si vous ne souhaitez pas installer le logiciel, cliquez sur **Annuler**.

Etape 4. Saisie des données concernant l'utilisateur

Saisissez dans la boîte de dialogue **Informations utilisateur** les données requises. Saisissez le nom dans le champ **Nom de l'utilisateur** et celui de la société dans le champ **Organisation**. Ces champs reprennent par défaut les données enregistrées dans la base du registre de Microsoft Windows.

Etape 5. Lecture des informations importantes relatives à l'application

Cette étape vous présente des informations importantes relatives au logiciel. Vous y trouverez une brève description des principales caractéristiques de Kaspersky Anti-Virus, les particularités de son fonctionnement, etc..

Pour passer à l'étape suivante de l'installation, cliquez sur **Suivant >**.

Etape 6. Utilisation des technologies de Kaspersky Lab

Cette étape de l'installation de Kaspersky Anti-Virus vous oblige à décider d'appliquer ou non les technologies suivantes développées par Kaspersky Lab :

Protection en temps réel du système de fichiers : analyse antivirus de tous les fichiers exécutés, ouverts et enregistrés sur l'ordinateur. La protection des fichiers est activée par défaut. Si vous ne souhaitez pas que Kaspersky Anti-Virus analyse les fichiers à chaque requête, désélectionnez la case **Utiliser la protection en temps réel du système de fichiers**.

Protection en temps réel du courrier : analyse antivirus des tous les messages envoyés ou reçus sur votre ordinateur, ainsi que des messages des bases de données de messagerie. La protection du courrier est activée par défaut. Si vous ne souhaitez pas que Kaspersky Anti-Virus analyse les messages, désélectionnez la case **Utiliser la protection en temps réel du courrier**.

Analyse des scripts exécutés : analyse antivirus de tous les scripts Java exécutés dans Microsoft Internet Explorer à l'ouverture de sites. L'analyse des scripts est activée par défaut. Si vous ne souhaitez pas utiliser Kaspersky Anti-Virus pour analyser les scripts, désélectionnez la case **Utiliser l'analyse des scripts**.

Analyse des macros : recherche de code malveillant dans toutes les macros VBA exécutées sur l'ordinateur. Cette analyse est activée par défaut. Pour désactiver l'analyse des macros, désélectionnez la case **Utiliser l'analyse des macros**.

Protection en temps réel du réseau est une technologie qui protège votre ordinateur contre les attaques des pirates informatiques. Cette technologie bloque les attaques qui ciblent votre ordinateur via le réseau et protège vos données contre le vol, l'accès non autorisé et la destruction. La protection en temps réel du réseau est desactivée par défaut. Pour appliquer cette protection, sélectionnez la case **Utiliser la protection en temps réel contre les attaques de réseau**.

La technologie iStreams™ accélère l'analyse antivirus des objets (pour de plus amples informations sur cette technologie, consultez l'Annexe B à la page 218). Pour désactiver cette technologie, désélectionnez la case **Utiliser la technologie iStreams™**.

Cette technologie est applicable uniquement aux partitions dotées d'un système de fichiers NTFS.

Si à cette étape vous avez décidé de ne pas utiliser ces technologies, vous devrez à nouveau installer le logiciel le jour où vous déciderez de les utiliser et sélectionner les technologies dont vous avez besoin.

Si pendant l'utilisation de Kaspersky Anti-Virus vous décidez de ne pas utiliser une forme quelconque de protection en temps réel ou la technologie iStreams™, vous devrez installer à nouveau l'application et désélectionner à cette étape les cases correspondantes.

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

Etape 7. Recherche d'autres logiciels antivirus éventuellement installés

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

Si une version antérieure de Kaspersky Anti-Virus est déjà installée (par exemple 4.5), la mise à jour de la version 4.x à la version 5 sera réalisée automatiquement (pour de plus amples informations, consultez le point 2.4 à la page 25).

Si la clé de licence pour Kaspersky Anti-Virus for Windows Workstations 4.x est découverte, la fenêtre d'installation de la clé de licence (cf. Etape 8, p. 20) reprendra les informations à son sujet. Pour utiliser l'application, vous pouvez utiliser cette clé de licence ou en choisir une autre.

En cas de découverte d'un logiciel antivirus développé par un autre éditeur, le programme d'installation vous suggèrera de le supprimer avant d'installer Kaspersky Anti-Virus.

Nous vous conseillons de supprimer ce programme. Pour ce faire, cliquez sur **Non** afin d'interrompre l'installation. Supprimez ensuite le logiciel indiqué et lancez à nouveau le fichier exécutable.

Les experts de Kaspersky Lab ne vous conseillent pas d'installer plusieurs logiciels antivirus sur l'ordinateur car cela peut entraîner des conflits.

Si le programme d'installation détecte que Kaspersky® Anti-Virus 5.0 for Windows Workstations est déjà installé, le message adéquat sera affiché. En choisissant de poursuivre l'installation, vous remplacerez la version déjà installée par la nouvelle.

Lors de la mise à jour à la version 5.0, la fenêtre d'installation de la clé de licence (cf. Etape 8 , p. 20) ne contiendra aucune information relative à la clé, mais la clé antérieure sera utilisée.

Etape 8. Activation de la clé de licence

Vous devez absolument choisir dans la boîte de dialogue **Clé de licence** la clé de licence que Kaspersky Anti-Virus utilisera pour vérifier la présence du contrat de licence et définir sa durée de validité.

Cette clé est votre clé personnelle qui reprend toutes les informations fonctionnelles indispensables au fonctionnement de Kaspersky Anti-Virus, à savoir :

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

Pour installer une nouvelle clé de licence :

1. Cliquez sur **Parcourir** et dans la fenêtre qui s'ouvre, sélectionnez le répertoire qui abrite le fichier de la clé de licence:
   - Si vous avez acheté Kaspersky Anti-Virus dans un magasin, la clé de licence se trouve sur la disquette. Vous devrez l'introduire dans le lecteur et y accéder.
   - Si vous avez acheté la licence en ligne, vous devrez enregistrer le fichier de clé de licence reçu par courrier électronique dans un répertoire du disque dur. Vous devrez ensuite indiquer le chemin d'accès à ce répertoire.

La liste des clés de licence disponibles apparaît à l'écran.

2. Sélectionnez la clé de licence nécessaire (fichier **.key**) et cliquez sur **Ouvrir**.

La fenêtre de l'Assistant d'installation reprendra les informations générales sur la licence et sur le chemin d'accès à celle-ci.

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

Si vous ne disposiez pas encore de la clé de licence au moment de l'installation du logiciel (ex. :vous l'avez commandée par Internet chez Kaspersky Lab mais ne l'avez pas encore reçue), sachez qu'il est possible de l'activer ultérieurement lorsque vous lancerez le programme pour la première fois ou à l'aide de l'utilitaire spécial d'installation de clé de licence (cf. Chapitre 8, p. 189). N'oubliez pas qu'il est impossible d'utiliser Kaspersky Anti-Virus sans cette clé.

Etape 9. Choix du répertoire d'installation

Dans la boîte de dialogue **Sélection du dossier d'installation**, indiquez le nom du dossier dans lequel Kaspersky Anti-Virus sera installé. Cliquez sur **Parcourir** pour sélectionner le répertoire.

A l'aide du bouton **Restaurer**, il est possible de restaurer le chemin d'accès au répertoire d'installation proposé par défaut : **<Disque>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 5.0 for Windows Workstations**.

Dans la fenêtre qui s'ouvre après que vous avez cliqué sur **Disque**, vous obtiendrez toutes les informations relatives à l'espace disque disponible et nécessaire sur les disques logiques du poste de travail pour l'installation.

Cliquez sur **Installer** pour poursuivre l'installation. Cette action lancera la copie des fichiers de Kaspersky Anti-Virus.

Etape 10. Fin de l'installation

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

En vue de conclure l'installation, il est indispensable d'enregistrer toute une série de services dans le système. Le programme d'installation vous proposera pour cette raison de redémarrer l'ordinateur. Cette étape est INDISPENSABLE pour terminer correctement l'installation du logiciel. Dans la fenêtre qui s'ouvre, cliquez sur **Oui** pour redémarrer l'ordinateur immédiatement ou sur **Non** si vous souhaitez le redémarrer plus tard.

Kaspersky Anti-Virus sera lancé automatiquement après le redémarrage de l'ordinateur.

Suite à l'installation de Kaspersky Anti-Virus :

- L'icône  du logiciel apparaît dans la barre des tâches.
- Les raccourcis du logiciel seront ajoutés au menu principal de Microsoft Windows (**Démarrer → Programmes → Kaspersky Anti-Virus 5.0 for Windows Workstations**).

2.2. Installation de l'application en mode silencieux

Kaspersky Anti-Virus 5.0 for Windows Workstations peut être installé via la ligne de commande. Pour ce faire, rendez-vous dans le répertoire où se trouve le fichier d'installation et exécutez la commande :

```
setup [/s] [/l<fichier_journal>]
[/p<propriété>="<valeur>"…]
```
[3]

Clé	Valeur
/s	Installation en mode silencieux.
/l<fichier_journal>	Consignation des événements dans le **fichier_journal** iniqué La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace..
/p<propriété>	Indication des paramètres d'installation de l'application. Les paramètres suivants sont admis : • **INSTALLDIR** : chemin d'accès complet au répertoire d'installation de l'application; • **USERNAME** : nom d'utilisateur; • **COMPANYNAME** : nom de l'organisation pour laquelle l'utilisateur travaille; • **KLKEY** : chemin d'accès complet à la clé de licence; • **KLUSEIDS** : réglementation de la protection contre les attaques de réseau. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est désactivée par défaut; • **KLUSEISTREAMS** : réglementation de l'utilisation de la technologie iStreams™. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est activée par défaut;

[3] Les valeurs entre crochets sont les clés non obligatoires.

Clé	Valeur
	• **KLUNINSTPASSWD** : mode de passe qu'il faudra saisir avant de pouvoir supprimer l'application; • **KLADMPASSWD** : mot de passe qu'il faudra saisir pour permuter entre le mode utilisateur et le mode administrateur; • **KLDELAYREBOOT** : détérmine s'il faudra redémarrer l'ordinateur après l'installation. Pour redémarrer, saisissez la valeur **"1"** ou **""** si vous ne souhaitez pas redémarrer. Le redémarrage est prévu par défaut; • **KLUSERTPFILE** : réglementation de l'utilisation de la protection en temps réel du système de fichiers. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est activée par défaut; • **KLUSERTPMAIL** : réglementation de la protection en temps réel du courrier. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est activée par défaut; • **KLUSERTPSCRIPT** : réglementation de l'analyse des scripts exécutés. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est activée par défaut; • **KLUSERTPMACRO** : réglementation de l'analyse des macros. Pour utiliser cette technologie, saisissez la valeur **"1"** ou **""** pour désactiver cette technologie. L'utilisation de cette technologie est activée par défaut.

Exemple :

```
setup /s /l"C:/Kaspersky Lab/Report"
/pINSTALLDIR="C:/Kaspersky Lab" /pKLADMPASSWD=password
```

Les paramètres de l'installation en mode silencieux peuvent également être définit dans la section **[Setup]** du fichier *.ini.

Le fichier des paramètres doit obligatoirement être appelé **setup.ini**.

Les paramètres suivants sont admis :

- **InstallDir** : chemin d'accès complet au répertoire d'installation de l'application;
- **User** : nom d'utilisateur;
- **Company** : nom de l'organisation pour laquelle l'utilisateur travaille;
- **Key** : chemin d'accès complet à la clé de licence;
- **IDS** : utilisation de la technologie de protection contre les attaques de réseau (valeurs: **enable** = activé, **disable** = désactivé);
- **IStreams** : utilisation de la technologie iStreams™ (valeurs: **enable** = activé, **disable** = désactivé);
- **UninstallPassword** : mot de passe qu'il faudra saisir avant de pouvoir supprimer l'application;
- **AdminPassword** : mot de passe pour permuter entre le mode utilisateur et le mode administrateur;
- **Reboot** : redémarrage de l'ordinateur après l'installation de l'application (valeurs : **yes** = activé, **no** = désactivé);
- **RTPFile** : utilisation de la technologie de protection en temps réel des fichiers (valeurs: **enable** = activé, **disable** = désactivé);
- **RTPMail** : utilisation de la technologie de protection en temps réel du courrier (valeurs: **enable** = activé, **disable** = désactivé);
- **RTPScript** : utilisation de la technologie d'analyse des scripts exécutés (valeurs: **enable** = activé, **disable** = désactivé);
- **RTPMacro** : utilisation de la technologie d'analye des macros (valeurs: **enable** = activé, **disable** = désactivé).

Exemples :

```
[Setup]
InstallDir=C:/Kaspersky Lab
Key=A:/License/00000001.key
User=Ivanov
```

```
IStreams=enable
```

2.3. Suppression de l'application

Si pour une raison quelconque, vous devez supprimer Kaspersky Anti-Virus, utilisez la commande **Démarrer→Programmes→Kaspersky Anti-Virus for Workstations→Kaspersky Anti-Virus for Workstation Uninstall** ou utiliser la fonction standard **Ajout/Suppression de programmes** dans Microsoft Windows.

Si dans le cadre de l'administration via Kaspersky Administration Kit vous avez défini un mot de passe pour empêcher la suppression non autorisée de l'application (cf. point 6.2.2.14, p. 161), vous devrez saisir ce mot de passe au début de la procédure de désinstallation.

Une demande de confirmation de la suppression apparaîtra à l'écran. Pour lancer la procédure de désinstallation, cliquez sur **OK**. Cette action entraîne l'ouverture d'une fenêtre vous permettant de supprimer ou de conserver les objets placés en quarantaine ou se trouvant dans le dossier de sauvegarde, ainsi que les fichiers des rapports.

Les fichiers du programme seront ainsi supprimés du disque dur de l'ordinateur.

Si le programme détecte, lors de la désinstallation, un fichier susceptible d'être utilisé par d'autres programmes, l'écran affichera une boîte de dialogue de confirmation de la suppression. Pour supprimer le fichier concerné, cliquez sur **Oui**.

La procédure de suppression de l'application se terminera par l'affichage d'une boîte de dialogue vous invitant à redémarrer le poste de travail. Sélectionnez l'option qui s'impose puis cliquez sur **Terminer**.

2.4. Mise à jour de la version 4.x à la version 5.0

Avant de procéder à la mise à jour de Kaspersky Anti-Virus, il est recommandé de traiter les objets qui se trouvent dans le dossier de quarantaine ou dans le dossier de sauvegarde.

Afin de procéder à la mise à niveau de la version 4.x de Kaspersky Anti-Virus for Windows Workstations à la version 5.0, lancez le fichier exécutable *setup.exe*. La version antérieure de Kaspersky Anti-Virus sera supprimée pendant l'installation.

Il faudra redémarrer le système d'exploitation à la fin de l'installation.

Veuillez noter que les paramètres de la version 4.x seront supprimés lors de la mise à niveau de Kaspersky Anti-Virus. Vous pouvez utiliser les paramètres recommandés définis par défaut ou reconfigurer l'application.

En cas d'administration à distance via Kaspersky Administration Kit (pour de plus amples informations, consultez le manuel de Kaspersky Administration Kit 5.0), la mise à jour de la version 4.x à la version 5.0 s'opère automatiquement : la version antérieure de Kaspersky Anti-Virus sera supprimée et l'ordinateur distant sera redémarré.

CHAPITRE 3. CONCEPT D'ADMINISTRATION DU PROGRAMME

Kaspersky Anti-Virus for Windows Workstations s'installe sur le poste de travail et peut être administré localement ou à distance grâce au programme Kaspersky Administration Kit (pour autant que l'ordinateur soit inclus dans le système d'administration centralisée à distance).

Il existe plusieurs catégories de personnes qui peuvent être amenées à utiliser Kaspersky Anti-Virus :

- *L'utilisateur du poste de travail*, c.-à-d. la personne dont l'ordinateur est équipé de Kaspersky Anti-Virus ;
- *L'administrateur de la sécurité antivirus* (ci-après, l'administrateur), c.-à-d. la personne chargée de l'administration locale de Kaspersky Anti-Virus ;
- *L'administrateur du réseau logique*, c.-à-d. la personne chargée de l'administration du fonctionnement de Kaspersky Anti-Virus via Kaspersky Administration Kit, le système d'administration centralisée.

En fonction de ses privilèges, chaque catégorie d'utilisateur disposera d'une interface spécifique proposant toutes les fonctions accessibles à son niveau d'utilisation.

L'**interface utilisateur** a été conçue en pensant à la productivité de l'utilisateur. Elle permet d'exécuter les tâches suivantes :

- Examen de l'état de la protection antivirus ;
- Lancement de l'analyse d'objets du système de fichiers ;
- Mise à jour des bases antivirus et des modules logiciels du programme (si cette option a été activée par l'administrateur) ;
- Consultation des informations relatives à l'état de la protection antivirus;
- Examen du résultat de l'exécution des tâches et du journal système ;
- Examen du contenu de la quarantaine et du dossier de sauvegarde ; envoi à Kaspersky Lab des fichiers mis en quarantaine en vue d'une étude plus approfondie.

L'**interface administrateur**, en plus des tâches utilisateur, permet la configuration flexible et aisée du fonctionnement de Kaspersky Anti-Virus. Elle permet de réaliser les tâches suivantes :

- Configuration des tâches liées à la protection en temps réel ;
- Création de tâches d'analyse d'objets du système de fichiers et de tâches de mise à jour ; gestion et programmation de celles-ci ;

Le programme d'administration centralisée Kaspersky Administration Kit permet l'administration à distance de l'ordinateur sur lequel la *console d'administration* a été installée.

Cette console se présente sous la forme d'une **interface** standard **intégrée au MMC**. Grâce à elle, l'administrateur du réseau logique peut exécuter les fonctions suivantes :

- Installation à distance de Kaspersky Anti-Virus sur les ordinateurs client ;
- Mise à jour des bases antivirus et des modules logiciels du programme ;
- Administration des stratégies et des tâches sur les ordinateurs client ;
- Activation des clés de licence sur les ordinateurs clients ;
- Examen des rapports d'activité du programme sur les ordinateurs clients.

Afin d'administrer l'application via Kaspersky Administration Kit, il est indispensable d'installer l'agent d'administration sur l'ordinateur client afin de garantir l'interaction entre le poste de travail et le serveur d'administration (pour de plus amples informations, consultez le Manuel de KASPERSKY ADMINISTRATION KIT 5.0).

Pour obtenir de plus amples informations sur le concept d'administration centralisée, consultez le Manuel de l'administrateur de « Kaspersky Administration Kit ».

3.1. Principes de base du concept d'administration

En cas d'administration locale de Kaspersky Anti-Virus, la protection est définie par l'administrateur via la configuration des tâches et de l'application.

Une **Tâche** est une action exécutée par Kaspersky Anti-Virus. Les tâches sont réparties en différents types selon leurs fonctions. On distingue ainsi la tâche d'analyse complète, la tâche de mise à jour des bases antivirus et des modules de l'application, etc.). A chaque tâche correspond un groupe de paramètres de

fonctionnement de Kaspersky Anti-Virus pendant l'exécution de la tâche. Il s'agit des *paramètres de la tâche*.

Paramètres de l'application : ensemble de paramètres de fonctionnement complémentaires comprenant les paramètres de la quarantaine, du dossier de sauvegarde, de réception des rapports, etc.

En cas d'administration centralisée via Kaspersky Administration Kit, l'administrateur détermine également la configuration des tâches et de l'application, mais uniquement pour les copies de Kaspersky Anti-Virus installée sur les ordinateurs distants du réseau.

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

La **stratégie** est un ensemble de paramètres de fonctionnement de l'application dans le groupe du réseau logique ainsi qu'un ensemble de restrictions sur la redéfinition des paramètres lors de la configuration de l'application et des tâches.

La stratégie intègre la configuration complète de toutes les fonctions de l'application. Elle reprend donc les paramètres de l'application et ceux de tous les types de tâches, à l'exception des paramètres qu'il faut définir directement au moment du lancement de la tâche.

3.2. Interface locale

L'interface de Kaspersky Anti-Virus est à la fois simple et conviviale. Ce chapitre est consacré à ses principaux éléments, à savoir : l'icône de la barre de tâches, le menu contextuel, la fenêtre principale et quelques boîtes de dialogue.

3.2.1. Icône de la barre des tâches

Dès que l'application a été lancée, une icône permettant de définir l'état de la protection antivirus apparaît dans la barre des tâches : protection en temps réel active ou analyse à la demande en cours d'exécution.

Si l'icône  est active (rouge), cela signifie que tous les fichiers de votre ordinateur sont placés sous le contrôle de Kaspersky Anti-Virus. Si l'icône  n'est pas activée (grise), cela signifie que la protection en temps réel est désactivée (vous avez par exemple suspendu celle-ci, vous l'avez désactivée ou vous avez décidé de ne pas l'utiliser au moment de l'installation).

Quand l'analyse complète de l'ordinateur, l'analyse d'un fichier ou d'un disque particulier ou l'analyse en temps réel d'un objet particulier est en cours

d'exécution, l'icône clignotante  apparaît dans la barre des tâches. Lors de l'analyse du courrier entrant, l'icône  apparaît. L'icône  , quant à elle, indique l'échec du lancement d'une des tâches de la protection en temps réel. L'icône prend cette forme  pendant le téléchargement de la mise à jour des bases antivirus, des bases d'attaques de réseau et des modules de l'application.

Si l'animation de l'icône a été désactivée dans les options avancées de Kaspersky Anti-Virus (cf. point 5.10.4, p. 120), l'icône prend seulement une seule valeur : active ou inactive.

Lorsqu'un événement important au niveau de la protection antivirus survient, un message reprenant les recommandations des experts de Kaspersky Lab apparaît pendant quelques instants au-dessus de l'icône (Cette fonction n'est pas disponible sous Microsoft Windows 98/NT).

3.2.2. Menu contextuel

Un clic-droit sur l'icône de l'application dans la barre des tâches vous permettra d'afficher un menu contextuel (cf. ill. 1) proposant les éléments suivants :

- **Ouvrir Kaspersky Anti-Virus** : ouvre la fenêtre principale du logiciel à l'onglet **Protection**. Vous pouvez également obtenir le même résultat en double-cliquant sur l'icône  du programme dans la barre des tâches.
- **Passer en mode utilisateur/Passer en mode administrateur** : permet de passer d'un mode de sécurité à l'autre.
- **Tâches lancées** : liste des tâches programmées en cours d'exécution. Ce point apparaît dans le menu contextuel lorsqu'une tâche quelconque est en cours d'exécution
- **Analyser mon Poste de travail** : lance l'analyse antivirus complète de l'ordinateur conformément au niveau de protection sélectionné.
- **Mettre à jour les bases antivirus** : procède à la mise à jour des bases antivirus.
- **Tâches exécutées** : liste des tâches exécutées selon l'horaire défini. Ce point apparaît dans le menu contextuel lorsqu'une tâche programmée quelconque est en cours d'exécution.
- **Rétablir la protection en temps réel / Arrêter la protection en temps réel :** active ou désactive la protection en temps réel de l'ordinateur. Ce point figure dans le menu uniquement si vous avez décidé d'utiliser la protection en temps réel contre les fichiers au moment de l'installation de Kaspersky Anti-Virus for Windows Workstations. Selon que la protection

en temps réel sera activée ou non, l'icône de l'application changera. Ce point est accessible uniquement aux administrateurs de Kaspersky Anti-Virus ; l'utilisateur conventionnel ne peut activer/désactiver la protection en temps réel de l'ordinateur.

Il est conseillé de ne pas suspendre la protection en temps réel car cela augmente considérablement le risque d'infection de l'ordinateur par des virus.

- **À propos du produit**: affiche la fenêtre de renseignements comportant les renseignements relatifs à Kaspersky Anti-Virus 5.0 for Windows Workstations.
- **Quitter** : décharge Kaspersky Anti-Virus de la mémoire de votre ordinateur. Ce point du menu contextuel est accessible uniquement à l'administrateur de Kaspersky Anti-Virus.

Illustration 1. Menu contextuel

3.2.3. Fenêtre principale du logiciel : structure générale

La fenêtre principale de Kaspersky Anti-Virus est l'élément qui permet d'exploiter toutes les possibilités de l'application en matière de protection antivirus de votre ordinateur. Vous pouvez notamment :

- Lancer et interrompre la recherche d'éventuels virus ou autres programmes malveillants sur l'ordinateur, sur les disques, dans des répertoires ou des fichiers ;
- Créer vos propres tâches d'analyse d'objets;
- Télécharger les mises à jour des bases antivirus, des bases d'attaques de réseau et des modules de l'application;
- Configurer la protection antivirus ;
- Travailler avec les objets en quarantaine ;

- Manipuler les copies des objets créées dans le dossier de sauvegarde avant leur réparation ou leur suppression;
- Utiliser les rapports;
- Administrer la configuration du programme.

Tous les paramètres de la protection antivirus, les informations indispensables et les tâches sont répartis entre les trois onglets suivants de la fenêtre principale :

- **Protection** : état et tâches spécifiques à la protection antivirus (analyse des objets et mise à jour des bases antivirus). Cet onglet vous donne également accès à la manipulation des objets en quarantaine, des objets dans le dossier de sauvegarde et des rapports. Il s'agit de l'onglet principal dans l'utilisation de l'application (cf. point 3.2.3.1, p. 32).
- **Paramètres** : état et tâches spécifiques à la configuration des principaux paramètres de la protection antivirus (cf. point 3.2.3.2, p. 34).
- **Assistance technique** : : onglet qui vous permet de consulter les informations relatives à la clé de licence, de renouveler la licence d'utilisation du logiciel, d'ouvrir des rubriques d'aide et d'envoyer des requêtes au service d'assistance technique (cf. point 3.2.3.3, p. 35)

Chacun de ces onglets est divisé en deux parties :

- *La partie gauche de l'onglet contient* des liens qui permettent d'exécuter les tâches obligatoires liées à l'utilisation de Kaspersky Anti-Virus. La composition de cette liste varie en fonction de l'onglet sélectionné. Ainsi, la liste des tâches de l'onglet **Protection** reprend toutes les tâches possibles liées à la recherche d'éventuels virus sur votre ordinateur tandis que celle de l'onglet **Paramètres** reprend les configurations de ces différentes tâches. L'onglet **Assistance technique** reprend les tâches liées à l'assistance au niveau de la protection antivirus.
- *La partie droite de l'onglet* reprend les informations relatives à l'état actuel de la protection antivirus de votre ordinateur (protection en temps réel, analyse complète et bases antivirus). Ainsi, dans l'onglet **Protection**, il s'agira de l'état de la protection antivirus tandis que dans l'onglet **Paramètres**, il s'agira de l'état des différentes configuration. Pour l'onglet **Assistance technique**, c'est l'état de la licence (informations relatives à la clé de licence), liens vers l'assistance technique et informations relatives au logiciel et au système d'exploitation.

3.2.3.1. Onglet *Protection*

C'est au départ de l'onglet **Protection** (cf. ill. 2) que vous lancerez les tâches d'analyse de votre ordinateur ou de disques, de répertoires ou de fichiers particuliers. Vous pouvez également :

- Lancer la mise à jour des bases antivirus, des bases d'attaques de réseau et des modules du programme ;
- Passer à la manipulation des rapports d'exécution de toutes les tâches lancées (consulter, supprimer, exporter vers un fichier);
- Passer à la manipulation des objets potentiellement infectés par un virus ou l'une de ses variantes préalablement mis en quarantaine.
- Passer à la manipulation des copies de sauvegarde des objets réparés ou supprimés.

Les tâches peuvent être lancées par l'intermédiaire des liens correspondants.

Illustration 2. Onglet **Protection**

La partie droite de l'onglet affiche *l'état actuel de la protection*, *de l'analyse complète* et *des bases antivirus*. L'illustration 2 représente le cas de figure où l'analyse en temps réel de l'ordinateur est suspendue mais où l'analyse complète est en cours. Des commentaires sur l'état de chacune des tâches de la protection antivirus sont également proposés.

Les recommandations des experts de Kaspersky Lab seront toujours reprises lorsque le niveau de la protection antivirus est jugé critique ou différent du niveau

recommandé. Pour accroître l'efficacité de la protection antivirus, vous aurez la possibilité de modifier la configuration actuelle, de rétablir la configuration recommandée par les experts de Kaspersky Lab, de lancer telle ou telle tâche, etc. Toutes ces suggestions apparaissent sous la forme d'un lien hypertexte qui vous conduira directement à l'action en question.

Si des objets infectés ou suspects ont été découverts pendant l'analyse, les informations correspondantes sont reprises dans la partie droite de la fenêtre. Par la suite, vous pourrez toujours passer au traitement des objets découverts à l'aide du lien traiter ces objets (pour de plus amples informations, consultez le point 5.4 à la page 92).

3.2.3.2. Onglet *Paramètres*

L'onglet **Paramètres** (cf. ill. 3) vous permet d'évaluer les configurations appliquées et de modifier les paramètres de base ou les options avancées qui régissent le fonctionnement de Kaspersky Anti-Virus.

La partie droite de l'onglet indique la configuration actuelle de la protection en temps réel, de l'analyse à la demande et de la mise à jour automatique des bases antivirus, des modules du programme et des bases des attaques de réseau connues. Ces informations sont accompagnées de commentaires détaillés et de conseils portant sur la modification de certains paramètres. Par exemple, si vous procédez manuellement à la mise à jour des bases antivirus, le logiciel vous proposera d'automatiser cette tâche et d'établir un horaire pour le lancement du téléchargement de la mise à jour.

Les liens repris dans la partie gauche vous permettent d'accéder directement aux fenêtres de configuration de la protection en temps réel, de l'analyse à la demande et des mises à jour. Vous pouvez également constituer des listes d'objets qui seront exclus de la protection et définir le type de base antivirus utilisé.

Illustration 3. Onglet **Paramètres**

Vous pouvez également configurer les paramètres de la quarantaine où sont placés les objets qui ont peut être été infectés par des virus ou leur modification et du dossier de sauvegarde prévu pour la conservation des copies de sauvegarde des objets. Le lien Options avancées ouvre la fenêtre de configuration des paramètres complémentaires de Kaspersky Anti-Virus.

Kaspersky Anti-Virus vous permet de créer diverses configurations et de les enregistrer dans des fichiers spéciaux, les *profils*. Par la suite vous pourrez revenir facilement à l'une ou l'autre configuration. En effet, il ne sera pas nécessaire de configurer à nouveau le logiciel mais de charger tout simplement le profil souhaité. Le lien Gestion des profils permet de créer et de charge des profils.

3.2.3.3. Onglet *Assistance technique*

L'onglet **Assistance technique** (cf. ill. 4) indique qui contacter en cas de problèmes de fonctionnement de Kaspersky Anti-Virus ou lorsque vous n'êtes pas en mesure de résoudre seul le problème auquel vous êtes confronté. Il affiche également toutes les informations sur le logiciel, la clé de licence et le

système d'exploitation installé sur votre ordinateur afin que toutes ces informations soient à votre portée en cas d'appel au Service d'assistance technique de Kaspersky Lab. Tous ces renseignements figurent dans la partie droite.

La partie gauche propose des liens qui vous permettent de :

- Contacter le Service d'assistance technique et d'envoyer pour examen à Kaspersky Lab des objets potentiellement infectés par un virus ou l'une de ses modifications.
- Renouveler la licence d'utilisation de Kaspersky Anti-Virus.

La partie gauche reprend également des liens vers des rubriques d'aide :

- Le lien Aide ouvre des fenêtres d'aide générale sur l'utilisation du logiciel.
- Le lien Encyclopédie des virus vous emmène sur le site www.viruslist.com qui contient une description détaillée de tous les programmes malicieux connus à ce jour.
- Le lien Site Web de Kaspersky Lab vous conduira sur le site Internet de Kaspersky Lab.

Illustration 4. Onglet Assistance technique

3.2.4. Fenêtre du processus d'analyse

La fenêtre du processus d'analyse (cf. ill. 5) apparaît dès le lancement de l'analyse complète de l'ordinateur ou de l'un de ses disques, fichiers ou répertoires.

La fenêtre est constituée de deux parties :

- La partie supérieure présente un indicateur qui illustre l'avancement (en pour cent) de l'analyse, le nom de l'objet analysé, l'heure estimée de fin de l'analyse et des statistiques générale sur le nombre d'objets analysés à ce moment, ainsi que sur le nombre d'objets réparés, supprimés et placés en quarantaine.

- Pour ouvrir la partie inférieure de la fenêtre, cliquez sur  . Elle abrite trois onglets : **Statistiques**, pour les résultats de l'analyse ; **Rapport** pour le rapport des événements survenus lors de l'analyse ; **Paramètres** pour une description de la configuration appliquée à cette analyse. Cliquez  sur pour refermer cette partie.

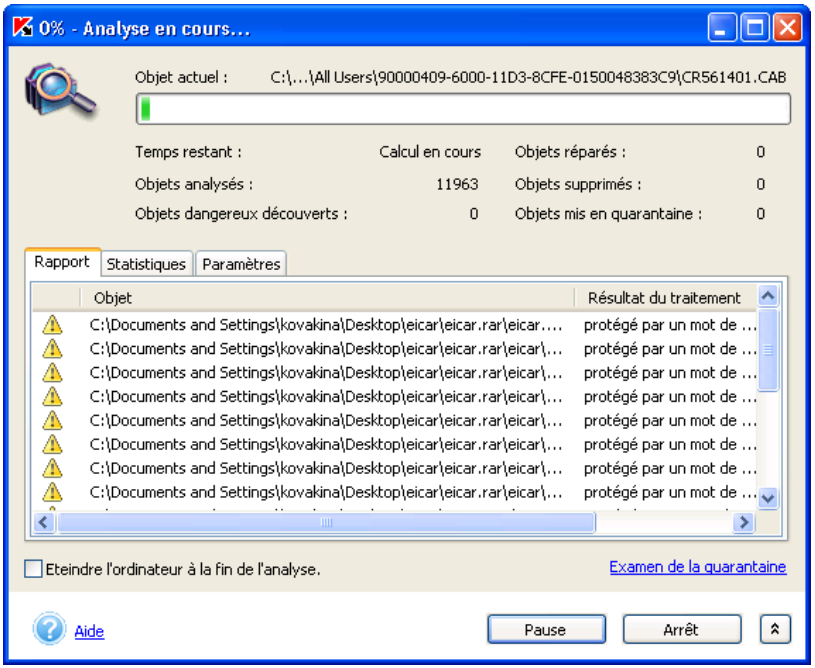

Illustration 5. Fenêtre du processus d'analyse

Le lien Examen de la Quarantaine vous conduira directement dans le répertoire de quarantaine (cf. point 5.10.1.2, p. 111).

Si vous réalisez l'analyse complète de l'ordinateur, cette fenêtre vous permettra d'activer l'arrêt de l'ordinateur à la fin de l'analyse. Ce mode est utile si vous avez l'habitude de lancer l'analyse à la fin de votre journée de travail et que vous ne souhaitez pas attendre que l'analyse soit terminée.

Ce mode requiert toutefois les préparatifs suivants : il faut, avant le lancement de l'analyse, désactiver, le cas échéant, la demande du mot de passe pendant l'analyse des objets (cf. point 5.3.3.1, p. 83), activer le traitement automatique des objets dangereux ainsi que leur suppression/placement dans le dossier de quarantaine ou la consignation des données dans le rapport (cf. point 5.3.3.2 , p. 86). Ces diverses actions entraînent la désactivation du mode interactif et l'analyse s'effectue sans interruption (aucune boîte de dialogue n'apparaîtra durant l'analyse).

Pour éteindre l'ordinateur à la fin de l'analyse, cochez la case Eteindre l'ordinateur à la fin de l'analyse.

3.2.5. Aide

Toutes les rubriques d'aide du logiciel sont accessibles via l'onglet **Assistance technique**. Il suffit de cliquer sur le lien Aide repris dans la colonne de gauche.

Si votre question porte sur une boîte de dialogue en particulier, enfoncez la touche **<F1>** ou cliquez sur le lien Aide dans le coin inférieur gauche de la boîte de dialogue en question.

CHAPITRE 4. PROTECTION DE L'ORDINATEUR SANS CONFIGURATION COMPLEMENTAIRE

La protection antivirus, appliquant les paramètres par défaut, est activée directement après l'installation du programme sur l'ordinateur. Ces paramètres ont été définis par les experts de Kaspersky Lab afin de garantir au maximum la sécurité de votre ordinateur.

En cas d'administration centralisée à l'aide de Kaspersky Administration Kit, les paramètres peuvent être définis par les stratégies et les tâches créées par l'administrateur de la sécurité. Pour ce faire, les paramètres en question doivent être "verrouillés" :  . Pour de plus amples informations, consultez l'aide de Kaspersky Administration Kit 5.0).

Il est possible également de modifier rapidement les paramètres en choisissant l'un des trois niveaux définis par les experts de Kaspersky Lab : *Sécurité maximale, Recommandé ou Vitesse maximale*

4.1. Configuration par défaut

Les paramètres par défaut sont définis pour chacune des tâches spécifiques à la protection antivirus :

PROTECTION EN TEMPS REEL EN MODE SURVEILLANCE

La protection en temps réel de votre ordinateur est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du programme.

Le *niveau recommandé*, avec les paramètres suivants, est appliqué par défaut à la protection en temps réel :

- Analyse des fichiers en lecture, écriture et exécution, à savoir :
    - Les fichiers des disques durs et amovibles, les secteurs d'amorçage ;

- Les fichiers des disques de réseau ;
- Les fichiers compactés, les objets OLE et les flux NTFS supplémentaires.

- Utilisation des technologies iChecker™ et iStreams™
- En cas de découverte d'un objet infecté, Kaspersky Anti-Virus tente de le réparer. Si la réparation est impossible, elle supprime l'objet après avoir créé une copie dans le dossier de sauvegarde. En cas de découverte d'un objet suspect, elle le met en quarantaine ;
- En cas de découverte d'un riskware, Kaspersky Anti-Virus empêche l'exécution de celui-ci et consigne les informations dans le rapport ;
- Le courrier électronique est analysé :
  - L'analyse de tous les messages entrants via le protocole POP3 est activée, ainsi que l'analyse des fichiers dans les archives ;
  - L'analyse du courrier sortant via le protocole SMTP est désactivée ;
- Les macros VBA, utilisées notamment par les programmes de la suite Microsoft Office, sont analysées. Lors de la découverte d'une macro suspecte, Kaspersky Anti-Virus bloque son exécution ;
- Les scripts dynamiques VBScript et JavaScript, traités par Microsoft Internet Explorer ou le module de traitement des scripts du système d'exploitation, sont analysés ; lors de la découverte d'un script suspect, Kaspersky Anti-Virus bloque son exécution.
- La protection contre les attaques de réseau est desactivée.

ANALYSE A LA DEMANDE

Le *niveau recommandé*, avec les paramètres suivants, est appliqué par défaut à l'analyse complète de l'ordinateur :

- L'analyse complète programmée est réalisée chaque vendredi à 20h00 ;
- Sont analysés :
  - Les fichiers des disques durs et les secteurs d'amorçage ;
  - Les fichiers situés dans les ressources de la mémoire vive et les objets lancés automatiquement au démarrage (objets de démarrage) et les flux NTFS complémentaires ;
  - Les objets compactés, les archives, les archives auto-extractibles et les objets OLE .

Lors de l'analyse complète de l'ordinateur, les boîtes aux lettres utilisées ne sont pas analysées.

- Utilisation des technologies iChecker™ et iStreams™
- Les objets situés sur les disques de réseau, les bases de données de messagerie et les messages individuels ne sont pas analysés ;
- En cas de découverte d'un objet suspect ou infecté, Kaspersky Anti-Virus diffère le traitement jusque la fin de l'analyse antivirus puis confirme l'action à réaliser auprès de l'utilisateur avant de traiter l'objet.
- En cas de découverte d'un riskware, Kaspersky Anti-Virus le laisse passer et consigne les informations dans le rapport.

MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES DE L'APPLICATION

Les paramètres suivants sont appliqués par défaut à la mise à jour des bases antivirus et des modules de l'application :

- La mise à jour des bases antivirus a lieu toutes les 3 heures à partir de l'installation de Kaspersky Anti-Virus ;

Si l'ordinateur est allumé moins de trois heures par jour, les bases seront actualisées directement après le nouveau démarrage de Kaspersky Anti-Virus.

- La mise à jour des bases antivirus et les mises à niveau urgentes de Kaspersky Anti-Virus sont autorisées. Le message de circonstance apparaît avant l'installation de la mise à jour.

ISOLEMENT DES OBJETS SUSPECTS

Les paramètres par défaut suivants sont appliqués à la mise en quarantaine des objets :

- La taille du dossier de quarantaine n'est pas limitée ;
- La durée de conservation des objets en quarantaine est limitée à 90 jours.

CONSERVATION D'UNE COPIE DE L'OBJET INFECTE

Avant la réparation ou la suppression d'un objet, une copie est créée dans le dossier de sauvegarde. Les paramètres suivants sont appliqués par défaut :

- La taille du dossier de sauvegarde n'est pas limitée ;
- La durée de conservation des objets dans le dossier de sauvegarde est limitée à 90 jours.

4.2. Niveau de protection antivirus

Afin de faciliter la configuration des paramètres de la protection antivirus, le logiciel propose trois niveaux préconfigurés (cf. Tableau 1. Configuration des paramètres des niveaux de protection*) :*

- **Sécurité maximale** : niveau de protection de l'ordinateur correspondant au niveau de protection maximum, au détriment d'un léger recul des performances du système.
- **Niveau recommandé** : niveau de protection antivirus qui repose sur les paramètres recommandés par les experts de Kaspersky Lab et qui assure la protection optimale de votre ordinateur.
- **Vitesse maximale** : niveau de protection de l'ordinateur correspondant à la vitesse maximale de fonctionnement, au détriment d'une légère réduction du nombre d'objets analysés.

En cas de modification des paramètres de n'importe quel niveau via l'interface locale ou via la console d'administration de Kaspersky Administration Kit 5.0, le niveau est renommé **Paramètres utilisateur**. Il s'agit du quatrième niveau de protection antivirus reposant sur les paramètres définis par l'utilisateur.

Si les paramètres sont modifiés via la console d'administration, la partie droite de l'onglet **Protection** indiquera que les paramètres sont définis par l'administrateur.

Le tableau ci-après reprend la valeur des paramètres des niveaux prédéfinis pour la protection en temps réel (**protection**) et l'analyse à la demande (**analyse**).

Valeurs conventionnelles :

- **+** paramètre activé ;
- **–** paramètre désactivé ;
- **x** aucune configuration prévue pour cette tâche.

Tableau 1. Configuration des paramètres des niveaux de protection

Paramètre	Sécurité maximale		Recommandé		Vitesse maximale	
	Protection	Analyse	Protection	Analyse	Protection	Analyse
Utiliser iChecker	+	+	+	+	+	+
Utiliser iStreams	+	+	+	+	+	+
Niveau d'analyse	Fichier en fonction du format	Tous les fichiers	Fichier en fonction du format	Tous les fichiers	Fichiers en fonction de l'extension	Fichier en fonction du format

Paramètre	Sécurité maximale		Recommandé		Vitesse maximale	
	Protection	**Analyse**	**Protection**	**Analyse**	**Protection**	**Analyse**
Taille maximale de l'objet analysé (Mo)	x	–	x	–	x	8
Durée maximale de l'analyse de l'objet (s.)	60	–	60	–	60	60
Disques durs	+	x	+	x	+	x
Disques amovibles	+	x	+	x	+	x
Disques de réseau	+	x	+	x	–	x
Flux NTFS	+	+	+	+	+	+
Secteurs d'amorçage des disques	+	+	+	+	+	+
Fichiers compactés	+	+	+	+	+	+
Archives	x	+	x	+	x	–
Archives auto-extractibles	+	+	–	+	–	+
Bases de données de messagerie électronique.	x	+	x	–	x	–
Messages individuels	x	+	x	–	x	–
Objets OLE	+	+	+	+	–	+

CHAPITRE 5. ADMINISTRATION DE L'APPLICATION VIA L'INTERFACE LOCALE

Ce chapitre explique de manière détaillée l'utilisation et la configuration des principales tâches exécutées par Kaspersky Lab ainsi que les possibilités complémentaires offertes via l'interface locale

5.1. Mise à jour des bases antivirus et des modules du logiciel

Kaspersky Anti-Virus permet d'automatiser le téléchargement de la mise à jour des bases antivirus qui reprennent la description des virus et des méthodes de réparation ainsi que de la mise à jour des modules du logiciel depuis les serveurs de mise à jour de Kaspersky Lab.

La mise à jour des bases antivirus est la garantie de la sécurité de votre ordinateur. Des centaines de nouveaux virus voient le jour chaque jour et les experts de Kaspersky Lab actualisent quotidiennement le contenu des bases antivirus. Il est conseillé de procéder à la mise à jour des bases antivirus au moins une fois toutes les 3 heures. Lors d'une épidémie, la fréquence devrait être la plus courte possible, une fois toutes les heures de préférence.

Afin de télécharger les mises à jour, Kaspersky Anti-Virus contacte les serveurs de mise à jour de Kaspersky Lab, le serveur http ou ftp défini par l'utilisateur ou un répertoire local ou de réseau de votre ordinateur. En cas d'utilisation de Kaspersky Administration Kit, la mise à jour peut être réalisée au départ du répertoire de mise à jour situé sur le *Serveur d'administration*.

Le lancement de ce programme peut s'opérer manuellement ou selon un horaire défini. Afin de toujours recevoir les versions les plus récentes des bases antivirus en temps opportun, il est recommandé de programmer le lancement automatique du programme de mise à jour (pour de plus amples informations sur la programmation, consultez le point 5.8 à la page 103).

5.1.1. Nécessité de la mise à jour

Le logiciel vous prévient lorsqu'il est temps de procéder à la mise à jour. Vous pouvez également vous rendre compte par vous-même de la nécessité d'une mise à jour en lisant une description de l'état des bases antivirus dans la partie droite de l'onglet **Protection** (cf. ill. 2).

L'état des bases est indiqué par l'un des trois icônes suivants :

Les bases antivirus ont été actualisées il y a peu ou sont actualisées à l'instant.

La mise à jour des bases antivirus est nécessaire. Si cette mise à jour est impossible en raison de la fin de validité de la licence, le logiciel affichera les informations sur la marche à suivre pour renouveler la licence ;

La mise à jour des bases antivirus est urgente car elles sont soit très dépassées, soit absentes, soit corrompues.

5.1.2. Mise à jour manuelle. Téléchargement des mises à jour

Afin de lancer manuellement le programme de mise à jour :

Cliquez sur le lien Télécharger les mises à jour dans la partie gauche de l'onglet **Protection** ;

Ou :

Cliquez sur le lien procéder à la mise à jour des bases antivirus dans le texte décrivant l'état des bases antivirus dans la partie droite de l'onglet **Protection** ;

Ou :

Sélectionnez le point **Mettre à jour les bases antivirus** dans le menu contextuel qui apparaît suite au clic-droit sur l'icône du programme dans la barre des tâches.

Cette action entraîne l'ouverture d'une fenêtre (cf. ill. 6) reprenant des renseignements sur l'exécution de la mise à jour des bases antivirus et des modules de l'application.

Le téléchargement des mises à jour est un processus qui peut être décomposé de la manière suivante :

1. Kaspersky Anti-Virus vérifie la connexion au réseau et établit la connexion à la source de la mise à jour
2. Le serveur des mises à jour de Kaspersky Lab envoie au logiciel la liste des mises à jour et leur taille respective.
3. Ensuite, Le logiciel compare l'état des bases antivirus et des modules de Kaspersky® Anti-Virus aux informations fournies par la source. Si la version la plus récente des bases antivirus est déjà installée sur votre ordinateur, la mise à jour est interrompue. Dans le cas contraire, les fichiers sont copiés sur votre ordinateur.

   Une barre d'état montre la progression de la copie. Le champ **Mise à jour télécharge** indique le volume de la mise à jour déjà téléchargé.
4. Le programme active automatiquement les bases antivirus reçues. Si cette opération réussit, Kaspersky Anti-Virus commence à utiliser les bases lors de l'analyse de l'ordinateur. Si une erreur survient suite à l'activation des bases antivirus actualisées, la remise à l'état antérieur sera lancée automatiquement.

Le redémarrage de l'ordinateur peut être requis pour assurer l'activation correcte des mises à jour. Dans ce cas, les avertissement de circonstance seront affichés.

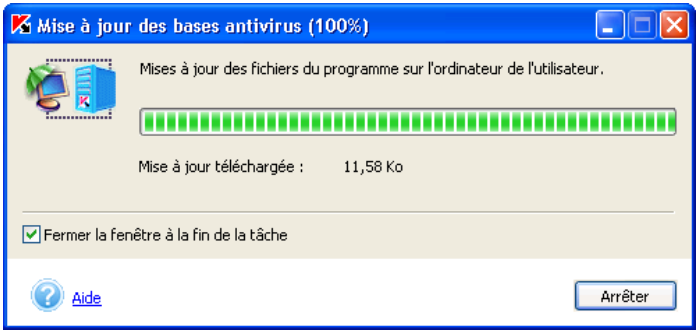

Illustration 6. Mise à jour des bases antivirus et des composants du logiciel

5.1.3. Configuration de la mise à jour

Pour configurer les paramètres de la mise à jour des bases antivirus :

Cliquez sur Mises à jour dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3).

Cette action entraîne l'ouverture de la fenêtre **Mise à jour des bases antivirus** (cf. ill. 7).

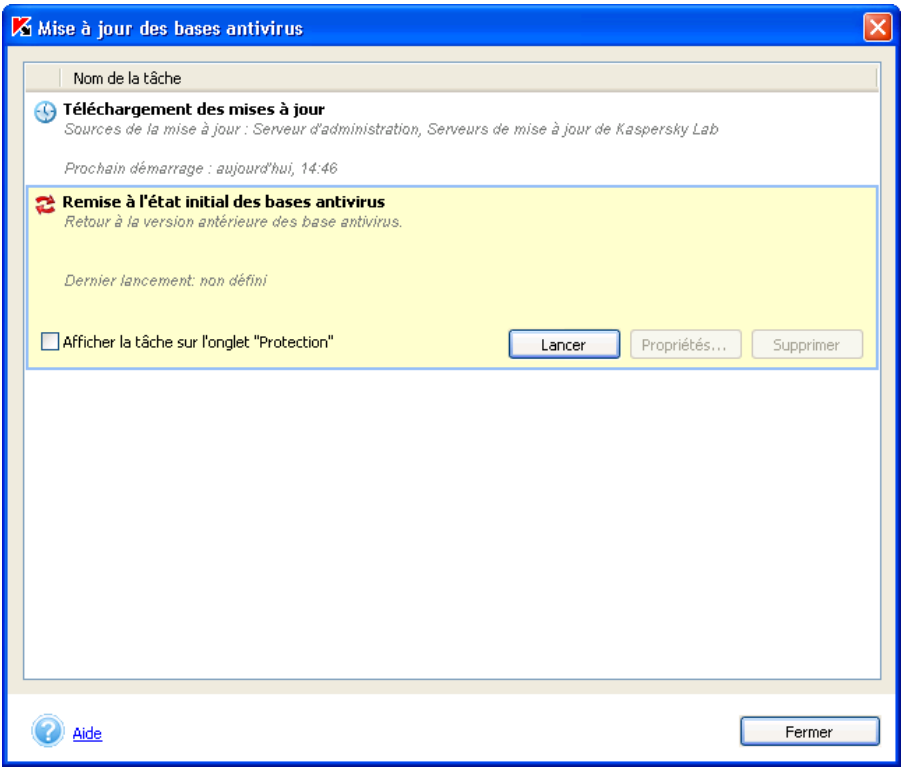

Illustration 7. Liste des tâches liées à la mise à jour des bases antivirus

En cliquant sur le nom de la tâche, vous ouvrez un bloc contenant les informations relatives à la source de la mise à jour et à l'heure du dernier et du prochain lancement de la mise à jour. Grâce au bouton **Lancer** de ce bloc, vous pouvez lancer manuellement la mise à jour des bases antivirus et à l'aide du

bouton **Propriétés…**, vous pouvez ouvrir la fenêtre de configuration de la mise à jour des bases antivirus (cf. ill. 8) et définir les paramètres suivants :

- Programmer le lancement automatique de la mise à jour (cf. point 5.8, page 103).
- Activer la mise à jour des modules de Kaspersky Anti-Virus (cf. point 5.1.3.1 , page 49).
- Configurer la copie des mises à jour dans un répertoire local afin de les diffuser sur les autres ordinateurs du réseau équipés de Kaspersky Anti-Virus (cf. point 5.1.3.2, p. 51).
- Sélectionner la source de la mise à jour : serveurs de Kaspersky Lab, serveur http ou ftp indiqué par l'utilisateur ou répertoire local ou de réseau de l'ordinateur (cf. point 5.1.3.3, p. 52).
- Configurer les paramètres du serveur proxy (cf. point 5.1.3.4, page 54).
- Configurer le lancement d'une tâche avec les privilèges d'un autre utilisateur (uniquement pour les ordinateurs tournant sous Microsoft Windows NT/2K/XP) (cf. point 5.9, p. 107)
- Sélectionner le type de base antivirus à télécharger (cf. point 5.1.3.5, p.55).

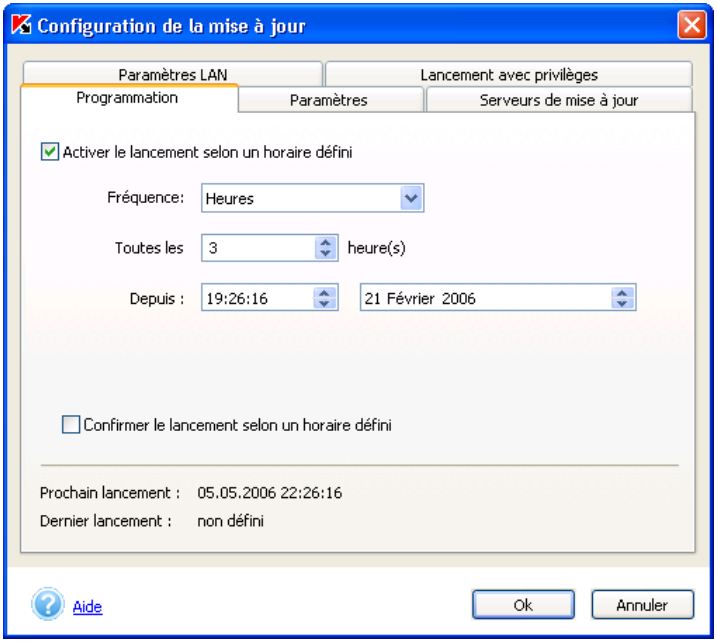

Illustration 8. Configuration de la mise à jour des bases antivirus

La tâche **Remise à l'état initial des bases antivirus** n'est pas configurable. Vous pouvez uniquement la lancer pour revenir à la version antérieure des bases antivirus..

5.1.3.1. Mise à jour des modules de l'application

En plus des bases antivirus, vous pouvez également mettre à jour les propres modules de Kaspersky Anti-Virus. Ces mises à jour sont diffusées sur le serveur de mise à jour au fur et à mesure de leur publication.

Vous pouvez mettre à jour les modules de l'application au départ de la source de mise à jour choisie pendant la configuration (cf. point 5.1.3.3, p. 52). Pour ce faire, il suffit de cocher la case **Installer la mise à jour des modules de l'application** dans l'onglet **Paramétres** de la boîte de dialogue **Configuration de la mise à jour** (cf. ill. 9). Sélectionnez les mises à jour que vous souhaitez installer :

- **Uniquement les mises à jour urgentes**;
- **Toutes les mises à jour accessibles.**

Si vous souhaitez que les mises à jour soient installées automatiquement après le téléchargement, désélectionnez la case **Confirmer l'installation**.

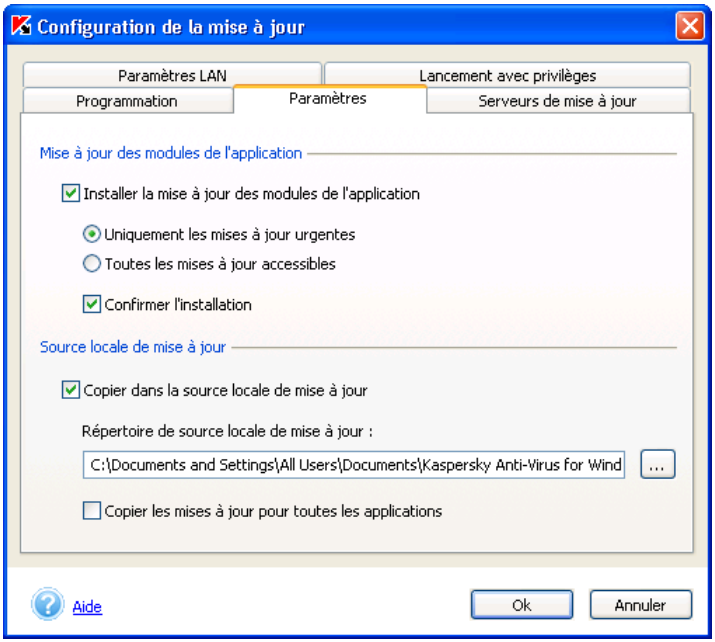

Illustration 9. Fenêtre de configuration de la mise à jour.
Onglet **Paramètres**

Au moment de la réception de la mise à jour des modules de l'application, la requête suivante s'affiche (cf. ill. 10). Choisissez l'une des options suivantes :

- **Installer la mise à jour des modules de l'application;**
- **Ne pas mettre à jour des modules de l'application et me rappeler plus tard** : rappeler l'installation de la mise à jour des modules du programme au prochain démarrage de Kaspersky Anti-Virus.
- **Désactiver l'installation de la mise à jour des modules de l'application** : en cas de sélection de cette option, la case **Installer la mise à jour des modules de l'application** de l'onglet **Paramètres** de la boîte de dialogue **Configuration de la mise à jour** (cf. ill. 9) sera désélectionnée et la mise à jour des modules de l'application sera désactivée.

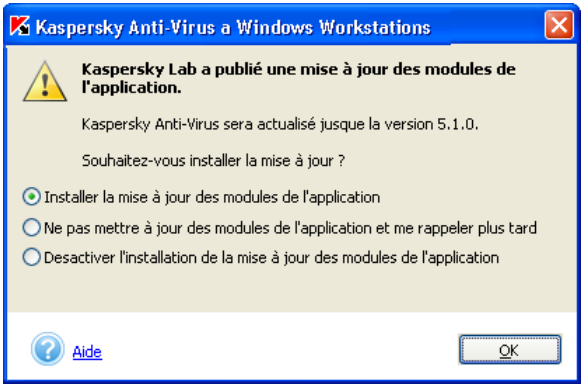

Illustration 10. Confirmation de l'installation des modules de l'application.

5.1.3.2. Copie de la mise à jour dans un répertoire local

Vous pouvez également configurer le service de copie de la mise à jour au départ de l'onglet **Paramétres** (cf. ill. 9). Ce service vous permet de conserver, dans un répertoire local, les mises à jour des bases antivirus et des modules logiciels de l'application obtenues sur le serveur de Kaspersky Lab afin de les distribuer aux autres ordinateurs du réseau (équipés de Kaspersky Anti-Virus) et de réduire ainsi le trafic de données Internet.

Cochez la case **Copier dans la source locale de mise à jour** afin d'activer le service. Saisissez dans le champ **Répertoire de source locale de mise à jour** le chemin d'accès au répertoire.

De plus, vous pouvez également sélectionner le mode de copie de la mise à jour :

- *complet* : la copie porte sur les bases antivirus et sur les mises à jour des modules pour toutes les applications de Kaspersky Lab. Pour sélectionner ce mode, cochez la case **Copier la mises à jour pour toutes les applications**.
- *partiel* : la copie porte sur les bases antivirus et les mises à jour des modules de l'application de Kaspersky Anti-Virus 5.0 for Windows Workstations et de Kaspersky Anti-Virus 5.0 for Windows File Servers. Afin de sélectionner ce mode de mise à jour, il convient de désélectionner la case **Copier la mises à jour pour toutes les applications** (cette case est cochée par défaut).

5.1.3.3. Sélection de la source de la mise à jour

La sélection de la source de la mise à jour s'opère sur l'onglet **Serveurs de mise à jour** de la boîte de dialogue **Configuration de la mise à jour** (cf. ill. 11).

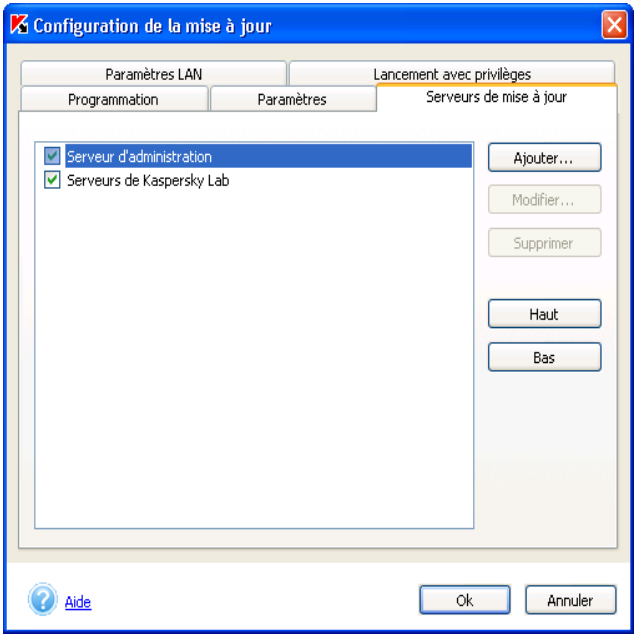

Illustration 11. Fenêtre de configuration de la mise à jour.
Onglets **Serveurs de mise à jour**

La mise à jour peut être réalisée au départ des ressources suivantes :

- *Serveur d'administration* : dossier central contenant les mises à jour et situé sur le serveur d'administration de Kaspersky Administration Kit. Cette source n'est pas accessible si l'agent d'administration n'est pas installé sur l'ordinateur (pour de plus amples informations, consultez le manuel de l'utilisateur de Kaspersky Administration Kit 5.0).
- *Serveurs de Kaspersky Lab* sont les sites Internet que Kaspersky Lab utilise pour diffuser les mises à jour des bases antivirus et des modules des applications.
- *Serveurs ftp ou http* ajoutés par l'utilisateur et contenant les mises à jour.
- Répertoire local ou de réseau.

Par défaut, la mise à jour s'opère via Internet depuis les serveurs de mises à jour de Kaspersky Lab ou depuis le serveur d'administration en cas d'utilisation de Kaspersky Administration Kit 5.0. Vous pouvez agrandir la liste et ajouter des sources complémentaires. Pour ce faire, cliquez sur **Ajouter…** et sélectionnez le type de source : *Adresse du serveur de mise à jour* ou *Répertoire*. Si vous choisissez *Adresse du serveur de mise à jour*, saisissez l'adresse du serveur ftp ou http (il convient de saisir également le préfixe du protocole utilisé, par exemple : *http://server.net* ou *ftp://10.0.0.1*). Si vous avez choisi *Répertoire*, indiquez le chemin d'accès au répertoire contenant la mise à jour.

Vous pouvez modifier les paramètres de la source de la mise à jour à l'aide du bouton **Modifier…**. Pour la source de type *Adresse du serveur* de mise à jour, vous pouvez modifier l'adresse et pour la source de *type Répertoire*, vous pouvez modifier le chemin d'accès.

Vous pouvez sélectionner l'emplacement géographique du serveur de Kaspersky Lab au départ duquel la mise à jour sera copiée grâce à la liste déroulante des pays **Emplacement** (cf. ill. 12). Par défaut, le pays est sélectionné sur la base des paramètres régionaux du système d'exploitation. Afin de définir le serveur le plus proche de vous géographiquement, il est conseillé d'indiquer votre situation géographique actuelle. Cela permet d'accélérer la vitesse de téléchargement des mises à jour. Vous pouvez également désactiver l'utilisation du serveur proxy en cochant la case adéquate.

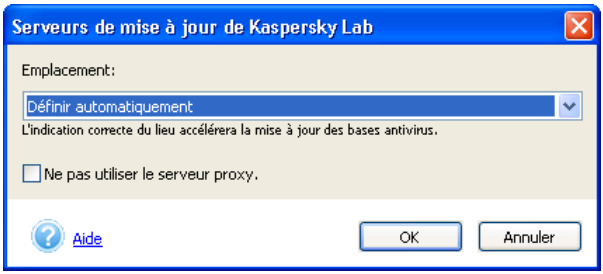

Illustration 12. Fenêtre de configuration de la mise à jour. Sélection de l'emplacement du serveur

Afin que la mise à jour soit réalisée au départ de la source définie, cochez la case qui se trouve en regard de celle-ci . Il est possible de sélectionner plusieurs sources simultanément. Dans ce cas, Kaspersky Anti-Virus réalisera la mise à jour au départ de la première source de la liste. Si cette source n'est pas accessible pour une raison quelconque, la mise à jour sera réalisée au départ de la source suivante et ainsi de suite. Il est possible de modifier l'ordre des sources à l'aide des boutons **Haut/Bas**.

5.1.3.4. Configuration du serveur proxy

Cliquez sur l'onglet **Paramètres LAN** (cf. ill. 13) afin d'ouvrir la fenêtre permettant la saisie des données nécessaires à la connexion. Il existe deux moyens pour définir les paramètres du serveur proxy :

- **Définir automatiquement les paramètres du serveur proxy**;
- **Utiliser un autre serveur proxy**.

La première option est sélectionnée par défaut. Les paramètres du serveur proxy seront identiques à ceux repris dans Microsoft Internet Explorer. Si le serveur proxy requiert une autorisation, sélectionnez la deuxième option et définissez manuellement les paramètres du serveur proxy :

Adresse: adresse IP du serveur proxy au format décimal (ex. : 10.10.10.102) ou son nom.

Port : numéro du port sur lequel est installé le serveur proxy. Sélectionnez une des valeurs proposées dans la liste déroulante : *3128*, *8080*, *8082*, *8903* ou saisissez une valeur spécifique.

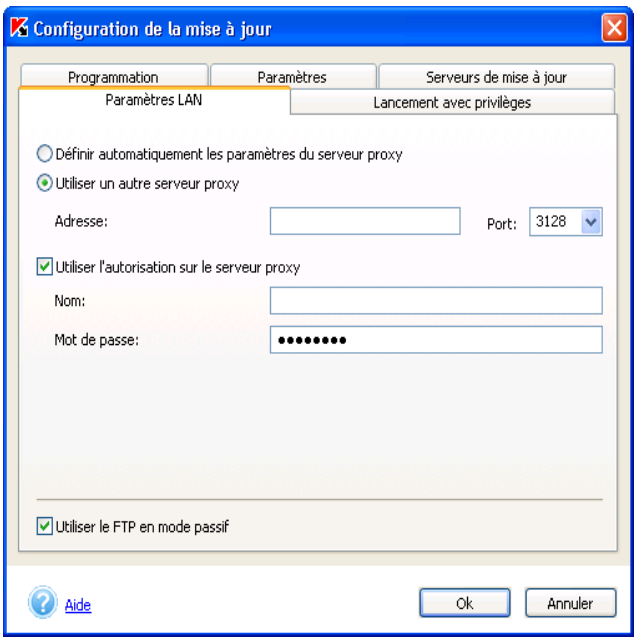

Illustration 13. Configuration des paramètres LAN

Si le serveur proxy requiert une autorisation, cochez la case **Utiliser l'autorisation sur le serveur proxy** et indiquez le nom et le mot de passe dans les champs de la partie inférieure.

Si l'autorisation sur le serveur proxy est requise et que vous n'avez pas indiqué le nom et le mot de passe correct ou que les données que vous avez saisies n'ont pas été acceptées par le serveur proxy pour une raison quelconque, vous devrez saisir le nom d'utilisateur et le mot de passe au lancement de la mise à jour. Si l'autorisation est accordée, le nom et le mot de passe utilisés seront sauvegardés pour la prochaine mise à jour. Dans le cas contraire, il faudra à nouveau saisir les paramètres d'autorisation.

Si un pare-feu est installé sur votre ordinateur et que vous ne parvenez pas à vous connecter à un serveur FTP en mode actif, cochez la case **Utiliser le FTP en mode passif**.

5.1.3.5. Sélection du type de mise à jour

Kaspersky Anti-Virus vous propose deux types de bases antivirus à utiliser :

- *Bases standard* : bases antivirus contenant les définitions de tous les programmes malveillants connus à ce jour et les moyens de les neutraliser.
- Si vous souhaitez protéger vos données contre les riskwares, vous devrez utiliser les *bases étendues*. En plus des définitions des bases standard, celles-ci reprennent les descriptions des adwares, des logiciels espion, des utilitaires d'attaque et d'autres programmes qui présentent un risque potentiel.

Les bases antivirus standard suffisent amplement pour assurer la protection normale de votre ordinateur. L'utilisation des bases étendues peut avoir un impact sur la vitesse de Kaspersky® Anti-Virus. De plus, il existe toute une série de logiciels que vous utilisez et qui pourraient être considérés comme des programmes présentant un risque potentiel.

Afin de sélectionner le type de base utilisé par Kaspersky Anti-Virus :

1. Cliquez sur le lien Menaces et exclusions dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3).
2. Dans la boîte de dialogue qui s'ouvre (cf. ill. 14) , cochez les cases **Adwares**, **riskwares**, **numéroteurs automatiques** dans la section **Menaces identifiées** si vous souhaitez utiliser les bases antivirus étendues. Afin de ne pas supprimer des programmes que vous utilisez, il est conseillé de choisir une action qui requiert la confirmation de

l'utilisateur en cas de découverte d'un objet dangereux (cf. point 5.3.3.2, p. 86).

La case **Virus, vers, chevaux de Troie et utilitaires d'attaques, logiciels espion** est cochée par défaut et ne peut pas être désélectionnée. Elle indique que les bases antivirus standard sont utilisées pour l'analyse.

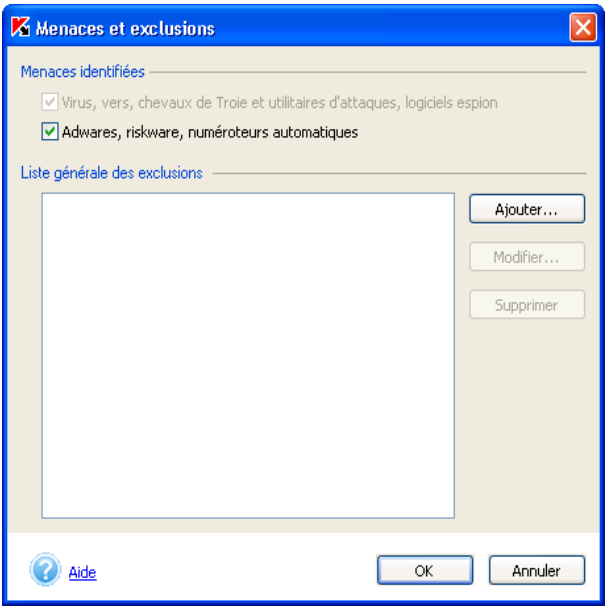

Illustration 14. Sélection du type de base antivirus

5.2. Mode de protection en temps réel

La protection en temps réel de votre ordinateur est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du programme.

En mode protection en temps réel, Kaspersky Anti-Virus se trouve en permanence dans la mémoire vive et contrôle en permanence toutes les requêtes vers les objets du système de fichiers, le courrier entrant et sortant ainsi que les scripts VBScript et JavaScript qui présentent un danger potentiel, les macros utilisées dans les applications bureautiques et les riskwares.

Lorsque l'utilisateur ou une application ouvre un objet en lecture/en écriture, l'application vérifie que l'objet est exempt de virus. Si elle en détecte un, elle propose soit de réparer l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction des paramètres définis). Ainsi, l'application permet de détecter et d'éradiquer les codes malicieux avant que le système soit réellement infecté.

Plusieurs fonctions sont exécutées dans le cadre de la protection en temps réel :

- Protection en temps réel des fichiers (cf. point 5.2.1, page 59);
- Protection en temps réel du courrier (cf. point 5.2.2, page 64);
- Analyse des macros VBA (cf. point 5.2.4, p.70);
- Protection en temps réel contre les scripts (cf. point 5.2.5, page 71);
- Protection en temps réel contre les attaques de réseau (cf. point 5.2.6, page 73);

Chacune de ces fonctions peut être configurée séparément ou désactivée, ce qui n'a aucune conséquence sur le fonctionnement des autres composantes de la protection en temps réel de l'ordinateur.

Toutes les informations relatives à l'état actuel de la protection en temps réel sont reprises dans la partie droite de l'onglet **Protection** (cf. ill. 2) de la fenêtre principale du logiciel.

L'état peut être caractérisé par l'un des symboles suivants :

La protection en temps réel est activée et la configuration correspond à celle recommandée ;

La protection en temps réel est activée et la configuration ne correspond pas à celle recommandée ;

La protection antivirus est suspendue. Cela signifie que la protection de votre ordinateur a été temporairement désactivée.

La protection en temps réel ne fonctionne pas. Dans ce cas, il est conseillé de configurer la protection de l'ordinateur et de la lancer.

La protection en temps réel est active depuis le démarrage du système d'exploitation jusqu'au moment où vous éteignez l'ordinateur. Il peut arriver qu'il faille suspendre la protection en temps réel. Pour ce faire, ouvrez le menu contextuel de Kaspersky Anti-Virus et sélectionnez le point **Arrêter la protection en temps réel** (cf. ill. 1)

Etant donné qu'il n'est pas recommandé de désactiver entièrement la protection en temps réel, Kaspersky Anti-Virus vous offre la possibilité de la suspendre pour une brève période.

Pour désactiver la protection en temps réel :

Dans la fenêtre **Arrêt de la protection en temps réel** (cf. ill. 15), sélectionnez une des options suivantes :

- **Dans 5/10/15 minutes** : la protection sera activée après le délai spécifié.
- **Lors de la prochaine connexion au réseau** : la protection sera à nouveau activée dès que l'ordinateur sera à nouveau raccordé au réseau (cette option apparaît dans la liste quand l'ordinateur n'est pas connecté au réseau).
- **Lors du prochain lancement de Kaspersky Anti-Virus** : la protection sera activée si vous lancez le programme au départ du menu **Démarrer → Programmes → Kaspersky Anti-Virus for Windows Workstations** ou après le redémarrage du système (si le lancement du logiciel au démarrage du système est activé).
- **Uniquement sur demande de l'utilisateur**: la protection sera uniquement réactivée lorsque vous l'aurez **décidé** Pour activer à nouveau la protection, sélectionnez **Rétablir la protection en temps réel** dans le menu contextuel de Kaspersky Anti-Virus.

Illustration 15. Désactivation temporaire de la protection en temps réel.

La désactivation de la protection en temps réel augmente considérablement les risques d'infection de votre ordinateur. Toutefois, lors de l'exécution de certaines opérations (ex. : défragmentation d'un disque utilisant le système de fichiers FAT32), vous pouvez désactiver la protection en temps réel afin de gagner du temps..

Le cas échéant, vous pouvez décider de désactiver non pas toute la protection, mais uniquement l'un de ses composants : la protection du système de fichiers (cf. point 5.2.1, p. 59), la protection du courrier (cf. point 5.2.2, p. 64), l'analyse des macros (cf. point 5.2.4, p. 70), l'analyse des scripts (cf. point 5.2.5, p. 71) ou la protection contre les attaques de réseau (cf. point 5.2.6, p. 73).

Pour consulter ou modifier les paramètres de la protection en temps réel :

Cliquez sur le lien Protection en temps réel dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3).

La boîte de dialogue de la protection en temps réel est divisée en onglets selon les fonctions de la protection. Vous trouverez ci-après une description détaillée de chacune de ces fonctions.

5.2.1. Analyse du système de fichiers

Lorsque la protection en temps réel est installée et activée, Kaspersky Anti-Virus vérifie si les requêtes adressées au système de fichiers sont exemptes de code malicieux.

La configuration de la protection en temps réel du système de fichiers s'opère dans l'onglet **Fichiers** (cf. ill. 16) de la fenêtre **Configuration de la protection en temps réel**. Il est possible de :

- Activer/désactiver la protection. Pour ce faire, cochez ou désélectionnez la case **Activer la protection en temps réel du système de fichiers**. La case est cochée par défaut, la protection est activée;
- Définir le niveau de la protection antivirus et procéder à une configuration détaillée du niveau sélectionné (cf. point 5.2.1.1, p. 60) ;
- Dresser la liste des objets qui ne seront pas soumis à la protection en temps réel des fichiers (cf. point 5.7, p. 99) ; pour ouvrir la fenêtre de constitution de la liste des exclusions, cliquez sur non défini/ défini à côté du paramètre d'**exclusion** dans la description des paramètres de protection définis. L'aspect des liens change en fonction de la définition ou non d'exclusions ;

- Dresser la liste des processus de confiance dont l'activité des fichiers ne sera pas soumises à la protection en temps réel des fichiers (cf. point 5.5, p. 96) ;
- Définir l'action qui sera exécutée par Kaspersky Anti-Virus en cas de découverte d'objets dangereux et suspects (cf. point 5.2.1.2, p. 62).

Si la protection en temps réel des fichiers n'est pas installée, la configuration de ces paramètres est impossible. Pour installer la protection des fichiers, vous devrez installer à nouveau le programme

Illustration 16. Paramètres de la protection des objets du système de fichiers

5.2.1.1. Sélection du niveau de protection

Sélectionnez dans le menu déroulant **Configuration du niveau de protection** l'un des trois niveaux prédéfinis par les experts de Kaspersky Lab (pour de plus amples informations, consultez le Chapitre 4 à la page 39). Par défaut, c'est le niveau recommandé qui est activé.

Vous pouvez personnaliser n'importe lequel de ces niveaux de protection. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**. Les

paramètres utilisateur ne seront pas sauvegardés après le rétablissement de l'un des trois niveaux prédéfinis.

Vous pouvez consulter et modifier les paramètres du niveau sélectionné dans la fenêtre **Configuration de la protection en temps réel des fichiers** (cf. ill. 17) qui s'ouvre lorsque vous avez cliqué sur **Configuration** dans l'onglet **Fichiers** (cf. ill. 16).

Dans la section **Zone d'analyse**, cochez les cases pour définir les disques à analyser.

Sélectionnez, dans la section **Objets à analyser**, les objets qui seront soumis à l'analyse :

- **Analyser tous les objets** : analyse tous les objets sans tenir compte de leur type et de leur extension.
- **Analyser uniquement les objets qui peuvent être infectés** : analyse les objets qui présentent un risque d'infection ; l'analyse s'opère sur la base de la structure interne du fichier.
- **Analyser les objets en fonction de l'extension** : analyse les fichiers qui présentent un risque d'infection ; l'analyse s'opère sur la base de l'extension du fichier.

Dans la rubrique **Paramètres complémentaires de la protection des fichiers**, vous pouvez limiter la durée de l'analyse d'un objet en définissant une durée en secondes et définir si les catégories suivantes seront analysées:

- Les objets associés ou intégrés à d'autres fichiers (les *objets OLE*) ;
- Les fichiers exécutables compactés ;
- Les archives auto-extractibles ;
- Les secteurs d'amorçage des disques.

La section **Accélération de l'analyse des objets** vous donne la possibilité de recourir ou non aux technologies d'accélération de l'analyse iChecker™ et iStreams™. Pour utiliser ces technologies, il suffit simplement de cocher les cases correspondantes.

Si pendant l'installation du logiciel vous avez décidé de ne pas utiliser la technologie iStreams™, vous devrez réinstaller Kaspersky Anti-Virus si vous souhaitez activez cette technologie. Tant que cela ne sera pas fait, il ne sera pas possible de configurer cette fonction.

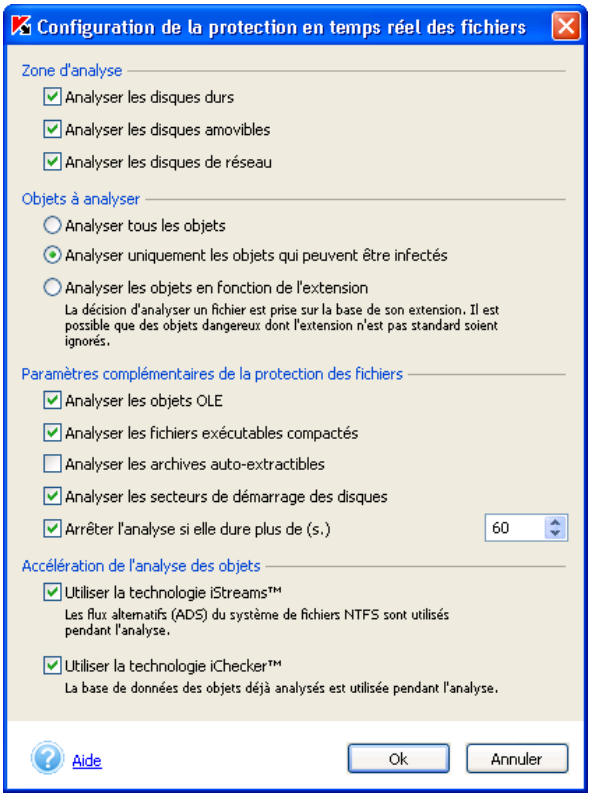

Illustration 17. Configuration détaillée de la protection en temps réel des fichiers

5.2.1.2. Sélection de l'action à réaliser sur l'objet découvert

Sélectionnez l'action qui sera réalisée par Kaspersky Anti-Virus suite à la découverte d'un objet suspect ou dangereux dans la section **Actions à réaliser sur les objets découvert** (cf. ill.16) :

- **Confirmer l'action auprès de l'utilisateur** : bloque l'accès à l'objet et affiche un message reprenant les différentes options de traitement possible. Il s'agit du mode de fonctionnement par défaut.

  Si vous ne réagissez pas dans les 30 secondes qui suivent l'affichage du message, l'action recommandée sera exécutée par défaut. Pour chaque type d'objet identifié, il existe une action recommandée.

Voici la liste de toutes les actions que Kaspersky Anti-Virus peut proposer (le contenu de la liste peut varier en fonction du type d'objet):

- *Réparer* l'objet infecté ;
- *Mettre* l'objet potentiellement infecté par un virus ou l'une de ses variantes *en quarantaine*.

Il arrive parfois, lors de la mise en quarantaine d'un fichier, qu'un message apparaisse et indique que l'objet ne peut être supprimé. Cela est du au fait que les objets mis en quarantaine sont déplacés : ils sont copiés dans le répertoire de quarantaine et supprimés de leur répertoire d'origine. Cependant, il n'est pas possible de supprimer tous les objets lors du déplacement. Ainsi, il est impossible de supprimer un objet qui est utilisé en ce moment par un programme quelconque.

- *Supprimer* l'objet dangereux qui n'a pas pu être réparé.
- *Ignorer* les objets infectés. Aucune action n'est réalisée et les informations sont simplement consignées dans le rapport.

- **Exécuter l'action recommandée** : bloque l'accès à l'objet et exécute l'action recommandée pour ce type d'objet. Pour les objets infectés, l'action recommandée est *Réparer, supprimer si la réparation est impossible*[4]. Pour les objets potentiellement infectés, l'action est *Mettre en quarantaine* et pour les chevaux de Troie et les vers, il s'agit de *Supprimer*. Si l'objet infecté/potentiellement infecté est un riskware, l'accès est bloqué.
- **Interdire l'accès, réparer ou supprimer si la réparation est impossible :** bloque l'objet et tente de le réparer. Si la réparation est impossible, l'objet est supprimé sans intervention de l'utilisateur. Lors de la réparation, une copie de sauvegarde est conservée dans le dossier de sauvegarde.
- **Interdire l'accès et supprimer l'objet** : bloque l'objet et le supprime sans avertissement complémentaire de l'utilisateur. Une copie de l'objet est conservée dans le dossier de sauvegarde.

[4] Par défaut, les objets infectés de la mémoire vive sont supprimés et les secteurs de démarrage infectés sont réparés ou bloqués si la réparation est impossible.

- **Uniquement Interdire l'accès** : bloque l'accès à l'objet sans afficher de message particulier à l'écran sur le traitement adopté ; consigne les informations dans le rapport ;
- **Mettre en quarantaine** (uniquement pour les objets suspects) : bloque l'accès, place l'objet suspect en quarantaine dans l'attente d'une nouvelle analyse à l'aide de bases antivirus actualisées, d'une restauration, de l'envoi aux experts de Kaspersky Lab pour examen ou de la suppression.

5.2.2. Analyse du courrier

La protection en temps réel du courrier entrant et sortant est assurée uniquement si vous aviez décidé de l'utiliser pendant l'installation du logiciel. Pour installer la protection du courrier, vous devrez réinstaller le logiciel.

Lorsque la protection en temps réel est activée, Kaspersky Anti-Virus analyse les requêtes d'envoi et de réception des messages électroniques, empêche l'intrusion de codes malicieux dans votre boîte aux lettres ainsi que l'envoi d'objets suspects ou infectés à vos destinataires.

Kaspersky Anti-Virus :

- Intercepte le courrier entrant et sortant via les protocoles SMTP et POP3 pour n'importe quel client de messagerie ;
- Intercepte le courrier entrant et sortant sous Microsoft Office Outlook via n'importe quel protocole de messagerie ;
- Démasque les objets suspects et infectés dans le corps des messages et les pièces jointes de n'importe quel degré d'intégration.

Pendant l'analyse du courrier, les paramètres du niveau de protection antivirus recommandé sont appliqués par défaut et permettent l'analyse :

- Du courrier entrant via le protocole POP3 ;
- Des archives jointes et des messages individuels.

Veuillez remarquer que, par défaut, le courrier sortant via le protocole SMTP N'EST PAS ANALYSE.

La configuration de la protection en temps réel du courrier s'opère sur l'onglet **Courrier** de la boîte de dialogue **Configuration de la protection en temps réel** (cf. ill. 18). Il est possible de :

- activer/désactiver la protection. Pour ce faire, cochez ou désélectionnez la case ☑ **Activer la protection en temps réel du courrier**. La case est cochée par défaut, la protection est activée;

- Définir le niveau de la protection antivirus et procéder à une configuration détaillée du niveau sélectionné (cf. point 5.2.1.1, p. 66) ;
- Dresser la liste des objets qui ne seront pas soumis à la protection en temps réel du courrier (cf. point 5.7, p. 99) ; Pour ouvrir la fenêtre de constitution de la liste des exclusions, cliquez sur non défini/ défini à côté du paramètre d'**exclusion** dans la description des paramètres de protection définis. L'aspect des liens change en fonction de la définition ou non d'exclusions ;
- Définir l'action qui sera exécutée par Kaspersky Anti-Virus en cas de découverte d'objets dangereux et suspects (cf. point 5.2.1.2, p. 62).

Un module spécial intégré au client de messagerie a été créé pour l'analyse du courrier de Microsoft Office Outlook. Après l'installation de Kaspersky Anti-Virus, la fenêtre de paramètres de Microsoft Office Outlook contient un onglet complémentaire (pour de plus amples informations, consultez le point 5.2.3 à la page 68).

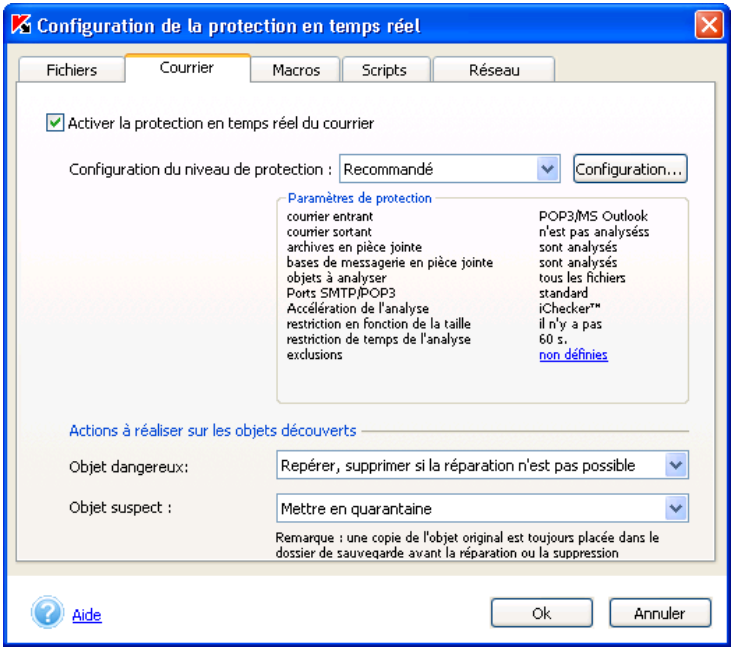

Illustration 18. Paramètres pour la protection du courrier

5.2.2.1. Sélection du niveau de protection

Sélectionnez dans le menu déroulant **Configuration du niveau de protection** l'un des trois niveaux prédéfinis par les experts de Kaspersky Lab (pour de plus amples informations, consultez le Chapitre 4 à la page 39). Par défaut, c'est le niveau recommandé qui est activé.

Vous pouvez personnaliser n'importe lequel de ces niveaux de protection. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**. Les paramètres utilisateur ne seront pas sauvegardés après le rétablissement de l'un des trois niveaux prédéfinis.

Vous pouvez consulter et modifier les paramètres du niveau sélectionné dans la fenêtre **Configuration de la protection en temps réel du courrier**(cf. ill. 19) qui s'ouvre lorsque vous avez cliqué sur **Configuration** dans l'onglet **Courrier** (cf. ill. 18).

La partie supérieure de l'onglet contient des cases qui définissent les objets à analyser. Lorsque la case est cochée, le logiciel intercepte et analyse les objets correspondants :

- **Analyser le courrier reçu via le protocole POP 3** : analyse le courrier entrant transmis par le protocole POP3 pour n'importe quel client de messagerie.
- **Analyser le courrier entrant de Microsoft Office Outlook** : analyse le courrier entrant de Microsoft Office Outlook reçu par n'importe quel protocole de messagerie.
- **Analyser le courrier envoyé via le protocole SMTP** : analyse le courrier sortant transmis par le protocole SMTP pour n'importe quel client de messagerie.
- **Analyser le courrier sortant de Microsoft Office Outlook** : analyse le courrier sortant de Microsoft Office Outlook envoyé par n'importe quel protocole de messagerie.
- **Analyser les archives en pièce jointe** : analyse les archives en pièce jointe.

  

  Nous attirons votre attention sur le fait que l'exclusion des archives en pièce jointe ne s'applique pas aux archives auto-extractibles qui sont toujours analysées quel que soit le niveau d'intégration.

- **Analyser les bases de messagerie en pièce jointe** : analyse des bases de messagerie en pièce jointe.

La section **Configuration des ports** vous permet de définir la valeur des ports POP3 et SMTP par lesquels le transfert des données est réalisé. Il s'agit par

défaut des ports 110 et 25. Si votre client de messagerie utilise d'autres ports, il conviendra de les utiliser.

De plus vous pouvez limiter la durée de l'analyse et la taille de l'objet analysé.

- **Ne pas analyser les messages de plus de (Ko)** : pour définir la taille maximale des objets à analyser, définissez la taille maximale en Ko.
- **Arrêter l'analyse si elle dure plus de (s.)**. Définissez la durée maximale de l'analyse en secondes pour limiter celle-ci.

La section **Accélération de l'analyse des objets** vous donne la possibilité de recourir ou non aux technologies d'accélération de l'analyse : cochez la case **Utiliser la technologie iChecker™** pour activer l'utilisation de cette technologie.

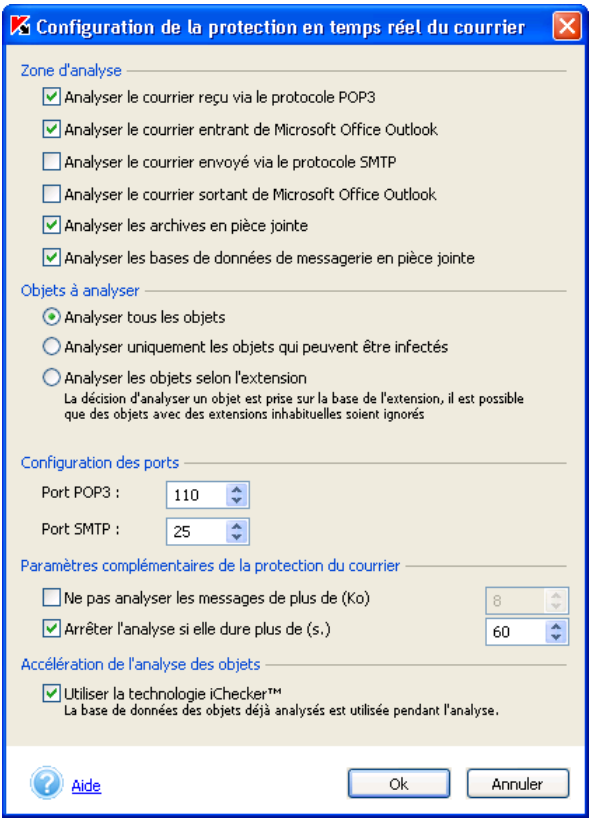

Illustration 19. Configuration détaillée de l'analyse du courrier

5.2.2.2. Sélection de l'action à réaliser sur l'objet découvert

Sélectionnez, dans la section **Actions à exécuter sur les objets découverts** (cf. ill. 18), l'action qui sera exécutée en cas de découverte d'un objet suspect ou infecté :

- *Réparer, supprimer si la réparation n'est pas impossible* : répare l'objet suspect. Si l'objet ne peut être réparé, il sera supprimé.
- *Mettre en quarantaine* : place l'objet suspect dans le répertoire de quarantaine dans l'attente d'une nouvelle analyse à l'aide de bases antivirus actualisées, d'une restauration, de l'envoi aux experts de Kaspersky Lab pour examen ou de la suppression.
- *Supprimer* : supprime l'objet infecté ou suspect. Le choix de cette action entraîne la création d'une copie de sauvegarde de l'objet qui sera placée dans le répertoire de sauvegarde. Cette copie pourra servir à la restauration du fichier ou pourra être envoyée à Kaspersky Lab pour examen.

5.2.3. Analyse du courrier de Microsoft Office Outlook

L'analyse du courrier de Microsoft Office Outlook s'opère grâce à un module spécial intégré à Microsoft Office Outlook. Il est prévu pour l'analyse de tout le courrier entrant (messages et pièces jointes) avant la lecture et l'analyse de tout le courrier sortant avant l'envoi.

Afin d'ouvrir la fenêtre d'analyse du courrier, sélectionnez, dans le menu principal de Microsoft Outlook, l'élément **Service → Paramètres**. Dans la fenêtre **Paramètres**, sélectionnez l'onglet **Kaspersky Anti-Virus** (cf. ill. 20).

La section **Etat** reprend les informations relatives à l'état du module d'analyse du courrier. Les informations suivantes peuvent apparaître en fonction de l'état :

- *L'analyse du courrier est activée*. Ce message apparaît lorsque Kaspersky Anti-Virus tourne et que l'analyse du courrier de Microsoft Office Outlook est activée.
- L'analyse du courrier entrant est activée. Ce message apparaît lorsque seule l'analyse du courrier entrant est activée.
- *L'analyse du courrier sortant est activée*. Ce message apparaît lorsque seule l'analyse du courrier sortant est activée.

- *L'analyse du courrier est désactivée*. Ce message apparaît lorsque l'analyse du courrier entrant et sortant de Microsoft Outlook est désactivée ou lorsque Kaspersky Anti-Virus ne tourne pas.

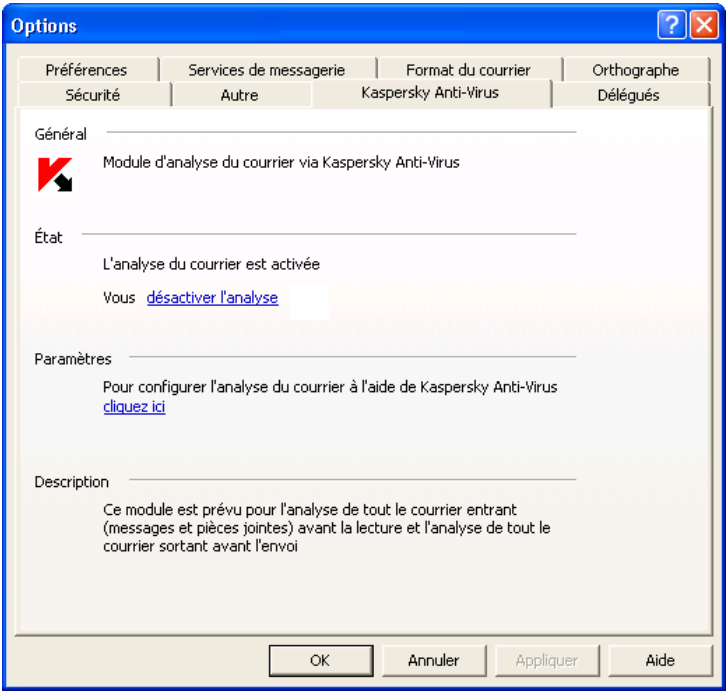

Illustration 20. Onglet Kaspersky Anti-Virus dans Microsoft Office Outlook

Pour configurer l'analyse du système de messagerie, utilisez le lien cliquez ici dans la section **Paramètres**. Si vous travaillez avec les paramètres utilisateur, La fenêtre de la configuration de la protection en temps réel s'ouvrira sur l'onglet **Courrier** (cf. ill. 18).

La boîte de dialogue de configuration de la protection en temps réel s'ouvre uniquement si la case **Afficher l'interface utilisateur** de l'onglet **Général** (cf. ill. 58) est cochée dans la fenêtre des options avancées de Kaspersky Anti-Virus.

Les utilisateurs d'un poste de travail verront uniquement dans cette fenêtre l'état « **L'analyse du courrier est activée/désactivée** » sur l'onglet **Kaspersky Anti-Virus** (cf. ill. 20). La zone de configuration n'est pas active.

5.2.4. Analyse des macros

En mode de protection en temps réel lorsque la protection contre les macros est installée et activée, Kaspersky Anti-Virus analyse le code déterminé des macros VBA et empêche l'exécution du code malicieux.

La configuration de l'analyse des macros s'opère sur l'onglet **Macros** (cf. ill. 22) dans la fenêtre **Configuration de la protection en temps réel**.

La protection contre les scripts est activée par défaut. Pour la désactiver, il faut décocher la case **Activer l'analyse des macros VBA**.

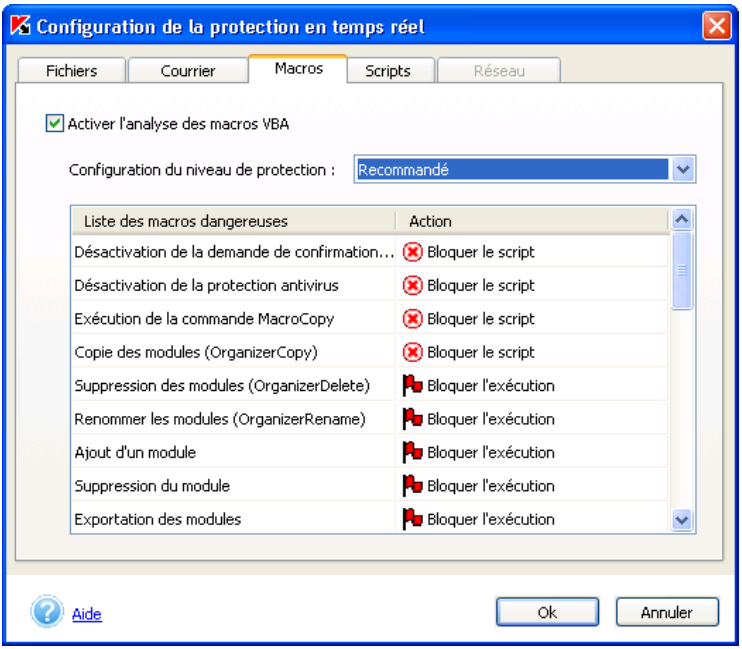

Illustration 21. Paramètre pour l'analyse des macros

Sélectionnez dans le menu déroulant **Configuration du niveau de protection** l'un des trois niveaux prédéfinis par les experts de Kaspersky Lab (pour de plus amples informations, consultez le Chapitre 4 à la page 39).

Les macros surveillées par le logiciel et l'action prévue pour chaque commande en fonction du niveau de protection défini sont reprises dans le tableau.

Autoriser l'exécution : autorise l'exécution des macros et ne prévoit aucune action.

Confirmer l'action : affiche à l'écran une demande de confirmation de l'exécution de l'action. Toutes les actions applicables à cette macro seront reprises dans ce message.

Bloquer l'exécution : bloque l'exécution des macros.

Bloquer le script : arrête l'exécution du script tournant dans la macro.

Vous pouvez personnaliser n'importe lequel de ces niveaux de protection. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**. Les paramètres utilisateur ne seront pas sauvegardés après le rétablissement de l'un des trois niveaux prédéfinis.

Afin de modifier les actions qui seront exécutées par Kaspersky Anti-Virus en cas de découverte d'une macro suspecte :

Sélectionnez la macro correspondante dans le tableau en cochant la case dans la colonne **Action** et sélectionné une des actions reprises dans la liste déroulante.

5.2.5. Analyse des scripts

La protection de votre ordinateur contre les scripts dangereux est garantie uniquement si vous avez décidé d'utiliser cette technologie lors de l'installation du programme.

Si l'analyse des scripts est activée en mode de protection en temps réel, Kaspersky Anti-Virus analyse les scripts VBScript et JavaScript avant leur exécution par le module de traitement des scripts du système d'exploitation et empêche l'exécution du code malicieux.

La configuration de l'analyse des macros s'opère sur l'onglet **Scripts** (cf. 22) dans la fenêtre **Configuration de la protection en temps réel**

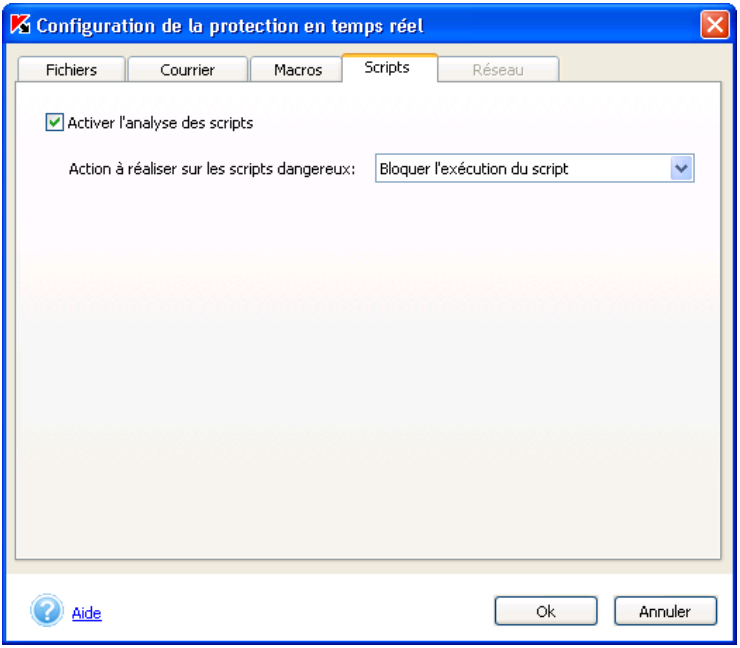

Illustration 22. Paramètres de la protection contre les scripts

La protection contre les scripts est activée par défaut. Pour la désactiver, il faut décocher la case **Activer l'analyse des scripts**.

Indiquez l'action qui sera réalisée par Kaspersky Anti-Virus en cas de découverte d'un script dangereux :

- **Confirmer l'action auprès de l'utilisateur** : affiche l'avertissement de la découverte d'un script représentant un danger potentiel et demande à l'utilisateur de confirmer l'action à réaliser. Toutes les actions envisageables seront reprises dans ce message.
- **Bloquer l'exécution du script** : bloque le lancement des scripts.
- **Autoriser l'exécution du script** : autorise le lancement des scripts.

Pendant l'analyse des scripts, l'icône clignotante de Kaspersky Anti-Virus apparaît dans la barre d'état de Microsoft Internet Explorer.

5.2.6. Protection contre les attaques de réseau

La protection de votre ordinateur contre les attaques de réseau est garantie uniquement si vous avez décidé d'utiliser cette technologie lors de l'installation du programme.

Kaspersky Anti-Virus protège votre ordinateur contre les attaques de pirates informatiques via le réseau local ou Internet.

L'identification des attaques de pirates s'opère grâce à l'utilisation d'une base de données reprenant les attaques connues à l'heure actuelle. Ces bases sont mises à jour et installées avec les bases antivirus (pour de plus amples informations, consultez le point 5.1 , à la page 44).

La protection contre les attaques de réseau est lancée au démarrage de Kaspersky Anti-Virus et analyse toutes les données reçues quelle que soit la source : réseau local ou Internet.

Dès qu'une tentative d'attaque est décelée, elle est immédiatement bloquée. Le message de circonstance apparaîtra à l'écran (cf. ill. 23) et fournira des informations sur le type d'attaque, l'adresse IP de l'ordinateur attaquant et le port local (si possible).

La configuration de la protection en temps réel contre les attaques de réseau s'opère sur l'onglet **Réseau** de la boîte de dialogue **Configuration de la protection en temps réel** (cf. ill. 24).

Lors de l'activation/désactivation de la protection en temps réel au départ du menu contextuel de Kaspersky Anti-Virus (cf. point 5.2 , p. 56), la protection contre les attaques de réseau est également désactivée.

Si vous souhaitez désactiver uniquement la protection contre les attaques de réseau, sans pour autant désactiver les autres tâches de la protection, désélectionnez la case **Activer la protection en temps réel contre les attaques de réseau** (cf. ill. 24). Le redémarrage de l'ordinateur s'impose en cas d'activation/de désactivation de la protection.

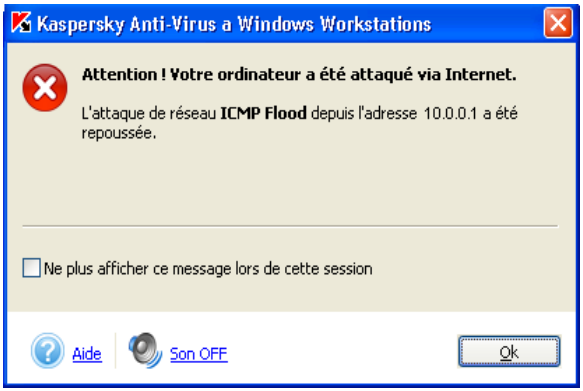

Illustration 23. Notification d'une attaque de réseau

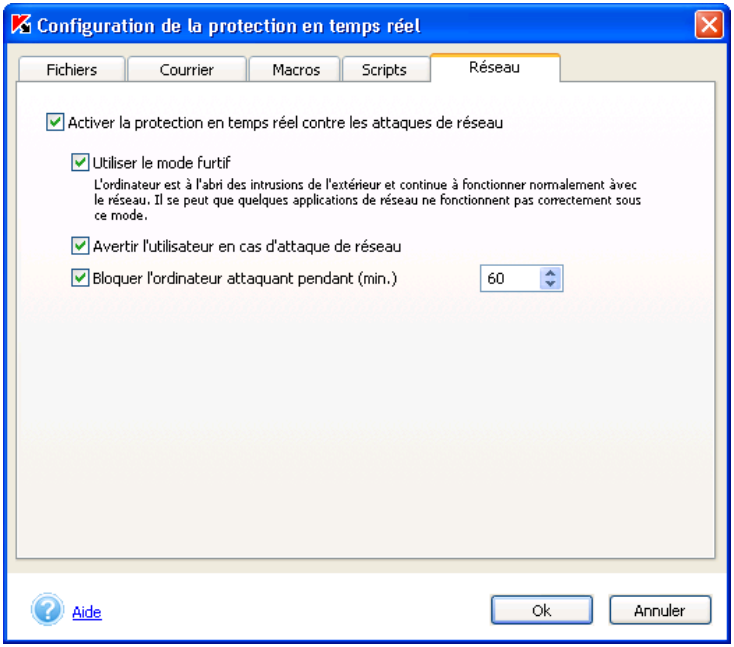

Illustration 24. Configuration de la protection en temps réel contre les attaques de réseau

Vous pouvez définir les paramètres de Kaspersky Anti-Virus applicables à la protection en temps réel contre les attaques de réseau :

- *Mode furtif*. Ce mode autorise uniquement les activités réseau initialisées par l'utilisateur ou par un des logiciels installés sur son ordinateur. Toutes les autres activités (connexion à distance à votre ordinateur, etc.) sont interdites. Cela signifie que votre ordinateur devient en quelque sorte « invisible » pour le monde extérieur. Le mode furtif permet également de déjouer n'importe quel type d'attaque par déni de service (DoS). Ce mode de fonctionnement n'a aucune répercussion négative sur votre utilisation d'Internet. Kaspersky Anti-Virus autorise les activités réseau qui émanent de l'utilisateur.

  

  Attention ! Le mode furtif ne vous met pas à l'abri des chevaux de Troie !

  Le mode furtif est désactivé par défaut. Pour l'activer, cochez la case **Utiliser le mode furtif**.

- *Notifications sur les attaques de réseau*. Par défaut, le logiciel vous avertit chaque fois qu'il détecte une tentative d'attaque sur votre ordinateur. L'écran affiche alors une boîte de dialogue (cf. ill. 23) qui reprend le type d'attaque exécutée, l'adresse IP d'origine et le port local victime (s'il est possible de définir cette information). Dans la mesure où ce message revêt un caractère purement informatif, vous pouvez désactiver son affichage en désélectionnant la case **Avertir l'utilisateur en cas d'attaque de réseau**; dans ce cas, les informations relatives aux attaques seront consignées dans le rapport.

- *Blocage de l'ordinateur à l'origine de l'attaque*. Kaspersky Anti-Virus peut bloquer tous les ordinateurs qui tentent d'attaquer le vôtre. Par défaut, le blocage de l'ordinateur à l'origine de l'attaque est désactivé. Si vous décidez de l'activer, il sera limité à 60 minutes. Pendant cette période, l'ordinateur à l'origine de l'attaque ne pourra pas établir de connexion de réseau avec votre ordinateur. Pour modifier cette durée, saisissez la valeur souhaitée pour le paramètre **Bloquer l'ordinateur attaquant pendant (min.)**. Désélectionnez la case à côté de ce paramètre si vous souhaitez désactiver cette fonction.

5.3. Analyse à la demande

L'analyse des objets à la demande est un mode de fonctionnement qui permet à l'administrateur ou à l'utilisateur d'un poste de travail de rechercher quand il le souhaite la présence d'éventuels virus, de supprimer les objets infectés et de mettre en quarantaine les objets suspects.

Grâce à Kaspersky Anti-Virus, vous pouvez réaliser soit une analyse complète de l'ordinateur ou soit une analyse de disques, de fichiers ou de répertoires particuliers. De plus, les objets dangereux découverts sont réparés ou supprimés tandis que les objets suspects sont placés en quarantaine.

Lors de l'installation de l'application, les tâches systèmes liées à l'analyse à la demande sont créées par défaut :

- **Analyser mon poste de travail** : analyse complète de tout le système de fichiers de l'ordinateur (cf. point 5.3.1, p. 76); par défaut, l'analyse est lancée chaque vendredi à 20h00.
- **Analyse les disques amovibles** : analyse des disques amovibles (disquettes, cédérom, cartes Flash, etc.); cette analyse est lancée manuellement par défaut (cf. point 5.3.5, p. 90).
- **Analyse des secteurs critiques** : analyse de la mémoire système, des objets de démarrage, des secteurs d'amorçage des disques ainsi que des répertoires système *Windows* et *Windows/system 32*; par défaut, cette analyse est lancée manuellement par l'utilisateur.
- **Analyse de la quarantaine** : analyse des objets placés en quarantaine; par défaut, elle est lancée manuellement par l'utilisateur.
- **Analyse au démarrage de Kaspersky Anti-Virus** : analyse des objets de démarrage, de la mémoire système et des secteurs d'amorçage; cette analyse est lancée par défaut au démarrage du système d'exploitation.

Il est possible également d'analyser un objet indiqué par l'utilisateur (cf. point 5.3.2, p. 78). De plus, vous pouvez vous-même créer des tâches complémentaires d'analyse des objets à la demande (cf. point 5.6, p. 97).

Pour que la réparation des bases de messagerie de Microsoft Outlook réussisse, il faut quitter Microsoft Outlook Express.

5.3.1. Analyse complète de l'ordinateur

L'analyse complète est capable d'analyser un nombre plus élevé d'objets que la protection en temps réel. Il est donc conseillé de l'effectuer au moins une fois par semaine à titre préventif.

Le logiciel vous avertira lorsqu'il est indispensable de lancer cette analyse. Au cas où la fenêtre principale du logiciel serait fermée, un message vous invitant à lancer immédiatement l'analyse complète de l'ordinateur apparaîtra au-dessus de l'icône de Kaspersky Anti-Virus dans la barre des tâches (pour autant que cette option n'ait pas été désactivée, cf. point 5.10.4, p. 120).

Pour obtenir de plus amples informations, il suffira d'ouvrir la fenêtre principale de l'application et de sélectionner l'onglet **Protection** (cf. ill. 2). La partie droite reprend l'état exact de l'analyse complète. Il existe trois états possibles :

L'analyse complète a été réalisée récemment ou est en cours d'exécution;

Il est temps de procéder à l'analyse complète, non sans avoir au préalable rétabli la configuration recommandée par les experts de Kaspersky Lab.

Vous devez *réaliser sans plus attendre l'analyse complète de votre ordinateur*.

Le cas échéant, vous pouvez lancer directement l'analyse complète en cliquant sur procéder à l'analyse complète.

Les experts de Kaspersky Lab conseillent de programmer le lancement de l'analyse complète. L'état de l'analyse indique notamment si ce mode est activé ou non.

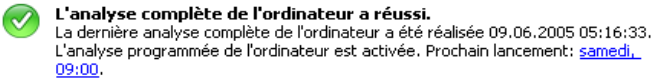

Illustration 25. Informations relatives à l'actualités de l'analyse

*Afin de lancer l'analyse à la demande de l'ordinateur, rendez-vous dans l'onglet **Protection** et sélectionnez dans la partie gauche :*

- Analyser le Poste de travail : lance l'analyse complète de l'ordinateur conformément aux paramètres définis (voir ci-après). Le même résultat s'obtient en cliquant sur le lien procéder à l'analyse complète dans la partie droite de l'onglet **Protection** ou en sélectionnant le point **Analyser mon Poste de travail** dans le menu contextuel qui apparaît après avoir fait un clic-droit sur l'icône dans la barre des tâches.

La fenêtre **Analyse** (cf. ill. 5) apparaît ensuite. Elle illustre l'avancement (en pour cent) de l'analyse, le nom de l'objet analysé, l'heure estimée de fin de l'analyse et des statistiques générale sur le nombre d'objets analysés à ce moment, ainsi que sur le nombre d'objets réparés, supprimés et placés en quarantaine.

Dans le cadre de l'analyse complète de l'ordinateur, les boîtes aux lettres, les disques amovibles et les disques de réseau (s'ils sont connectés à votre ordinateur) sont ignorés.

Vous pouvez fermer la fenêtre d'analyse en cliquant sur dans le coin supérieur droit ou en sélectionnant l'option **Fermer la fenêtre, poursuivre l'analyse** dans la fenêtre qui s'ouvre.

Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 5.10.2 à la page 115).

5.3.2. Analyse d'objets individuels

Vous pouvez sélectionner des objets individuels à analyser au départ de Kaspersky Anti-Virus ou à l'aide des méthodes Microsoft Windows traditionnelles (ex. : dans la fenêtre de l'**Assistant** ou au départ du **Bureau**, etc.).

Pour sélectionner l'objet à analyser au départ de Kaspersky Anti-Virus :

Cliquez sur le lien Analyser les objets dans la partie gauche de l'onglet **Protection** (cf. ill. 2).

La boîte de dialogue **Sélection des objets à analyser** (cf. ill. 26) qui apparaît reprend une liste des objets qui peuvent être analysés, ainsi qu'un bouton de modification du contenu de la liste et un bouton de gestion de l'analyse.

La liste originale reprend les éléments suivants :

- Les disques amovibles (y compris les disquettes et les CD-rom) ;
- Les disques durs ;
- Les disques de réseau (si ceux-ci sont connectés à votre ordinateur);
- Les boîtes aux lettres Microsoft Office Outlook et Microsoft Outlook Express ;
- Le dossier **Mes documents**;
- La mémoire système;
- Les objets de démarrage ;
- Les secteurs d'amorçage des disques.

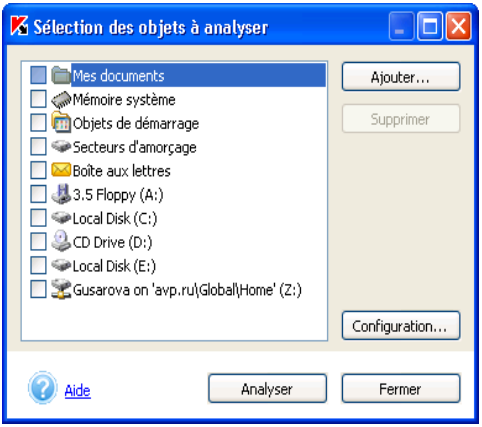

Illustration 26. Sélection des objets à analyser

Cliquez sur **Ajouter…** pour ajouter de nouveaux objets à la liste et sélectionnez le dossier ou le fichier souhaité. Tous les objets que vous aurez ajoutés à la liste seront préservés jusqu'à la prochaine analyse.

Au moment de la création du chemin d'accès au répertoire ou à l'objet, vous pouvez utiliser les variables système. Par exemple, vous pouvez sélectionner pour l'analyse le répertoire d'installation de Microsoft Windows en saisissant **%windir%** en tant que variable.

Pour effacer un objet de la liste, sélectionnez-le et cliquez sur **Supprimer**. Sachez cependant que vous ne pouvez supprimer que les objets que vous aurez ajoutés manuellement. Les objets présents dans la liste d'origine ne peuvent être supprimés.

Si vous souhaitez modifier les paramètres de l'analyse à la demande, cliquez sur **Configuration…** (pour de plus amples informations, consultez le point 5.3.3 à la page 80). Les paramètres saisis seront conservés pour les analyses suivantes de la liste d'objets ainsi que pour les objets sélectionnés via Microsoft Windows.

Pour analyser simultanément plusieurs objets de la liste :

1. Sélectionnez les objets dans la liste ;
2. Cliquez sur **Analyser**.

Pour analyser l'objet sélectionné au départ de Microsoft Windows :

Placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 27). Lors de l'analyse,

les paramètres repris dans la fenêtre **Sélection des objets à analyser** (cf. ill. 26) seront utilisés.

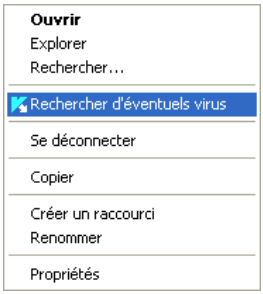

Illustration 27. Recherche d'éventuels virus dans un objet au départ de Microsoft Windows

Si Kaspersky Anti-Virus n'est pas lancé, vous devrez le faire au moment de lancement de l'analyse de l'objet sélectionné au départ de Microsoft Windows.

Quel que soit le moyen utilisé pour lancer l'analyse de l'objet (depuis le menu contextuel dans Microsoft Windows ou depuis la liste d'objet de Kaspersky Anti-Virus), la fenêtre **Analyse** (cf. ill. 5) s'ouvre. Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 5.10.2 à la page 115).

Si l'analyse d'un objet quelconque doit être réalisée fréquemment, vous pouvez créer la tâche correspondante d'analyse à la demande (pour de plus amples informations, consultez le point 5.6 à la page 97).

5.3.3. Configuration de l'analyse à la demande

Pour consulter ou modifier les paramètres de l'analyse à la demande :

Cliquez sur le lien Analyse à la demande dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3).

Cette action entraîne l'ouverture de la boîte de dialogue **Analyse à la demande** (cf. ill. 28) qui contient la liste des tâches système et la liste des tâches définies par l'utilisateur.

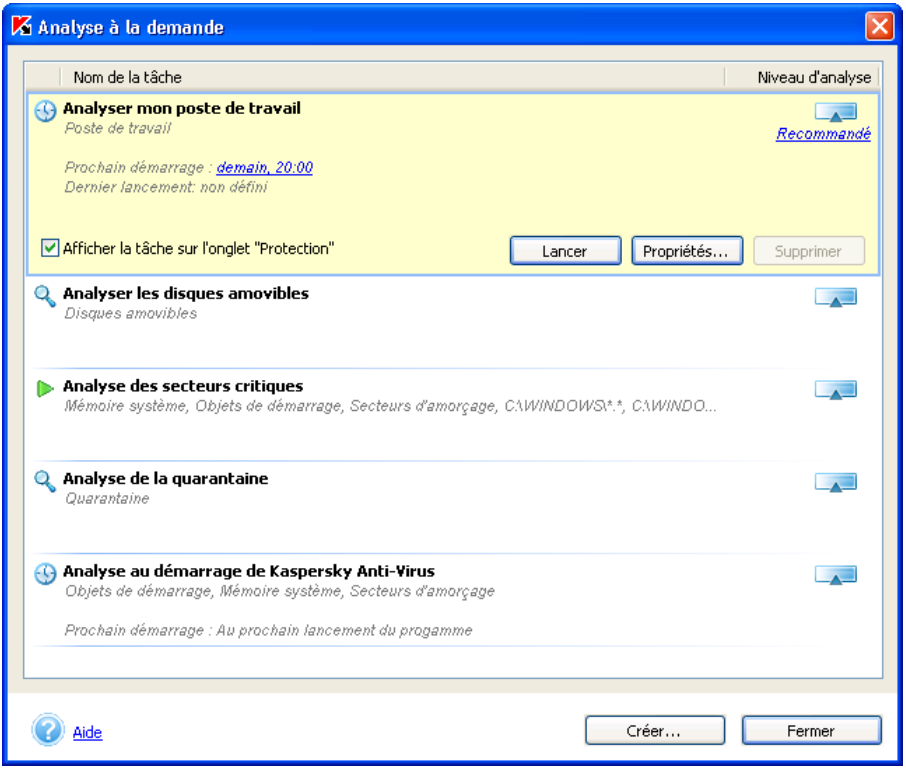

Illustration 28. Liste des analyses à la demande

En cliquant sur le nom de la tâche, vous ouvrez un bloc contenant les informations relatives au secteur d'analyse ainsi qu'à l'heure du dernier et du prochain lancement de l'analyse. Grâce au bouton **Ouvrir** de ce bloc, vous pouvez lancer manuellement l'analyse à la demande et à l'aide du bouton **Comportement…**, vous pouvez ouvrir la fenêtre de configuration de l'analyse (cf. ill. 29) et définir les paramètres suivants :

- sélectionner les objets à analyser. La sélection est possible pour les tâches créées manuellement. Pour ajouter un nouvel objet, cliquez sur **Ajouter** et sélectionnez-le dans la liste déroulante. Pour analyser un objet qui n'est pas repris dans la liste, par exemple un répertoire ou un fichier distinct, sélectionnez **Parcourir** dans la liste et indiquez le chemin d'accès à l'objet en question. Pour supprimer un objet, sélectionnez-le dans la liste et cliquez sur **Supprimer**;
- Définir le niveau de la protection antivirus et procéder à une configuration détaillée du niveau sélectionné (cf. point 5.3.3.1, p. 83) ;

- Dresser la liste des objets qui ne seront pas analysés (cf. point 5.7, p. 99) ; Pour ouvrir la fenêtre de constitution de la liste des exclusions, cliquez sur non défini/ défini dans la description des paramètres de protection définis. L'aspect des liens change en fonction de la définition ou non d'exclusions ;
- Définir l'action qui sera exécutée par Kaspersky Anti-Virus en cas de découverte d'objets dangereux et suspects (cf. point 5.3.3.2, p. 86).
- Programmer le lancement automatique de l'analyse (cf. point 5.7, page 99).
- Configurer le lancement d'une tâche avec les privilèges d'un autre utilisateur (uniquement pour les ordinateurs tournant sous Microsoft Windows NT/2K/XP) (cf. point 5.9, p. 107).

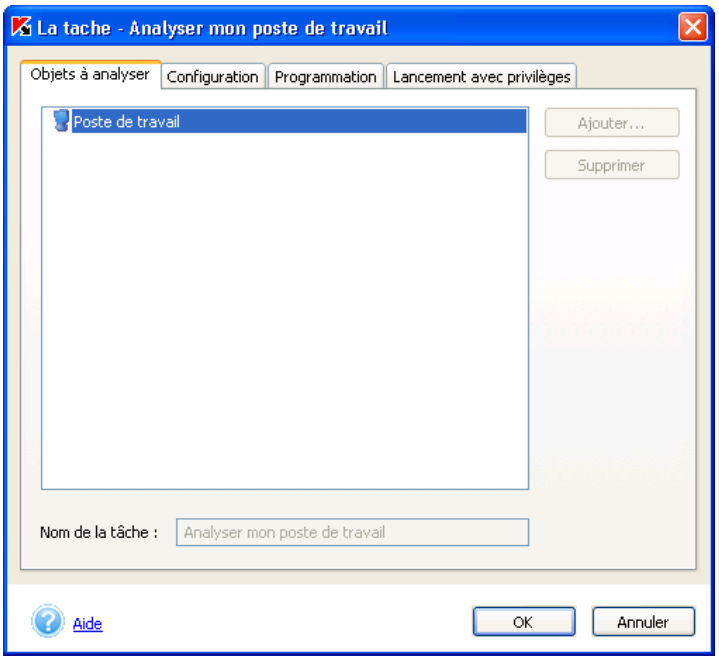

Illustration 29. Fenêtre de configuration de l'analyse à la demande. Onglet **Objets à analyser**

Si vous avez l'intention d'exécuter une tâche fréquemment, il est conseillé de cocher la case **Illustrer la tâche sur l'onglet "Protection"** dans le bloc d'informations relatives à la tâche. Ainsi, vous pourrez lancer la tâche rapidement en cliquant sur le lien portant son nom dans la partie gauche de l'onglet **Protection** (cf. ill. 2).

En fonction de la situation les icônes suivantes peuvent apparaître à gauche du nom de la tâche :

 indique que cette tâche a été programmée pour être exécutée automatiquement.

 indique que cette tâche est en cours d'exécution.

Afin de créer d'autres tâches d'analyse, cliquez sur **Créer** dans la fenêtre **Analyse à la demande** (cf. ill. 28). Pour obtenir de plus amples informations sur la création d'une tâche, consultez le point 5.6 à la page 97.

Pour supprimer une tâche, sélectionnez-la dans la liste et cliquez sur **Supprimer**. Sachez cependant que vous pouvez uniquement supprimer les tâches que vous aurez ajoutées manuellement. Les tâches système ne peuvent être supprimées. De plus, il est impossible de supprimer une tâche en cours d'exécution.

5.3.3.1. Sélection du niveau d'analyse

Sélectionnez dans le menu déroulant **Configuration du niveau d'analyse** de l'onglet **Configuration** (cf. ill. 30) l'un des trois niveaux prédéfinis par les experts de Kaspersky Lab (pour de plus amples informations, consultez le Chapitre 4 à la page 39). Par défaut, c'est le niveau recommandé qui est activé pour l'analyse.

Vous pouvez personnaliser n'importe lequel de ces niveaux de protection. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**. Les paramètres utilisateur ne seront pas sauvegardés après le rétablissement de l'un des trois niveaux prédéfinis.

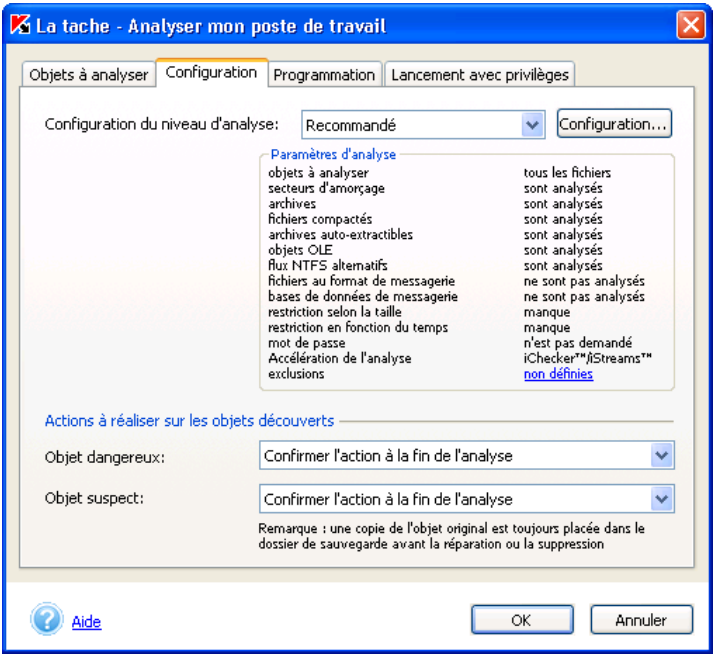

Illustration 30. Configuration de l'analyse à la demande

Vous pouvez consulter et modifier les paramètres du niveau sélectionné dans la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 31) qui s'ouvre lorsque vous avez cliqué sur **Configuration…** (cf. ill. 30).

Sélectionnez, dans la section **Objets à analyser**, les objets qui seront soumis à l'analyse de Kaspersky Anti-Virus :

- **Analyser tous les objets** : analyse tous les objets sans tenir compte de leur type et de leur extension.
- **Analyser uniquement les objets qui peuvent être infectés** : analyse les objets qui présentent un risque d'infection ; l'analyse s'opère sur la base de la structure interne du fichier.
- **Analyser les objets en fonction de l'extension** : analyse les fichiers qui présentent un risque d'infection ; l'analyse s'opère sur la base de l'extension du fichier.

Vous pouvez définir si les objets suivants seront analysés dans la section **Paramètres complémentaires de l'analyse** :

- Les secteurs d'amorçage;

- Les archives ;
- Les fichiers exécutables compactés ;
- Les archives auto-extractibles ;
- Les objets associés ou intégrés à d'autres fichiers (les objets OLE) ;
- Les flux NTFS alternatifs ;
- Les fichiers au format de messagerie ;
- Les bases de messagerie.

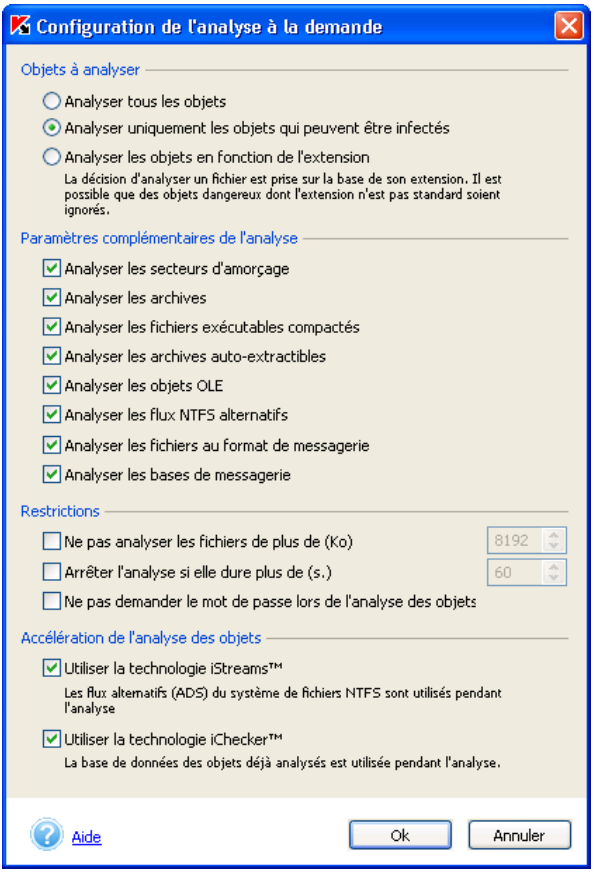

Illustration 31. Configuration détaillée de l'analyse à la demande

Cochez les cases souhaitées dans la section **Restrictions** :

- **Ne pas analyser les fichiers de plus de (Ko)** : pour définir la taille maximale des objets à analyser, définissez la taille maximale en Ko.
- **Arrêter l'analyse si elle dure plus de (s.)**. Définissez la durée maximale de l'analyse en secondes pour limiter celle-ci.
- **Ne pas demander le mot de passe lors de l'analyse des objets** afin que le mot de passe ne soit pas demandé lors de l'analyse d'objets protégés par un mot de passe. Si cette case est cochée, les objets protégés par un mot de passe seront ignorés lors de l'analyse antivirus.

La section **Accélération de l'analyse des objets** vous donne la possibilité de recourir ou non aux technologies d'accélération de l'analyse iChecker™ et iStreams™. Pour utiliser ces technologies, il suffit simplement de cocher les cases correspondantes.

Si pendant l'installation du logiciel vous avez décidé de ne pas utiliser la technologie iStreams™, vous devrez réinstaller Kaspersky Anti-Virus si vous souhaitez activez cette technologie. Tant que cela ne sera pas fait, il ne sera pas possible de configurer cette fonction.

5.3.3.2. Sélection de l'action à réaliser sur l'objet découvert

Sélectionnez, dans les sections **Actions à exécuter sur les objets suspects/infectés**, le type d'action qui sera exécuté en cas de découverte d'objets suspects ou infectés :

- **Confirmer l'action à la fin de l'analyse** : propose de traiter les objets dangereux à la fin de l'analyse. Ce mode est activé par défaut et ne requiert pas votre présence permanente à proximité de l'ordinateur. Dans la mesure où une analyse peut durer longtemps nous vous conseillons d'utiliser ce mode lorsque vous ne pouvez pas contrôler le traitement des objets au fur et à mesure de leur découverte.
- **Confirmer l'action auprès de l'utilisateur** :le logiciel affiche une boîte de dialogue vous permettant de décider de la suite des opérations. Cette boîte de dialogue reprend **toutes** les options possibles, dont une recommandée par les experts de Kaspersky Lab. Sélectionnez ce mode si vous avez l'intention de rester à proximité de votre ordinateur pendant l'analyse.
- **Exécuter l'action recommandée** : exécute **l'action** recommandée par les experts de Kaspersky Lab. Celle-ci est toujours fondée, si bien que ce mode est adapté à la majorité des cas. Les recommandations sont les suivantes :

- *Réparer* l'objet infecté; supprimer si la réparation est impossible[5] ;
- *Mettre* l'objet potentiellement infecté par un virus ou l'une de ses variantes *en quarantaine*.

Il arrive parfois, lors de la mise en quarantaine d'un fichier, qu'un message apparaisse et indique que l'objet ne peut être supprimé. Cela est du au fait que les objets mis en quarantaine sont déplacés : ils sont copiés dans le répertoire de quarantaine et supprimés de leur répertoire d'origine. Toutefois, il n'est pas possible de supprimer tous les objets déplacés, comme les objets utilisés à ce moment par une application quelconque.

- *Supprimer* l'objet dangereux s'il s'agit d'un cheval de Troie ou d'un ver.

Si l'objet infecté/potentiellement infecté est un riskware, il est ignoré.

- **Réparer, supprimer si la réparation est impossible:** tente de réparer l'objet dangereux. Si la réparation échoue, l'objet est supprimé. Dans ce cas, les objets présentant un risque potentiel sont également soumis à la réparation et à la suppression si la réparation est impossible. Lors de la réparation, une copie de l'objet est préservée dans le dossier de sauvegarde.
- **Supprimer les objets** assure la suppression des objets dangereux découverts pendant l'analyse sans tenter de réparation ni demander de confirmation auprès de l'utilisateur. Une copie de l'objet est conservée dans le dossier de sauvegarde avant la suppression. Nous vous conseillons d'adopter ce mode uniquement si vous êtes certain que vous ne perdrez pas d'informations cruciales.

- **Consigner les informations dans le rapport** : aucune action n'est réalisée et les informations relatives à la l'infection sont simplement consignées dans le rapport. Il n'est pas conseillé d'utiliser ce mode fréquemment car les objets dangereux et malveillants demeurent sur votre ordinateur.

[5] Par défaut, les objets infectés de la mémoire vive sont supprimés et les secteurs de démarrage infectés sont réparés ou bloqués si la réparation est impossible.

Il peut arriver qu'il soit impossible d'exécuter l'action sur l'objet. C'est le cas par exemple lorsque l'objet est utilisé par une autre application au moment de l'analyse. Un message apparaîtra alors à l'écran (cf. ill. 32) et proposera les actions suivantes:

- *Réparer lors du redémarrage de l'ordinateur (recommandé)* . Cette action est exécutée uniquement lorsque la réparation de l'objet est possible.
- Supprimer lors du redémarrage de l'ordinateur;
- *Ignorer*. Aucune action n'est réalisée et les informations sont simplement consignées dans le rapport.

  Si vous fermez la fenêtre en cliquant sur le bouton dans le coin supérieur droit, l'action qui avait été sélectionnée ne sera pas exécutée et l'objet sera ignoré.

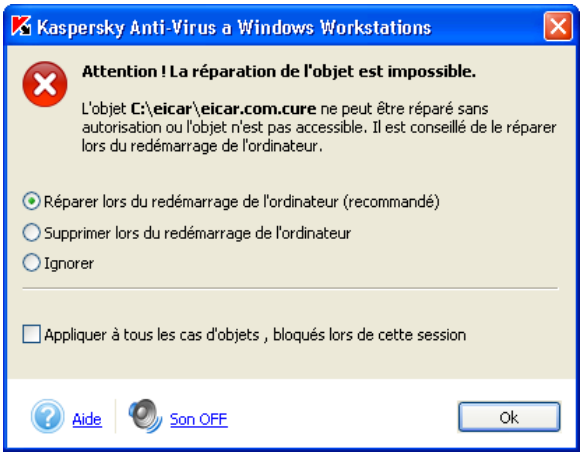

Illustration 32. La réparation immédiate de l'objet est impossible

5.3.4. Analyse des archives

Kaspersky Anti-Virus analyse les archives uniquement si le niveau **Sécurité maximale** ou **Recommandé** a été sélectionné et si l'analyse des archives n'a pas été désactivée (la case **Analyser les archives** de la **Fenêtre d'analyse à la demande** n'est pas sélectionnée, cf. ill. 30).

Kaspersky Anti-Virus analyse tous les objets à l'intérieur des archives et répare uniquement les objets dans les archives *zip, arj, cab, rar, lha* et *ice*.

Kaspersky Anti-Virus NE REPARE PAS les archives auto-extractibles !

Au cas où l'objet à l'intérieur de l'archive serait protégée par un mot de passe et que la demande du mot de passe aurait été activée, une boîte de dialogue pour la saisie du mot de passe (cf. ill. 33) apparaîtra avant son analyse. Si le mode de traitement différé des objets a été sélectionné (l'option **Confirmer l'action à la fin de l'analyse a été sélectionnée**, cf. point 5.3.3.2, p. 86), la requête du mot de passe apparaîtra à la fin de l'analyse.

La case **Ne pas demander le mot de passe lors de l'analyse des objets**, dans les paramètres de configuration de l'analyse, permet d'afficher ou non la fenêtre de saisie du mot de passe (cf. point 5.3.3.1, p. 83). Par défaut, la case est désélectionnée uniquement pour le niveau **Vitesse maximale**.

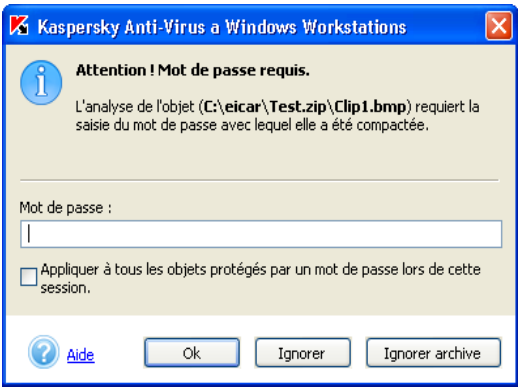

Illustration 33. Saisie du mot de passe pour l'analyse de l'archive

Saisissez dans le champ **Mot de passe** le mot de passe d'accès aux objets renfermés dans l'archive analysée puis cliquez sur **OK**. L'analyse antivirus de l'archive et des objets qu'elle contient se poursuivra.

Pour le traitement (réparation, suppression) des objets à l'intérieur d'une archive, Kaspersky Anti-Virus décompacte l'archive dans un dossier temporaire, analyse les objets qu'elle contient, les traite, les compacte sous le même nom et copie l'archive dans son emplacement original (écrase la copie existante). Le traitement des objets protégés par un mot de passe au sein d'une archive se déroule selon le même processus. La seule différence étant que les objets sont compactés sans mot de passe après le traitement.

Si Kaspersky Anti-Virus découvre pendant l'analyse une autre archive protégée, il tentera d'utiliser le mot de passe saisi pour l'analyse des objets de la première archive. La boîte de dialogue de saisie du mot de passe apparaîtra à nouveau à l'écran uniquement si ce premier mot de passe n'est pas valide.

Si vous ne connaissez pas le mot de passe, il sera impossible de procéder à l'analyse des objets repris dans l'archive protégée. Il est recommandé dans ce cas de cliquer sur **Ignorer** et de poursuivre.

Cliquez sur **Ignorer archive** afin d'exclure de l'analyse en cours tous les objets protégés par un mot de passe et repris dans l'archive analysée. Dans ce cas, tous les objets à l'intérieur de l'archive qui ne sont pas protégés par un mot de passe seront analysés et traités conformément aux paramètres de l'analyse antivirus.

La case **Appliquer à tous les objets protégés par un mot de passe lors de cette session** concerne l'action sélectionnée par la suite.

Ainsi, si vous cochez cette case et que vous aviez choisi **Ignorer**, **Ignorer archive**, les objets restants protégés par un mot de passe ne seront pas analysés. Par contre, si vous aviez saisi un mot de passe et cliquez sur **OK**, ce mot de passe sera appliqué à tous les objets restants sans que la boîte de saisie n'apparaisse.

Si l'archive ne peut être réparée et que l'option **Exécuter l'action recommandée** a été sélectionnée dans les paramètres de l'analyse, Kaspersky Anti-Virus ne supprimera pas l'archive mais se contentera de consigner sa découverte dans le rapport.

Si l'option **Confirmer l'action à la fin de l'analyse** ou **Confirmer l'action pendant l'analyse** (cf. point 5.3.3.2, p. 86) a été sélectionnée dans les paramètres de l'analyse, vous pourrez supprimer les fichiers qui ne peuvent pas être réparés en sélectionnant Supprimer dans la boîte de dialogue de requête de l'action. De plus, vous pouvez supprimer cette archive manuellement.

5.3.5. Analyse des disques amovibles

Vous pouvez lancer l'analyse des disques amovibles depuis la fenêtre principale de Kaspersky Anti-Virus ou depuis le menu contextuel de Microsoft Windows ouvert via l'**Assistant** ou le **Bureau.**

Pour analyser les disques amovibles au départ du menu contextuel de Microsoft Windows :

Sélectionnez les disques (il est possible de sélectionner directement le CD et la disquette), ouvrez le menu contextuel de Microsoft Windows d'un clic droit et choisissez **Rechercher d'éventuels virus** (cf. ill. 27).

Pour rechercher d'éventuels virus sur le CD ou la disquette au départ de la fenêtre principale de Kaspersky Anti-Virus :

1. Introduisez le CD ou la disquette dans le lecteur. Le logiciel est en mesure d'analyse le CD et la disquette en une session.
2. Cliquez sur le lien Analyser les disques amovibles dans la partie gauche de l'onglet **Protection** (cf. ill. 2). Ce lien est visible si la case **Illustrer la tâche sur l'onglet protection** a été cochée dans le bloc d'information de la tâche (cf. ill. 28).

   Ou

   Cliquez sur le lien Analyser les objets pour ouvrir la fenêtre **Sélection des objets à analyser** (cf. ill. 26). Sélectionnez les disques amovibles et cliquez sur **Analyser**.

   Ou

   Sélectionnez l'onglet **Paramètres** dans la fenêtre principale et cliquez sur Analyse à la demande. Cette action entraîne l'ouverture de la boîte de dialogue **Analyse à la demande** (cf. ill. 28). Sélectionnez **Analyser les disques amovibles** dans la liste des tâches et cliquez sur **Lancer**.

La fenêtre **Analyse** (см. ill. 5) apparaît à l'écran dès le lancement de l'analyse et illustre la progression de la tâche pour les objets sélectionnés dans la liste.

Si vous avez sélectionné un seul disque amovible, Kaspersky Anti-Virus vous proposera d'introduire le suivant à la fin de l'analyse.

Voici quelques caractéristiques du fonctionnement du logiciel auxquelles il convient de prêter attention.

- Si au moment de lancer l'analyse vous avez oublié d'introduire le disque ou la disquette ou si le lecteur ou le CD-ROM n'est pas branché, l'analyse n'aura pas lieu et le logiciel n'affichera aucun message à ce sujet.
- Les disquettes introduites dans le lecteur après le début de l'analyse ne seront pas analysées. Il en va de même pour les CD-ROM et les autres types de disques amovibles
- Si vous éjectez la disquette ou éteignez le disque amovible pendant l'analyse, le logiciel consignera l'erreur dans le rapport mais il n'affichera aucun message à ce sujet. Le logiciel passera, le cas échéant, à l'analyse du disque amovible suivant.

Lorsque le disque amovible est monté dans le système d'exploitation (lorsque celui-ci définit le disque en tant que nouveau périphérique), Kaspersky recherche

d'éventuels virus d'amorçage sur ce disque, pour autant que la protection en temps réel des fichiers soit activée.

5.4. Traitement des objets dangereux découverts

Les actions exécutées par Kaspersky Anti-Virus en cas de découverte d'un objet infecté, d'un programme malicieux ou d'un objet potentiellement infecté par un virus ou l'une de ses variantes dépendent entièrement et uniquement de la configuration de la protection en temps réel et de l'analyse à la demande. Ce chapitre aborde les situations où Kaspersky Anti-Virus vous propose un choix d'actions à exécuter sur un objet pendant l'analyse ou à la fin de celle-ci.

Cela se produit lorsque vous avez sélectionné :

- **Confirmer l'action auprès de l'utilisateur** (cf. point 5.2.1.2, p. 62) dans les paramètres de la protection en temps réel. Dans ce cas, la requête pour l'action s'affichera dès qu'un objet dangereux aura été découvert.
- dans les paramètres de l'analyse à la demande (cf. point 5.3.3.2, page 86).
    - **Confirmer l'action pendant l'analyse**. La sélection de l'action sur l'objet dangereux s'opère au moment de sa découverte par Kaspersky Anti-Virus.

  Ou

    - **Confirmer l'action à la fin de l'analyse.** La sélection de l'action sur les objets dangereux s'opère si vous avez lancé le traitement de ces objets en cliquant sur **Traiter** dans la fenêtre des résultats de l'analyse (cf. ill. 34).

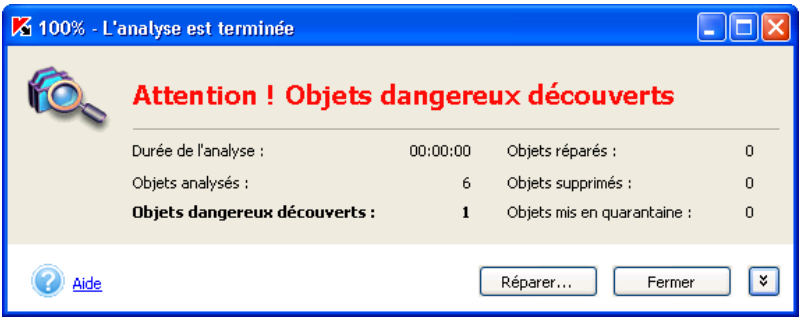

Illustration 34. Traitement différé des objets dangereux

Ainsi, lors de la découverte d'un objet dangereux, un message contenant les informations suivantes (cf. ill. 35) apparaît :

- Une description détaillée de l'objet avec le nom du programme dangereux;
- Une sélection des actions qui peuvent être exécutées sur l'objet. Cette sélection reprend toujours au moins une action recommandée par les experts de Kaspersky Lab. Le terme **(recommandé)** est repris à côté de cette action. Voici l'ensemble des actions possibles (les actions proposées en réalité dépendent du type d'objet découvert) :
    - **Réparer…** : tente de réparer l'objet si possible. Une copie de l'objet est conservée dans le dossier de sauvegarde avant la première réparation.
    - **Supprimer** : supprime l'objet infecté ou potentiellement infecté. Une copie de l'objet est conservée dans le dossier de sauvegarde avant la suppression.
    - **Ignorer** : aucune action n'est réalisée, seules les informations sont consignées dans le rapport.

      L'objet dangereux sera ignoré si vous fermez la boîte de dialogue relative à sa découverte en cliquant sur le bouton dans le coin supérieur droit.
    - **Mettre en quarantaine** : place l'objet potentiellement infecté par un virus ou l'une de ses modifications en quarantaine en vue d'une nouvelle analyse, d'une tentative de réparation ou de son envoi à Kaspersky Lab pour examen.
    - **Ignorer, ajouter aux exclusions** : ajouter le programme identifié aux exclusions de l'analyse et de la protection antivirus.

      Afin de pouvoir utiliser l'exclusion que vous avez ajoutée, il convient de cocher la case **Utiliser la liste générale des exclusions** dans la fenêtre **Liste des exclusions** (cf. ill. 38).

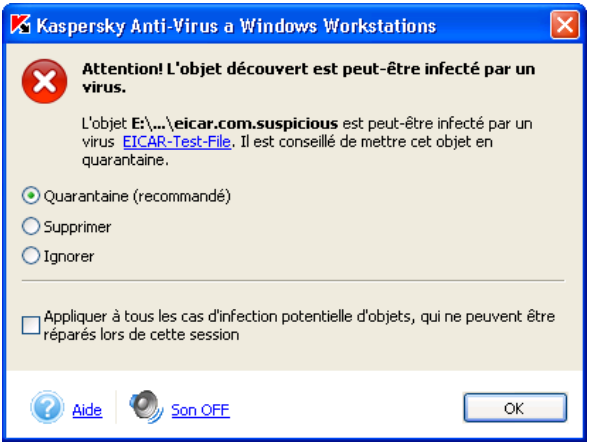

Illustration 35. Mesage relatif à la découverte d'un objet infecté

Vous pouvez appliquer l'action sélectionnée à tous les objets du même type en cochant la case adéquate. Ainsi, pour appliquer une action à tous les objets infectés qui ne peuvent être réparés, cochez ☑ **Appliquer à tous les cas d'infection potentielle d'objets, qui ne peuvent être réparés lors de cette session**.

Si pour une raison quelconque vous avez décidé de ne pas traiter un objet en cliquant sur **Ignorer**, sachez que vous pourrez le traiter ultérieurement. Pour ce faire, cliquez sur le lien traiter ces objets dans la partie droite de l'onglet **Protection**. Cette action entraîne l'ouverture de la boîte de dialogue Objets dangereux découverts (cf. ill. 36) qui contient une description détaillée de chacun des objets dangereux ainsi qu'un lien vers la description détaillée dans l'encyclopédie des virus à l'adresse www.viruslist.com/fr.

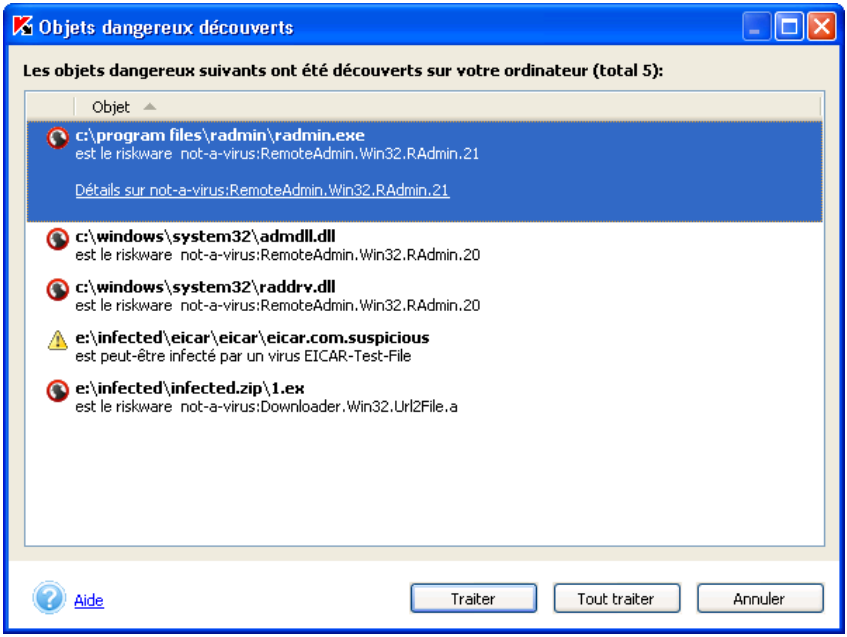

Illustration 36.Liste des objets dangereux découverts

Grâce au bouton **Traiter**, vous pouvez traiter l'objet sélectionné dans la liste. Le bouton **Tout traiter** vous permettra de traiter l'ensemble des objets de la liste. Cette action entraînera l'affichage de messages (cf. ill. 35) qui vous permettront de choisir l'action à réaliser sur l'objet (pour une description détaillée des actions envisageables, voir plus haut).

Pour supprimer un objet de la liste sans le traiter, utilisez la commande du menu contextuel **Supprimer de la liste** (cf. ill. 37).

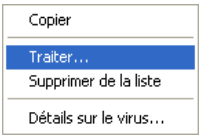

Illustration 37. Menu contextuel de la fenêtre **Objets dangereux découverts**

Si un objet dangereux quelconque a été supprimé manuellement, il disparaîtra de la liste des objets dangereux découverts lors de la tentative de traitement.

5.5. Contrôle de l'activité des processus des programmes

Kaspersky Anti-Virus vous permet de créer des listes de processus de programmes dont l'activité ne sera pas contrôlée.

Vous estimez par exemple que les objets utilisés par le **Bloc-Notes** de Windows sont inoffensifs et ne doivent pas être soumis à la protection en temps réel. En d'autres termes, vous faites confiance aux processus de ce logiciel. Pour exclure les objets utilisés par ce programme de l'analyse, ajoutez le **Bloc-Notes** à la liste des processus de confiance.

Pour constituer la liste des processus de confiance :

Cliquez sur non défini/défini à côté du paramètre processus de confiance dans la section **Paramètres de la protection** de l'onglet **Fichiers** (cf. ill. 16).

La boîte de dialogue **Liste des exclusions** s'affichera (cf. ill. 38). Vous pouvez compléter ou modifier la liste à l'aide des boutons situés à droite.

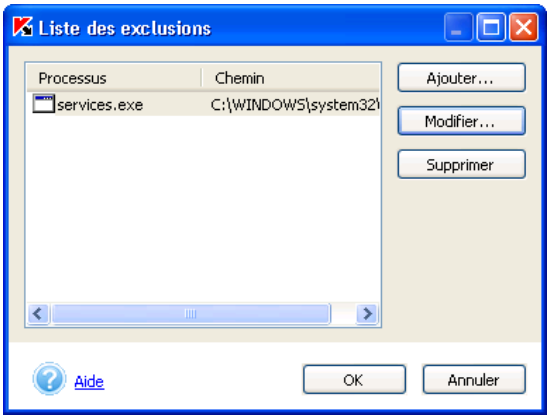

Illustration 38. Boîte de dialogue de constitution de la liste des processus de confiance

Grâce au bouton **Ajouter…**, vous pouvez ajouter à la liste des exclusions :

- *un fichier exécutable*. Cliquez sur **Parcourir…** et sélectionner le fichier avec l'extension **.exe**;

- *un processus lancé*. Pour ce faire, utilisez la commande **Processus lancés** et sélectionnez un des processus en cours dans la liste déroulante.

Pour supprimer un processus de la liste, sélectionnez-le et cliquez sur **Supprimer.**

Si vous cliquez sur **Modifier**, vous ouvrez une nouvelle fenêtre (cf. ill. 39).

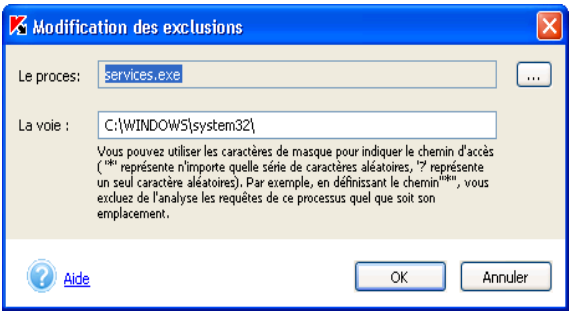

Illustration 39. Ajout d'un processus de confiance

Vous pouvez choisir le nom du processus à l'aide du bouton  . Lorsque le nom est sélectionné, Kaspersky Anti-Virus enregistre les attributs internes du fichier du processus grâce auxquels il pourra identifier le processus comme un processus de confiance lors de l'analyse antivirus.

Le chemin d'accès au fichier est saisi automatiquement lors de la sélection du nom. Vous pouvez le modifier manuellement.

En guise de chemin, saisissez le chemin d'accès complet au fichier du processus ou le masque ***** (n'importe quel quantité de caractères aléatoires) ou **?** (un symbole aléatoire).
Ainsi, l'utilisation du masque * signifie que le processus lancé sera considéré comme un processus de confiance quel que soit le répertoire où se trouve le fichier du processus.

Cochez dans la fenêtre **Liste des exclusions** (cf. ill. 38) la case **Exclure le riskware autorisé** afin que les programmes autorisés soient exclus de l'analyse. Ces programmes sont repris dans la fenêtre **Menaces et exclusions** qui s'ouvre lorsque vous aurez cliqué sur **Détails** (cf. point 5.7, p. 99).

5.6. Tâches définies par l'utilisateur

Lors de l'installation, Kaspersky Anti-Virus crée une liste de tâches système. Cette liste comprend les mises à jour (mise à jour des bases antivirus, mises à

jour des modules de l'application, annulation de la mise à jour des bases antivirus) et les tâches liées à l'analyse (analyse complète de Mon poste de travail, analyse automatique des objets au démarrage de Kaspersky Anti-Virus, analyse des disques amovibles, analyse de la quarantaine).

Vous pouvez lancer les tâches système, configurer les paramètres et les programmer. La suppression de ces tâches est impossible.

La configuration des tâches liées à la mise à jour des bases antivirus et des composants est décrite au point 5.1 à la page 44. La tâche liée au rejet des dernières mises à jour ne dispose pas de paramètres particuliers.

L'administrateur peut créer différentes tâches d'analyse des objets des utilisateurs et les administrer dans Kaspersky Anti-Virus.

L'utilisateur du poste de travail ne peut ni créer, ni administrer les tâches. Il peut uniquement consulter la liste des tâches créées par l'administrateur qui sont reprises dans la partie gauche de l'onglet **Protection** (cf. ill. 2) et les exécuter.

En cas d'administration à distance de Kaspersky Anti-Virus, la liste des tâches reprendra également les tâches locales et de groupe créées via Kaspersky Administration Kit (cf. point 6.3, p. 166). L'administration des tâches locales est identique à l'administration des tâches créées par l'utilisateur : il est possible de les lancer, de les supprimer ou de modifier leurs paramètres. Les tâches de groupe ne peuvent être lancées, supprimées ou modifiées au niveau de la configuration; l'administration de ces tâches est uniquement possible via Kaspersky Administration Kit.

Lorsque la modification de paramètres quelconque est interdite lors de l'administration des tâches via Kaspersky Administration Kit (ils sont "verrouillés": ), la modification via l'interface locale sera également inaccessible.

Afin de créer une nouvelle tâche :

Cliquez sur **Créer** dans la boîte de dialogue **Analyse à la demande** (cf. ill. 28). Cette action entraîne l'ouverture d'une boîte de dialogue (cf. ill. 29) contenant les onglets suivants : **Zone d'analyse**, **Configuration**, **Programmation** et **Lancement avec les privilèges**.

Saisissez le nom de la tâche dans le champ **Nom de la tâche** et procédez au reste de la configuration (consultez le point. 5.3.3 à la page 80).

La case **Illustrer la tâche sur l'onglet "Protection"** (qui commande l'affichage de la tâche dans la fenêtre principale du logiciel) figure dans les paramètres de toutes les tâches. Si la case est cochée, la tâche apparaîtra dans la partie gauche de l'onglet et pourra être exécutée.

Pour supprimer une tâche de la liste, sélectionnez-la et cliquez sur **Supprimer**. Sachez cependant que vous pouvez uniquement supprimer les tâches que vous aurez ajoutées manuellement. Les tâches système ainsi que les tâches de groupe créées via Kaspersky Administration Kit ne peuvent être séparées.

Afin d'exécuter une tâche, sélectionnez-la dans la liste puis cliquez sur **Lancer**. Ceci entraînera l'ouverture d'une fenêtre reprenant des informations relatives à l'exécution de la tâche.

Afin de consulter les paramètres de la tâche créée, sélectionnez-la dans la liste et cliquez sur **Propriétés.**

5.7. Constitution de la liste des exclusions

Il arrive parfois que certains objets doivent être exclus de l'analyse ou de la protection. Vous pouvez rédiger une liste d'exclusions pour l'analyse à la demande, l'analyse en temps réel, la protection en temps réel des fichiers et la protection en temps réel du courrier.

La liste générale des exclusions de la protection antivirus de l'ordinateur peut être consultée et modifiée dans la fenêtre **Menaces et exclusions** (cf. ill. 16). Cliquez sur le lien Menaces et exclusions dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3) pour ouvrir cette fenêtre. La liste des exclusions est rédigée à l'aide des boutons correspondants.

*Pour ajouter une exclusion, cliquez sur **Ajouter**.*

La fenêtre **Objet exclus** (cf. ill. 40) s'ouvre et vous permet de définir les exclusions pour Kaspersky Anti-Virus.

Les exclusions suivantes sont envisageables:

- Disques, répertoires, fichiers et masques de fichiers.
- *Menaces* : types de programmes malveillants ou de riskwares.
- *Fichiers d'un type de menace défini* : fichiers concrets auxquels un type de menace défini a été attribué après analyse.

Pour exclure un répertoire ou un fichier quelconque de la protection offerte par Kaspersky Anti-Virus (selon un masque),

il est indispensable de remplir le champ **Objet** en cliquant sur le bouton  .

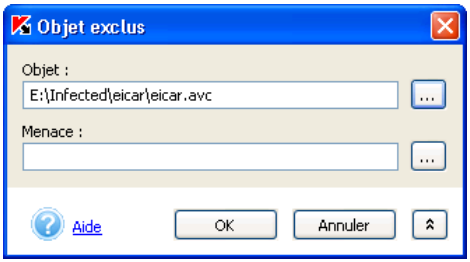

Illustration 40. Création de la liste des exclusions

Au moment de la création du chemin d'accès au répertoire ou à l'objet que vous souhaitez exclure de l'analyse, vous pouvez utiliser les variables système. Par exemple, vous pouvez exclure de l'analyse le répertoire d'installation de Microsoft Windows en saisissant **%windir%** en tant que variable.

Lors de l'ajout d'objets selon un masque, il est permis de saisir simultanément plusieurs masques en les séparant par un espace. Si le nom du fichier contient des espaces, il faudra le saisir entre guillemets.

Voici quelques exemples de masques admis :

- Masques sans chemin vers les objets :
  - *.**exe** : tous les fichiers **.exe*
  - ***.ex?** 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 objets :
  - **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*
  - **C:\dir**: tous les fichiers du répertoire *C:\dir* et de ses sous-répertoires
- Masque avec chemin d'accès relatif aux objets :
  - **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
- **dir**: tous les fichiers dans tous les répertoires *dir*\ et leurs sous-répertoires

La saisie des masques *.* et * sans indication du chemin est interdite car cela équivaut à la désactivation de la protection en temps réel.

Il n'est pas conseillé de ranger le disque virtuel formé sur la base du répertoire du système de fichiers à l'aide de la commande *subst* parmi les exclusions. Cela est dépourvu de sens car, pendant l'analyse, Kaspersky Anti-Virus considère ce disque virtuel comme un répertoire et l'analyse par conséquent.

Pour exclure du traitement antivirus tous les fichiers auxquels un type de menace particulier a été attribué,

Déployez la partie complémentaire de la fenêtre (cf. ill. 40) en cliquant sur  et sélectionnez la menace dans la fenêtre **Liste des menaces découvertes** (cf. ill. 41) qui s'ouvre à l'aide du bouton  .

Dans cette fenêtre, vous pouvez rechercher la menace au départ d'une partie du nom, trier la liste des menaces selon l'en-tête de la colonne **Nom** et copier le nom de la menace dans le Presse-Papiers à l'aide des commandes correspondantes du menu contextuel. Vous pouvez également consulter une description détaillée de la menace sur www.viruslist.com/fr. Pour ce faire, sélectionnez la menace et choisissez la commande **Détails** du menu contextuel.

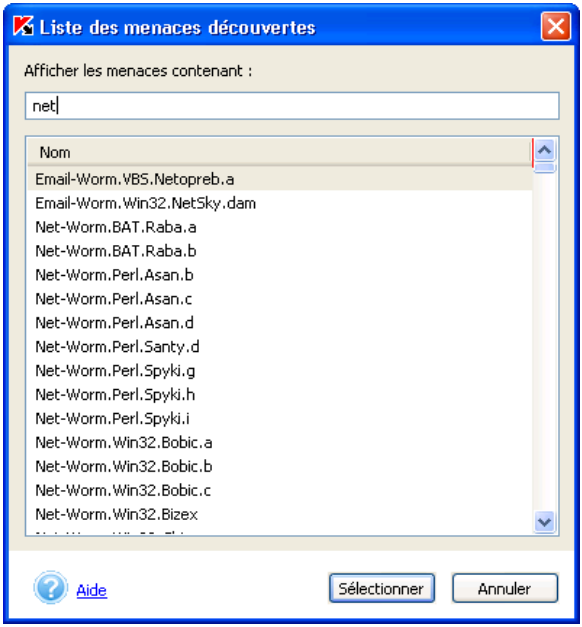

Illustration 41. Liste des menaces identifiées

Pour exclure de la protection un objet particulier rangé dans une catégorie de menace que vous connaissez:

1. Saisissez le nom de l'objet dans le champ **Objet**.
2. Définissez la menace dans le champ **Menace**.

Il est possible également d'exclure un fichier constituant une menace définie au départ de la notification qui s'affiche lorsque Kaspersky Anti-Virus découvre un tel fichier (cf. ill. 42). Si vous estimez que ce programme ne présente aucun danger et que vous pouvez l'utiliser sur votre ordinateur, choisissez l'option **Ajouter à la liste des programmes de confiance**. Le programme sera ajouté à la liste des exclusions de l'analyse dans la fenêtre **Menaces et exclusions** (cf. ill. 16).

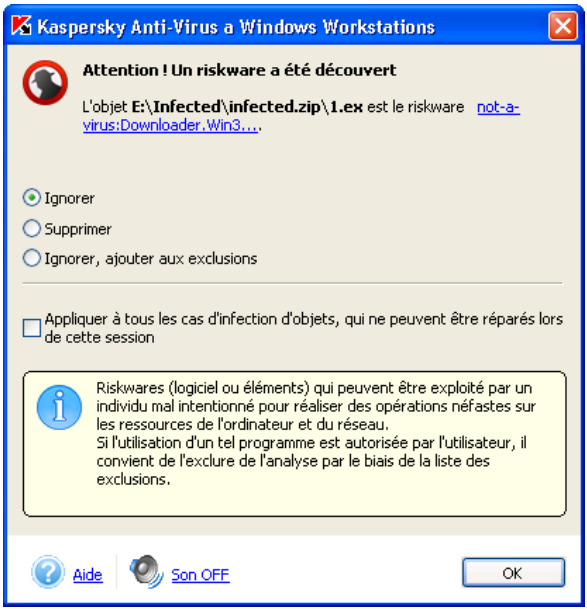

Illustration 42. Notification relative à une menace

5.8. Configuration de la programmation

Les tâches liées à l'analyse à la demande et à la mise à jour peuvent être lancées automatiquement selon un horaire défini. Vous recevrez ainsi la mise à jour des bases antivirus en temps opportuns et vous pourrez procéder à des analyses régulières de votre ordinateur.

Par défaut, Kaspersky Anti-Virus met à jour les bases antivirus toutes les trois heures et réalise une analyse complète de l'ordinateur tous les vendredi à 20:00.

Pour modifier l'horaire des mises à jour des bases antivirus :

1. Cliquez sur le lien Mises à jour dans la partie gauche de l'onglet **Paramètres**.
2. Dans la fenêtre qui s'ouvre, sélectionnez la tâche pour laquelle il faut créer/modifier un horaire puis, cliquez sur **Propriétés**.

Cette action entraînera l'ouverture de la boîte de dialogue de configuration de la mise à jour à l'onglet **Programmation** (cf. ill. 8).

Pour créer/modifier un horaire pour l'analyse à la demande :

1. Cliquez sur le lien Analyse à la demande dans la partie gauche de l'onglet **Paramètres**.
2. Sélectionnez, dans la liste des tâches d'analyse (cf. ill. 28), la tâche pour laquelle il convient de créer ou de modifier l'horaire puis cliquez sur **Propriétés**.

Cette action entraîne l'ouverture de la boîte de dialogue de configuration détaillée de cette tâche (cf. ill. 29). La configuration de l'horaire s'opère sur l'onglet **Programmation** (cf. ill. 43).

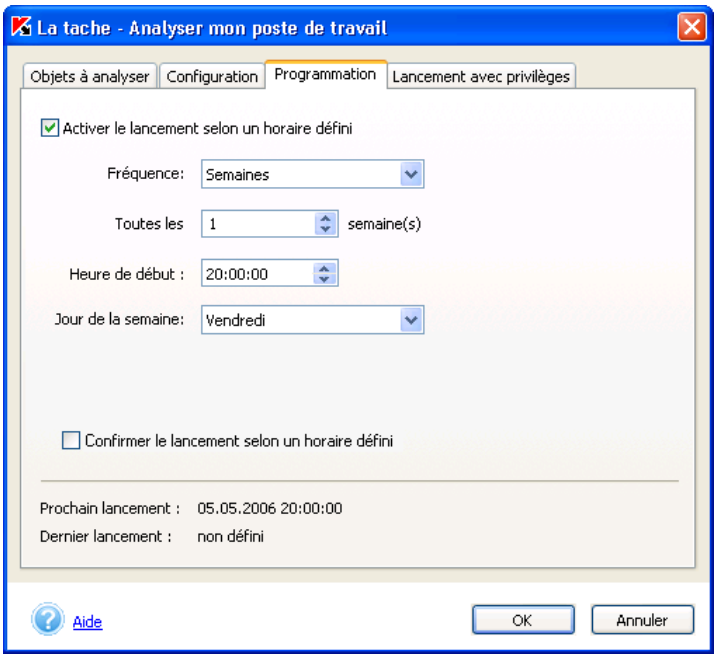

Illustration 43. Création d'une nouvelle tâche. Onglet **Programmation**

Pour activer le lancement automatique de la tâche selon l'horaire défini, cochez la case **Activer le lancement selon un horaire défini**.

Si vous souhaitez être averti du début de la mise à jour, cochez la case **Confirmer le lancement selon un horaire défini**. Lorsque cette case est

cochée, la fenêtre **Lancement de la tâche programmée** (cf. ill. 44) apparaît avant le lancement de l'analyse programmée. Cliquez sur **Lancer** pour lancer l'analyse programmée. Pour reporter l'analyse à plus tard, sélectionnez l'intervalle souhaité dans la liste déroulante et cliquez sur **Reporter**. Si aucune action n'est prise dans les trois minutes qui suivent dans la boîte de dialogue de confirmation, la tâche sera lancée automatiquement.

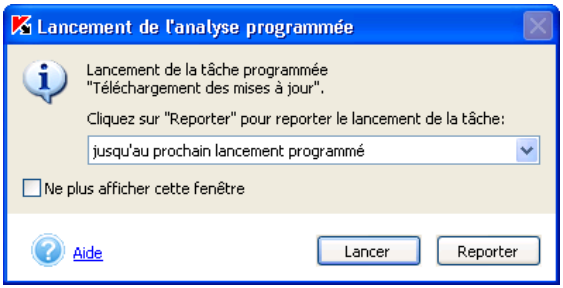

Illustration 44. Requête de lancement de l'analyse programmée

Sélectionnez dans le champ **Fréquence** la fréquence selon laquelle cette tâche sera exécutée. Vous avez le choix entre : *heure, jour, semaine*, ou *au démarrage du logiciel*. La partie centrale avec les champs de saisie des données changera en fonction de la fréquence sélectionnée :

- *Heure* : la tâche sera lancée selon une fréquence de quelques heures. Définissez l'intervalle (en heures) ainsi que la date et l'heure de la première exécution.

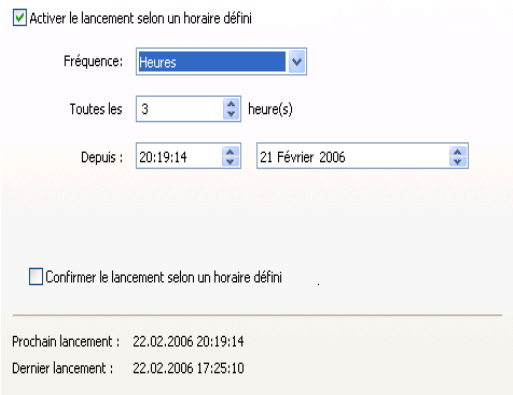

Illustration 45. Programmation selon une fréquence horaire

- *Jour* : la tâche sera lancée selon une fréquence de quelques jours. Définissez l'intervalle (en jours) et l'heure de début.

Illustration 46. Programmation selon une fréquence quotidienne

- *Semaine* : la tâche sera lancée selon une fréquence de quelques semaines. Définissez la fréquence (en semaines) et sélectionnez le jour et l'heure de lancement.

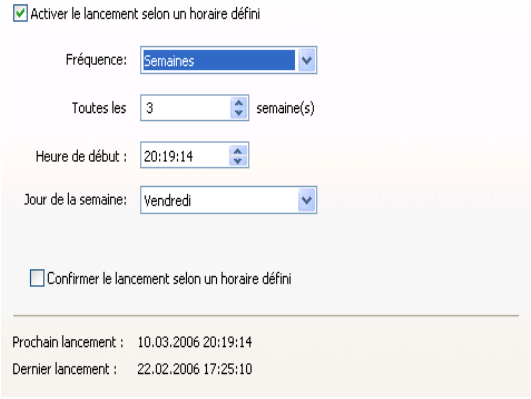

Illustration 47. Programmation selon une fréquence hebdomadaire

- *Au démarrage du logiciel* : la tâche est lancée directement après le démarrage de Kaspersky Anti-Virus.

5.9. Lancement d'une tâche au nom d'un utilisateur sélectionné

Kaspersky Anti-Virus 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 ouverte. Lorsque cette option est activée, l'administrateur saisit les données du compte jouissant des privilèges adéquats pour accéder à l'objet : par exemple, pour l'analyse à la demande, il est indispensable de jouir du privilège d'accès à l'objet et pour la mise à jour, il faut pouvoir accéder au répertoire local où se trouvent les mises à jour ou être autorisé à utiliser le serveur proxy.

Ceci évite les erreurs pendant l'exécution de l'analyse à la demande ou des mises à jour qui surviennent lorsque l'utilisateur qui lance la tâche ne jouit pas des privilèges adéquats.

La configuration de l'exécution des tâches au nom d'un autre compte s'opère dans l'onglet **Lancement avec privilèges** (cf. ill.48).

Pour activer le service, cochez la case **Lancer avec les privilèges utilisateur**. Cette case n'est pas sélectionnée par défaut et la tâche sera réalisée conformément aux privilèges du compte courant.

Saisissez en dessous les données du compte sous lequel la tâche sera exécutée : nom d'utilisateur et mot de passe.

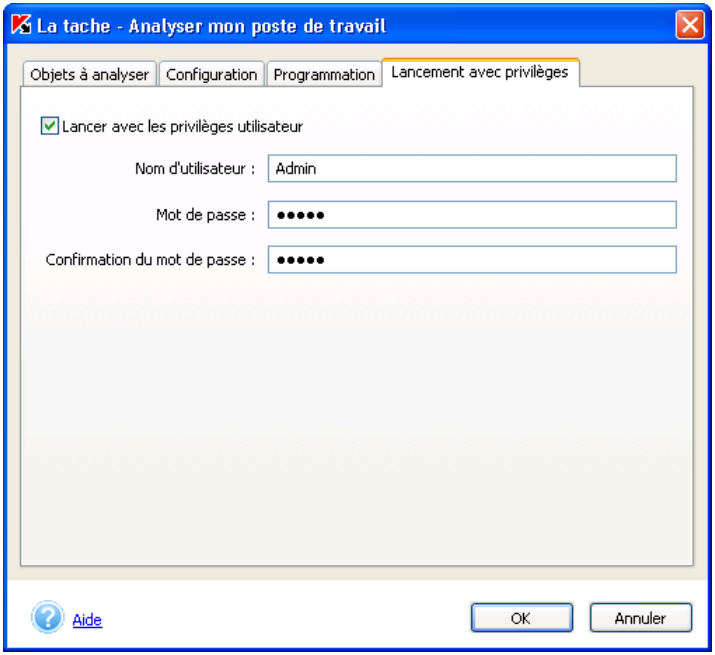

Illustration 48. Onglet **Exécuter comme**

5.10. Possibilités complémentaires

Kaspersky Anti-Virus propose les possibilités suivantes au niveau de la configuration et de l'utilisation telles que :

- La manipulation des objets suspects placés dans le répertoire de quarantaine ;
- La manipulation des copies des objets supprimés ou modifiés par Kaspersky Anti-Virus et placées dans le dossier de sauvegarde ;
- Rapport sur l'activité du logiciel ;
- Administration de la configuration de Kaspersky Anti-Virus
- Les options avancées.
- Configuration des confirmations
- Utilisation du mode administrateur et du mode utilisateur

5.10.1. Quarantaine et dossier de sauvegarde

Kaspersky Anti-Virus permet d'isoler les objets suspects dans un dossier de quarantaine et de conserver une copie des objets infectés dans le dossier de sauvegarde avant de les réparer ou de les supprimer.

En cas de découverte d'un objet suspect, l'application l'isole dans le répertoire de quarantaine. Là, il pourra être à nouveau analysé, supprimé, restauré ou envoyé à Kaspersky Lab pour analyse.

La copie de sauvegarde est créée lors de la première suppression ou réparation après la découverte de l'objet. Elle est placée dans le dossier de sauvegarde. L'objet pourra être restauré s'il renferme des informations capitales.

5.10.1.1. Configuration des dossiers de quarantaine et de sauvegarde

Afin de consulter ou de modifier les paramètres appliqués à la quarantaine ou au dossier de sauvegarde :

Cliquez sur le lien Quarantaine et dossier de sauvegarde dans la partie gauche de l'onglet **Paramètres**.

La fenêtre **Configuration de la quarantaine et du dossier de sauvegarde** reprend des onglets qui vous permettront de définir les différents paramètres.

Dans la fenêtre qui s'ouvre (cf. ill. 49), modifiez les paramètres suivants sur les onglets correspondant à la quarantaine et au dossier de sauvegarde :

Décochez la case **Supprimer les fichiers après (jours)**. Par défaut, la durée de conservation des fichiers en quarantaine n'est pas définie (la case n'est pas cochée). Vous pouvez préciser cette durée en cochant la case adéquate et en saisissant la valeur souhaitée dans le champ (la durée proposée par défaut est de 90 jours).

Cochez la case **Taille maximum (Mo)** La taille de la quarantaine n'est pas limitée par défaut (cette case n'est pas cochée). Si vous souhaitez limiter la taille totale des fichiers dans le dossier, cochez la case adéquate et précisez la taille souhaitée dans la liste déroulante (la valeur de 100 Mo est sélectionnée par défaut). Sélectionnez ensuite l'action exécutée par Kaspersky Anti-Virus une fois que le dossier est plein :

- *Avertir l'utilisateur* : le message interrogeant l'utilisateur sur les actions à prendre s'affiche lorsque la limite est atteinte
- *Supprimer les objets les plus anciens* : supprime les fichiers mis en quarantaine avant les autres.

Analyser automatiquement tous les objets en quarantaine après chaque mise à jour des bases antivirus. Ce mode de fonctionnement vous permet de procéder automatiquement à une nouvelle analyse des objets en quarantaine après chaque mise à jour des bases antivirus.

Kaspersky Anti-Virus ne peut analyser les objets en quarantaine directement après la mise à jour des bases antivirus si vous utilisez la quarantaine à ce moment.

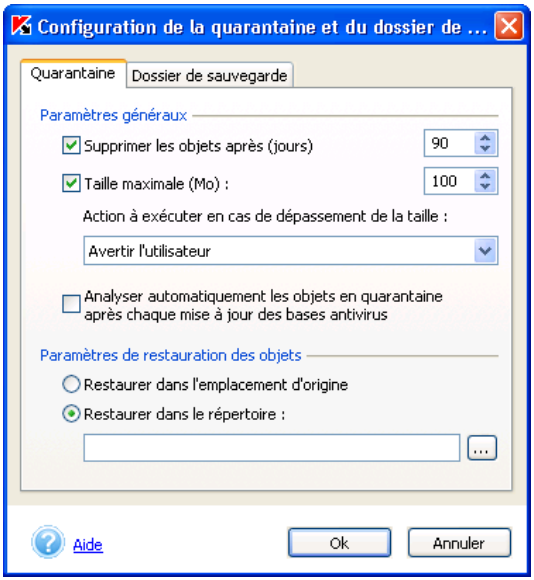

Illustration 49. Configuration de la quarantaine

Le champ **Paramètres de restauration des objets** reprend par défaut le chemin d'accès au dossier où seront placés les objets lors de la restauration.

Restaurer dans l'emplacement d'origine. Par défaut, la copie est restaurée à l'endroit où Kaspersky Anti-Virus a découvert le fichier original.

Restaurer dans le répertoire. Si vous choisissez cette option, vous devrez indiquer le chemin d'accès au répertoire dans lequel les objets restaurés seront sauvegardés

Les paramètres liés à la taille maximale du dossier de sauvegarde, à la durée de conservation des copies de sauvegarde et à leur restauration sont identiques aux paramètres équivalents de la quarantaine.

5.10.1.2. Utilisation de la quarantaine

Tous les objets suspects découverts pendant l'analyse antivirus ou interceptés par la protection en temps réel sont mis en quarantaine par Kaspersky Anti-Virus. Vous pouvez continuer à manipuler ces fichiers une fois qu'ils sont en quarantaine (analyse, restauration, suppression, etc.).

Par défaut, après chaque mise à jour des bases antivirus, Kaspersky Anti-Virus analyse les objets qui se trouvent en quarantaine. S'il est nécessaire de procéder à une analyse manuelle des objets, nous vous conseillons de réaliser la mise à jour des bases antivirus avant de procéder à l'analyse. Il est possible en effet qu'à ce moment les bases contiennent les définitions des virus qui pourraient avoir infectés les fichiers et ceux-ci pourront être réparés.

Avant d'analyser les fichiers en quarantaine, nous vous conseillons de mettre les bases antivirus à jour. Il se peut en effet que ces nouvelles bases contiennent les définitions des virus qui auraient infecté les fichiers, ce qui permettrait leur réparation.

Le traitement des objets suspects s'opère dans la fenêtre **Quarantaine** (cf. ill. 50) accessible en cliquant sur le lien Consulter la quarantaine de l'onglet **Protection** (cf. ill. 2) ou sur le lien du même nom dans la boîte de dialogue d'analyse (cf. ill. 5).

Le nombre d'objets placés en quarantaine figure entre parenthèses à côté du lien Consulter la quarantaine sur l'onglet **Protection** (cf. ill. 4).

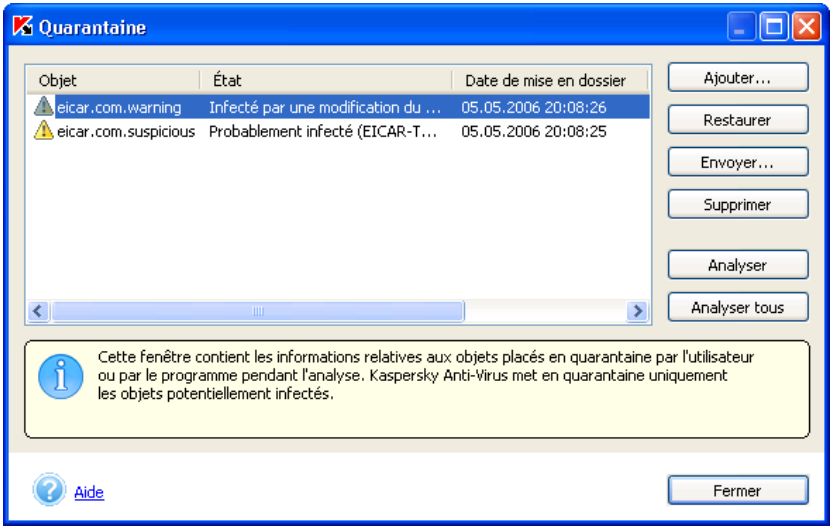

Illustration 50. Fenêtre des objets en quarantaine

Vous pouvez réaliser les opérations suivantes au départ de cette boîte de dialogue :

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

- Analyser et réparer à l'aide des dernières bases antivirus tous les objets potentiellement infectés ou uniquement certains d'entre eux. Pour ce faire, cliquez sur **Analyser tous** ou **Analyser** (après avoir sélectionné les objets à analyser).

  L'état de chaque objet en quarantaine après l'analyse et la réparation peut être soit *infecté*, *probablement infecté*, *fausse alerte, sain, 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 bel et bien dangereux 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 Kaspersky Anti-Virus.

Il est possible de lancer l'**Analyse de la quarantaine** au départ de la fenêtre **Analyse à la demande** (cf . ill. 28). La fenêtre **Analyse** (cf. ill. 5) apparaît lors du lancement de la tâche. Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 5.10.2 à la page 115).
La tâche **Analyse de la quarantaine** est identique à la tâche lancée via le bouton **Tout analyser** dans la **Quarantaine** (cf. ill. 50).

- Restaurer les fichiers dans leur répertoire d'origine, là 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.

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

- Envoyer les objets potentiellement infectés aux experts de Kaspersky Lab en vue d'un examen. Veuillez envoyer ces objets uniquement si l'état *Probablement infecté* ne change pas en dépit d'analyses et de tentatives de réparation répétées. Pour ce faire, cliquez sur **Envoyer…** (Consultez l'Annexe A à la page 214 pour de plus amples informations).

Nous attirons votre attention sur le fait que chaque fichier que vous envoyez à Kaspersky Lab doit avoir été analysé par Kaspersky Anti-Virus à l'aide des bases antivirus mises à jour au plus tard un jour avant l'envoi.

- 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**.

5.10.1.3. Utilisation du dossier de sauvegarde

Avant la réparation ou la suppression d'un objet infecté ou suspect, Kaspersky Anti-Virus crée une copie de celui-ci dans le dossier de sauvegarde.

Le cas échéant, vous pourrez restaurer n'importe lequel de ces objets par exemple si des données ont été perdues pendant la réparation, si l'objet a été supprimé par accident ou si vous souhaitez essayer de le réparer une fois de plus à l'aide des bases antivirus actualisées.

Les manipulations sur les copies de sauvegarde sont réalisées dans la fenêtre **Dossier de sauvegarde** (cf. ill. 51) qui apparaît en cliquant sur Dossier de sauvegarde dans l'onglet **Protection** (cf. ill. 2) de la fenêtre principale de l'application.

Le nombre de copies de sauvegarde figure entre parenthèses à côté du lien Dossier de sauvegarde sur l'onglet **Protection** (cf. ill. 4).

Vous pouvez réaliser les opérations suivantes dans le dossier de sauvegarde :

- Restaurer les objets dans leur répertoire d'origine, là où ils se trouvaient avant d'être mis dans le dossier de sauvegarde ou bien dans le répertoire de restauration. Pour restaurer un objet, sélectionnez-le dans la liste et cliquez sur **Restaurer**.

  L'objet est restauré au départ de la copie 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.

- Supprimer n'importe quel fichier ou groupe de fichiers du dossier de sauvegarde. Pour supprimer un fichier, sélectionnez-le dans la liste puis cliquez sur **Supprimer**.

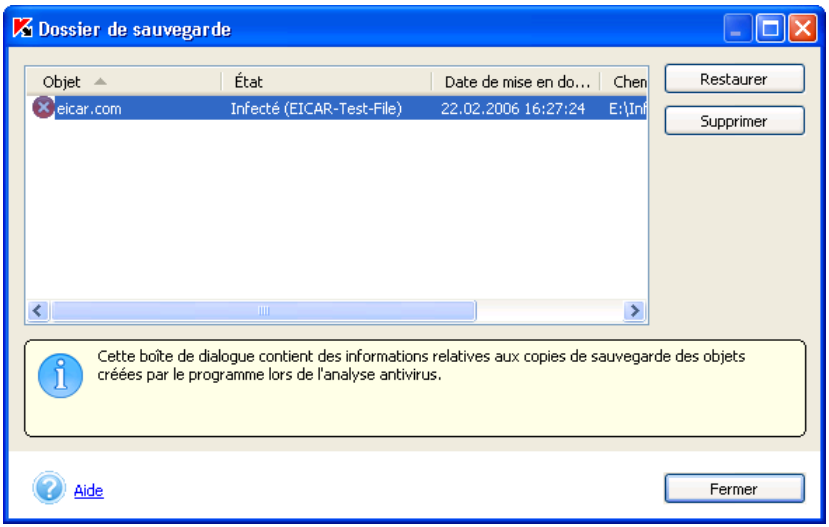

Illustration 51. Fenêtre du dossier de sauvegarde

Quand peut-on restaurer une copie de sauvegarde ?

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

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

Par défaut, la durée de conservation des copies de sauvegarde et la taille maximale du répertoire ne sont pas définies. Il est conseillé de consulter régulièrement le contenu du répertoire et de le nettoyer. Il est possible également de configurer le programme afin qu'il supprime lui-même les copies les plus anciennes ou qu'il vous avertisse lorsque le répertoire déborde (pour de plus amples informations, consultez le point 5.10.1.1 à la page 109).

5.10.2. Utilisation des rapports

Des rapports sont constitués lors de l'analyse complète de l'ordinateur, lors de la mise à jour des bases antivirus ainsi que pendant la protection en temps réel. Ces rapports fournissent des indications sur les objets analysés et le résultat de leur traitement ainsi que des statistiques d'ordre général.

Kaspersky Anti-Virus tient une liste du résultat des actions exécutées dans le journal des tâches (cf. ill. 52). Pour ouvrir ce journal, cliquez sur le lien Consulter les rapports dans la partie gauche de l'onglet **Protection** (cf. ill. 2). Le rapport reprend l'état de chaque tâche, ainsi que la date et l'heure de la fin d'exécution.

Les informations relatives au traitement d'un objet peuvent être de cinq types :

 ou  *Informations* contient de simples renseignements (ex. : tâche lancée, tâche arrêtée, tâche exécutée, tâche en cours d'exécution).

 Le *rapport* contient des informations critiques (par exemple, Attention ! Il reste des objets qui n'ont pas été traités).

 *Commentaires* sur certains moments importants (par exemple : la tâche a été interrompue).

En règle générale, les messages confirmant la réussite d'une opération ou de simples informations sont fournis à titre purement informatif et n'ont aucune importance critique. Vous pouvez décider de ne pas afficher dans les rapports ces messages à caractère purement informatif. Pour ce faire, désélectionnez la

case **Afficher les rapports informatifs**. N'oubliez pas que les rapports sur l'exécution en cours d'une tâche quelconque signalés par l'icône seront toujours affichés.

Illustration 52. Fenêtre **Rapports**

Vous pouvez également classer les rapports en fonction de leur type, par ordre alphabétique ou par heure de fin de l'exécution de la tâche. Pour annuler le classement des rapports, il suffit d'un clic gauche sur le titre de la colonne selon laquelle les rapports avaient été classés.

Vous pouvez, grâce au menu contextuel ouvert à l'aide d'un clic droit de la souris sur le nom du rapport, exécutez les tâches suivantes au départ de cette fenêtre :

- **Exporter le rapport détaillé dans le fichier…**. Dans la fenêtre Microsoft Windows, saisissez le nom du fichier, l'emplacement pour le sauvegarder puis cliquez sur **Enregistrer**. Le rapport est enregistré sous la forme d'un tableau Microsoft Excel ou dans un fichier texte.
- **Envoyer le rapport à Kaspersky Lab.** Vous pouvez envoyer le rapport si la tâche (ex. : analyse de l'ordinateur ou mise à jour des bases antivirus) a été interrompue ou si elle s'est soldée par un échec et que vous en ignorez les causes. Cette action entraînera l'ouverture automatique du client de messagerie installé sur votre ordinateur, comme Microsoft Outlook Express, et la création d'un nouveau message reprenant le rapport en annexe. Ensuite, envoyez le message et les spécialistes de

Kaspersky Lab tenteront de résoudre votre problème le plus rapidement possible.

La création automatique du message s'opère toujours dans les clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express. Si votre ordinateur est équipé d'un autre client de messagerie (ex. :The Bat !), il faudra au préalable modifier les paramètres de prise en charge de SimpleMAPI de votre client.

- Supprimer un ou tous les rapports de la liste à l'aide de la commande **Supprimer la rapport** ou **Supprimer tout les rapports**. Vous ne pouvez pas supprimer le rapport d'une tâche qui est toujours en cours d'exécution.

Il est possible, pour n'importe quelle tâche reprise dans le journal, d'étudier ses paramètres, ses statistiques et de consulter le rapport sur les objets découverts. Il suffit simplement de cliquer sur **Détails**.

Les onglets **Statistiques**, **Rapports** et **Paramètres** de la fenêtre qui s'affiche vous fourniront tous les détails demandés.

Ainsi, l'onglet **Statistiques** (cf. ill. 53) reprend les informations générales sur le travail exécuté par Kaspersky Anti-Virus dans le cadre de cette tâche : date et heure du lancement, nombre d'objets analysés, nombre d'objets infectés et réparés ainsi que le nombre d'objets mis en quarantaine. La taille de la mise à jour à télécharger et le volume déjà téléchargé sur l'ordinateur apparaissent sur l'onglet pendant la mise à jour.

Illustration 53. Onglet **Statistiques**

L'onglet **Rapport** (cf. ill. 55) n'affiche aucune information par défaut sur les objets sains. Pour changer cet état de fait, il convient de cocher la case **Enregistrer tous les rapports** dans les options avancées de Kaspersky Anti-Virus (cf. point 5.10.4, p. 120). Désormais, l'onglet reprendra les informations relatives à chaque objet analysé. Pendant la mise à jour, il affichera des informations sur chacune des étapes de la procédure : connexion à la source de mise à jour, nom des fichiers téléchargés et informations sur les résultats de leur installation sur l'ordinateur. Ces informations sont reprises en permanence, même si la case **Enregistrer tous les rapports** n'a pas été cochée dans les options avancées de Kaspersky Kaspersky Anti-Virus.

*Pour ne pas afficher les rapports à caractère purement informatif lors de la séance en cours sans désélectionner la case **Enregistrer tous les rapports** :*

Lors de la consultation des rapports dans l'onglet **Rapport** (cf. ill. 55) affichez le menu contextuel d'un clic droit (cf. ill. 54) et décochez **Afficher rapport détaillé**.

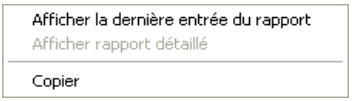

Illustration 54. Menu contextuel des rapports

Vous pouvez copier les informations relatives à un événement particulier dans le presse-papiers. Pour ce faire, sélectionnez l'événement qui vous intéresse et choisissez la commande **Copier** dans le menu contextuel.

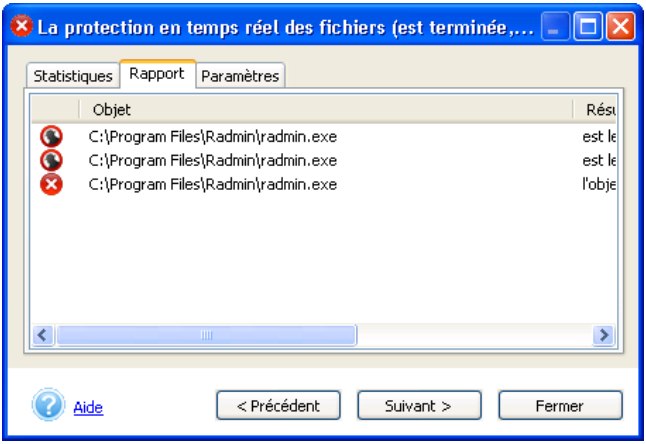

Illustration 55. Onglet **Rapport**

L'onglet **Paramètres** (cf. ill. 56) reprend les paramètres utilisés pour l'exécution des différentes tâches. Il reprend notamment les informations relatives aux objets de l'analyse et au niveau de protection défini pour cette tâche, aux actions exécutées sur les objets infectés, les programmes malicieux et les fichiers potentiellement infectés.

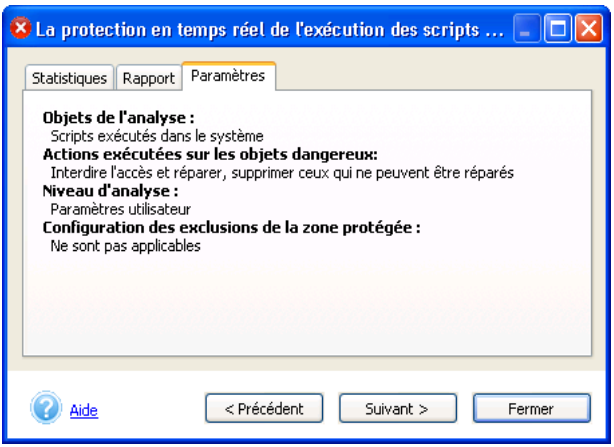

Illustration 56. Onglet **Paramètres**

Pour passer d'une tâche à l'autre dans le journal ou dans le rapport détaillé, vous pouvez utiliser les boutons **Suivant>** et **<Précédent** ou sélectionnez le nom de la tâche dans la liste déroulante.

Vous pouvez configurer le journal des rapports dans la fenêtre **Options avancées** (cf. ill. 58) qui s'ouvre en cliquant sur le lien du même nom dans la partie gauche de l'onglet **Paramètres** (voir point 5.10.4 à la page 120 pour de plus amples informations). Vous pouvez définir la durée maximale de conservation des rapports et autoriser ou non l'enregistrement des messages à caractère purement informatif dans le rapport détaillé.

5.10.3. Administration de la configuration de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet d'utiliser plusieurs configuration. Vous pouvez désormais définir une configuration pour un mode d'utilisation particulier, l'enregistrer dans un fichier spécial (*un profil*) et l'utiliser quand vous en avez besoin.

Cliquez sur le lien Gestion des profils dans la partie gauche de l'onglet Paramètres (cf. ill. 3) pour passer à l'administration de la configuration du programme.

Le bouton **Sauvegarder profil…** dans la fenêtre qui s'ouvre (cf. ill. 57) vous permet de sauvegarder la configuration actuelle dans un fichier de configuration spécial. Le bouton **Charger profil…** quant à lui vous permet d'appliquer un fichier de configuration quelconque pour Kaspersky Anti-Virus défini antérieurement. Il est possible que le chargement d'une nouvelle configuration entraîne le redémarrage de l'ordinateur car certains modes de fonctionnement sont activés lors du démarrage du système.

Pour rétablir la configuration recommandée, cliquez sur **Restaurer**.

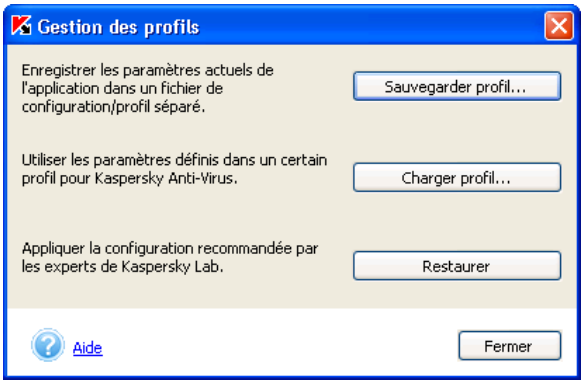

Illustration 57. Administration des profils

5.10.4. Options avancées

En plus de la configuration de tâches concrètes, Kaspersky Anti-Virus permet la configuration de paramètres généraux et de service (cf. ill. 58). Dans la partie gauge de l'onglet Paramètres (cf. ill. 3) .

Pour configurer les paramètres avancés de Kaspersky Anti-Virus :

Cliquez sur Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3). Cette action entraîne l'ouverture d'une boîte de dialogue présentant les onglets suivant : **Général**, **Performances** et **Sécurité**.

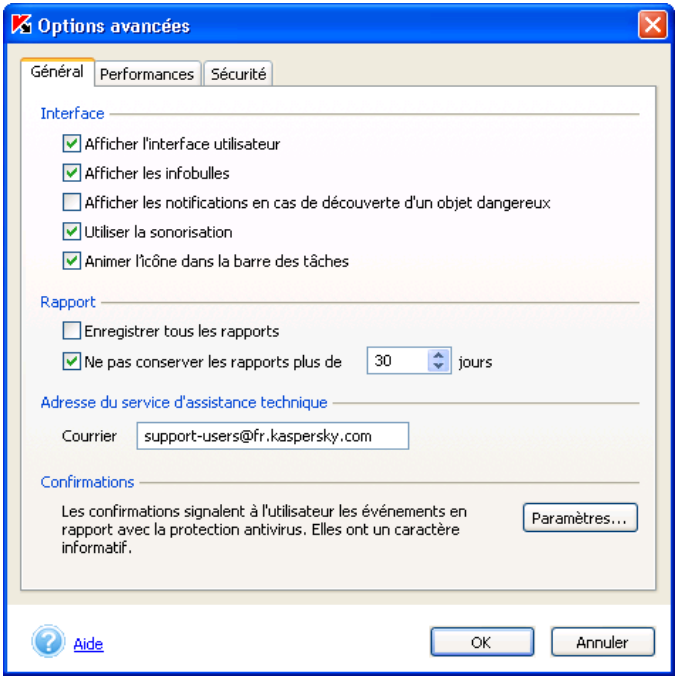

Illustration 58. Options avancées de Kaspersky Anti-Virus.
Onglet **Général**

Vous pouvez ainsi modifier les paramètres suivants sur l'onglet **Général** (cf. ill. 58):

- **Afficher l'interface utilisateur** : active l'affichage de l'icône du programme dans la barre d'état et permet le lancement de la fenêtre principale de l'application en mode utilisateur (cf. point 5.10.7, p. 126).

  Les paramètres de l'affichage de l'interface entrent en vigueur uniquement après le redémarrage de l'ordinateur.

- **Afficher les infobulles** : active l'affichage à l'écran de tous les messages prévus pendant l'utilisation de Kaspersky Anti-Virus. Ils apparaissent au-dessus de l'icône du logiciel dans la barre des tâches.

  L'affichage des messages informatifs n'est pas accessible sous Windows 98 ou Microsoft Windows NT Workstation 4.0.

- **Afficher la notification en cas de découverte d'un objet dangereux** :active l'affichage d'un message relatif à la découverte d'un objet dangereux.

- **Utiliser la sonorisation** : active l'émission d'effets sonores lors d'événemens définis qui surviennent pendant l'utilisation de Kaspersky Anti-Virus. Vous pouvez consulter la liste des événements et modifier la sélection de son à l'aide des outils du système d'exploitation Microsoft Windows (**Démarrer → Panneau de configuration → Sons et périphériques audio → Sons**).
- **Animer l'icône dans la barre des tâches** : active l'animation de l'icône en fonction de l'opération exécutée par Kaspersky Anti-Virus. Ainsi, lors de l'analyse d'un message, une enveloppe qui clignote se superpose à l'icône.
- **Enregistrer tous les rapports**: enregistre tous les rapports générés pendant l'utilisation du logiciel : les messages informatifs, les avertissements d'erreur. Ce mode est désactivé par défaut. Le rapport contiendra uniquement les messages les plus importants comme les erreurs survenues à la fin d'une tâche, l'interruption de l'exécution d'une tâche, etc.
- **Ne pas conserver les rapports plus de … jours** : Par défaut, les rapports sont conservés trente jours. Vous pouvez modifier cette durée en saisissant un autre chiffre dans le champ ou lever toute restriction en désélectionnant la case. La vérification de la durée de conservation des rapports et la suppression des anciens rapports s'opèrent lors du démarrage de Kaspersky Anti-Virus.

Vous pouvez indiquer l'adresse électronique du service d'assistance technique dans le champ **Adresse du service d'assistance technique**. L'adresse reprise par défaut est celle du service d'assistance technique de Kaspersky Lab (support@kaspersky.com). Vous pouvez saisir par exemple dans ce champ l'adresse électronique de l'administrateur de la sécurité ou l'URL de la page ouverte en cas d'appel au service d'assistance technique.

La rubrique **Confirmation** vous permet de contrôler l'affichage des notifications relatives à certains événements qui surviennent dans le travail de Kaspersky Anti-Virus. En règle général, les confirmations ont un caractère purement informatif. Pour de plus amples informations sur la configuration de la confirmation, consultez le point 5.10.5 à la page 125.

L'onglet **Performances** (cf. ill. 59) vous permet de définir des restrictions appliqués à l'analyse à la demande afin de réduire la consommation de la batterie (pour les ordinateurs portables) et d'épargner les ressources du système d'exploitation (pour de plus amples informations, consultez le point 5.10.6 à la page 126).

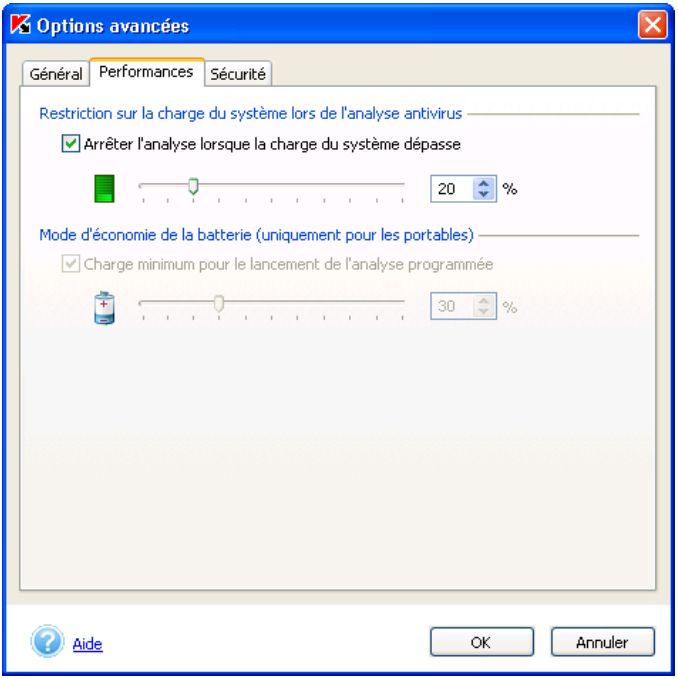

Illustration 59. Options avancées de Kaspersky Anti-Virus.
Onglet **Performances**

L'onglet **Sécurité** (cf. ill. 61) propose les paramètres suivants :

- **Lancer Kaspersky Anti-Virus au démarrage du système** : démarre Kaspersky Anti-Virus après le redémarrage du système d'exploitation.

  Nous insistons sur la nécessité de ne jamais fermer Kaspersky Anti-Virus car cela pourrait entraîner une infection de votre ordinateur.

  La configuration de ce mode n'est admissible que si vous jouissez des privilèges d'administrateur sur l'ordinateur.

- **Utiliser le système de restauration après les échecs** : active le système de restauration du fonctionnement de Kaspersky Anti-Virus en cas d'échecs. Si le fonctionnement de l'application est interrompu, la fenêtre principale de Kaspersky Anti-Virus se ferme (si elle était ouverte) et un message apparaît au dessus de l'icône de l'application dans la barre des tâches. (cf. ill. 60). Ensuite, le rétablissement du fonctionnement de l'application s'opère automatiquement.

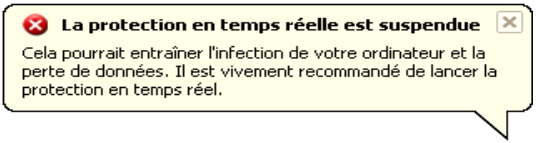

Illustration 60. Echec de l'application

Protéger le logiciel par mot de passe : un mot de passe devra être saisi pour basculer en mode administrateur. Nous vous recommandons ce mode si d'autres personnes ont accès à votre ordinateur et que vous ne souhaitez pas qu'elles puissent modifier la configuration de la protection antivirus, désactiver la protection en temps réel ou décharger Kaspersky Anti-Virus (pour de plus amples informations, consultez le point 5.10.7 à la page 126). En activant ce mode, saisissez le mot de passe dans le champ **Mot de passe** et confirmez-le dans le champ **Confirmation du mot de passe**.

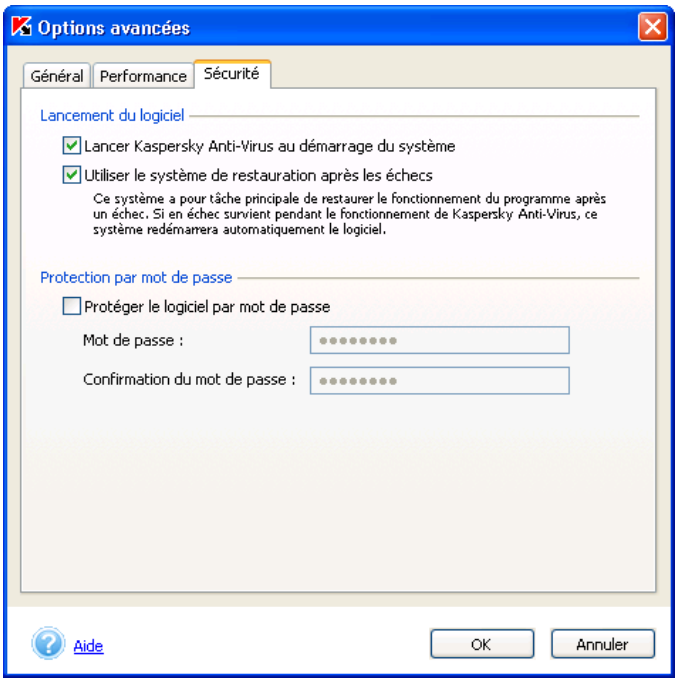

Illustration 61. Options avancées de Kaspersky Anti-Virus. Onglet **Sécurité**

5.10.5. Configuration des confirmations

Si vous souhaitez être prévenu de certains événements dans le cadre du fonctionnement du logiciel, cliquez sur le lien Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3). Cliquez sur **Configuration** dans la section **Confirmation** dans la fenêtre des options avancées qui s'ouvre. La boîte de dialogue de configuration de la confirmation s'affiche (cf. ill. 62).

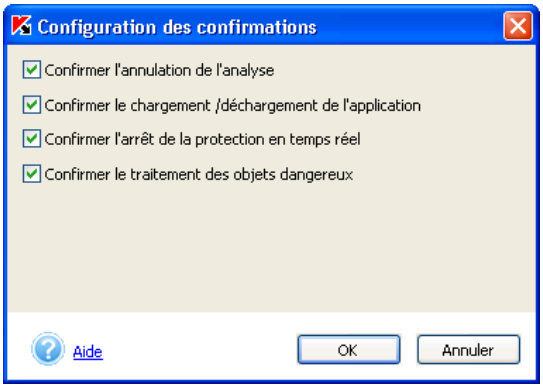

Illustration 62. Configuration de la confirmation

Les événements suivants sont prévus :

- **Confirmer l'annulation de l'analyse** : affiche à l'écran une boîte de dialogue demandant la confirmation de l'annulation de l'analyse à la demande. Suite à l'annulation de l'analyse, une info-bulle reprenant la cause de l'annulation de l'analyse apparaîtra au-dessus de l'icône de l'application dans la barre des tâches
- **Confirmer le chargement/déchargement de l'application** : affiche à l'écran une boîte de dialogue demandant la confirmation du lancement/de l'arrêt de Kaspersky Anti-Virus.
- **Confirmer l'arrêt de la protection en temps réel** : affiche à l'écran un message vous avertissant de la désactivation totale de la protection en temps réel de votre ordinateur. Cette option n'est pas disponible si vous avez décidé de ne pas utiliser la protection en temps réel des fichiers au moment de l'installation de Kaspersky Anti-Virus.
- **Confirmer le traitement des objets dangereux** : affiche à l'écran un message vous avertissant que certains objets infectés non pas été traités.

5.10.6. Restriction des performances de Kaspersky Anti-Virus

Vous pouvez introduire des restrictions sur le lancement de l'analyse à la demande lorsqu'il faut épargner les ressources de l'ordinateur. Pour ce faire, cliquez sur Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 3). Ouvrez l'onglet **Performances** (cf. ill. 59) de la fenêtre des options avancées du programme.

Les restrictions suivantes sont prévues :

- **Arrêter l'analyse lorsque la charge du système dépasse… %** : suspend l'analyse à la demande si la charge du système de fichier dépasse le niveau indiqué. Dès que cette charge revient à un niveau admissible, l'analyse sera reprise. Vous pouvez définir ce niveau soit à l'aide du curseur, soit en saisissant directement la valeur (en %) au dessus de laquelle le lancement de l'analyse programmée n'aura pas lieu.

  L'effet de ce paramètre touche uniquement l'analyse à la demande (par exemple, analyse d'un objet sélectionné). La protection en temps réel n'est pas affectée.

- **Charge minimum pour le lancement de l'analyse programmée** : annule le lancement de l'analyse sur votre ordinateur portable lorsque la charge de la batterie est inférieure à la valeur que vous aurez définie. Vous pouvez définir ce niveau soit à l'aide du curseur, soit en saisissant directement la valeur (en %) en dessous de laquelle le lancement de l'analyse programmée n'aura pas lieu.

  Ce paramètre est accessible uniquement lorsque Kaspersky Anti-Virus est installé sur un ordinateur portable qui n'est pas branché sur une prise secteur.

5.10.7. Utilisation du mode administrateur et du mode utilisateur

Kaspersky Anti-Virus peut fonctionner selon deux modes : administrateur ou utilisateur. L'utilisation de ces modes peut être utile lorsque d'autres personnes utilisent votre ordinateur. Vous pouvez empêcher la modification de la configuration de la protection, la désactivation de la protection en temps réel et le déchargement de Kaspersky Anti-Virus. En mode utilisateur, l'interface du logiciel est modifiée : les paramètres inaccessibles sont dissimulés (par exemple, l'onglet **Paramètres** n'apparaît pas dans la fenêtre principale).

Vous pouvez activer le mode utilisateur ou le mode administrateur via l'interface locale ou à l'aide de Kaspersky Administration Kit (cf. point 6.2.2.14, p. 161).

Pour activer le mode utilisateur ou le mode administrateur via l'interface locale :

Cochez la case **Protéger le logiciel avec un mot de passe** sur l'onglet **Sécurité** (cf. ill. 61) dans la fenêtre des options avancées de Kaspersky Anti-Virus. Saisissez le mot de passe dans le champ **Mot de passe** et saisissez le à nouveau dans le champ **Confirmation du mot de passe**.

La commande **Passer en mode utilisateur** apparaît dans le menu contextuel (cf. ill. 1) qui permet de passer au mode utilisateur. Pour revenir au mode administrateur, utilisez la commande **Passer en mode administrateur** dans le menu contextuel et saisissez le mot de passe dans la fenêtre qui s'ouvre (cf. ill. 63).

Si la case **Protéger le logiciel avec un mot de passe** (cf. ill. 61) n'est pas cochée, Kaspersky Anti-Virus tourne en mode administrateur.

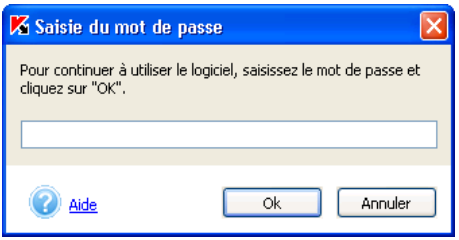

Illustration 63. Saisie du mot de passe

Pour dissimuler complètement l'interface de l'application en mode utilisateur :

Désélectionnez la case **Afficher l'interface utilisateur** sur l'onglet **Général** (cf. ill. 58) dans la fenêtre des options avancées de Kaspersky Anti-Virus.

Dans ce cas en mode utilisateur dans la tâche système l'icône Kaspersky Anti-Virus ne sera pas visible et la fenêtre principale de l'application ne s'ouvrira pas.

CHAPITRE 6. ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT

6.1. Administration des paquets d'installation

Cette rubrique explique comment créer et configurer des paquets d'installation pour Kaspersky Anti-Virus 5.0 for Windows Workstations. Pour obtenir de plus amples informations sur l'administration des paquets d'installation, consultez le Manuel de l'administrateur de Kaspersky Administration Kit 5.0.

6.1.1. Création d'un paquet d'installation

Pour créer un paquet d'installation, suivez les instructions reprises ci-après:

1. Connectez-vous au serveur d'administration voulu.
2. Sélectionnez le noeud **Installation distant** dans l'arborescence, ouvrez le menu contextuel et sélectionnez le point **Nouveau** / **Paquet d'installation** ou sélectionnez l'élément identique du menu **Action**. Suivez les instructions données par l'Assistant qui s'ouvre.

L'interface du programme de création des stratégies est identique à l'interface des Assistants sous Microsoft Windows et se présente sous la forme d'une succession de boîtes de dialogue. La navigation entre ces différentes boîtes s'opèrent à l'aide de boutons **< Précédent** et **Suivant >**. Cliquez sur **Terminer** pour quitter l'Assistant à la fin de l'installation. Pour interrompre l'Assistant à n'importe quelle étape du processus, cliquez sur **Annuler**.

La création du paquet d'installation s'accompagne de la configuration d'une petite sélection de paramètres. Les autres valeurs sont définies par défaut et correspondent aux valeurs par défaut en cas d'installation locale. Vous pouvez

modifier les paramètre du fichier d'installation en modifiant celui-ci (cf. point 6.1.2, page131).

Etape 11. Saisie du nom paquet d'insallation

La première fenêtre de l'Assistant est une fenêtre d'introduction. Vous devez obligatoirement saisir le nom du paquet d'instalation (champ **Nom**).

Etape 12. Connexion du fichier descriptif du paquet d'installation

Dans cette fenêtre de l'Assistant, il convient d'indiquer l'application à installer (cf. ill. 64). Dans la liste déroulante, sélectionnez : **Générer le paquet d'application Kaspersky Lab** et à l'aide du bouton **Parcourir**, sélectionnez le fichier avec la description de l'application (il s'agit d'un fichier **.kpd** qui fait partie de la distribution de Kaspersky Anti-Virus 5.0 for Windows Workstations). Les champs contenant le nom de l'application et le numéro de série sont remplis automatiquement.

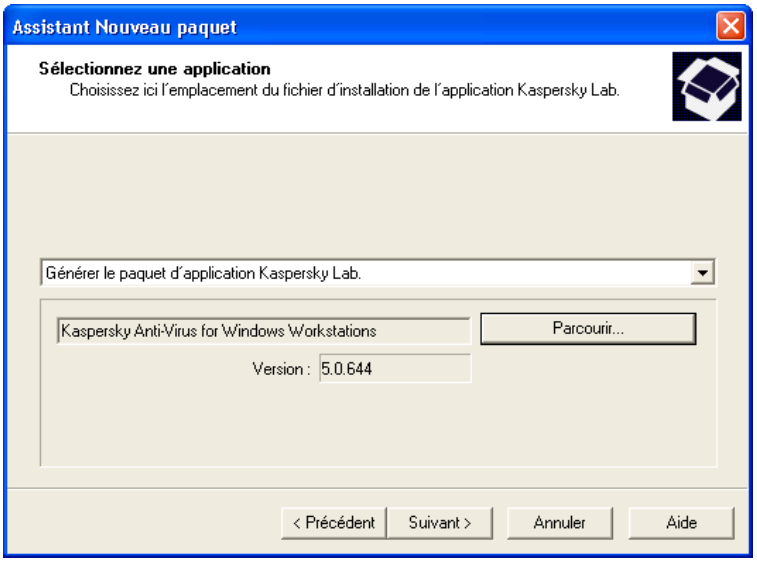

Illustration 64. Création du paquet d'installation. Sélection de l'application à installer

Etape 13. Sélection du fichier de clé de licence

Cette fenêtre de l'Assistant (cf. ill. 65) vous permet d'indiquer la clé de licence qui sera intégrée au paquet d'installation. Pour ce faire, cliquez sur **Parcourir** et sélectionnez le fichier de clé de licence requis (fichier * **.key**).

Si vous ne souhaitez pas inclure la clé de licence dans le paquet d'installation, cliquez sur **Suivant >**.

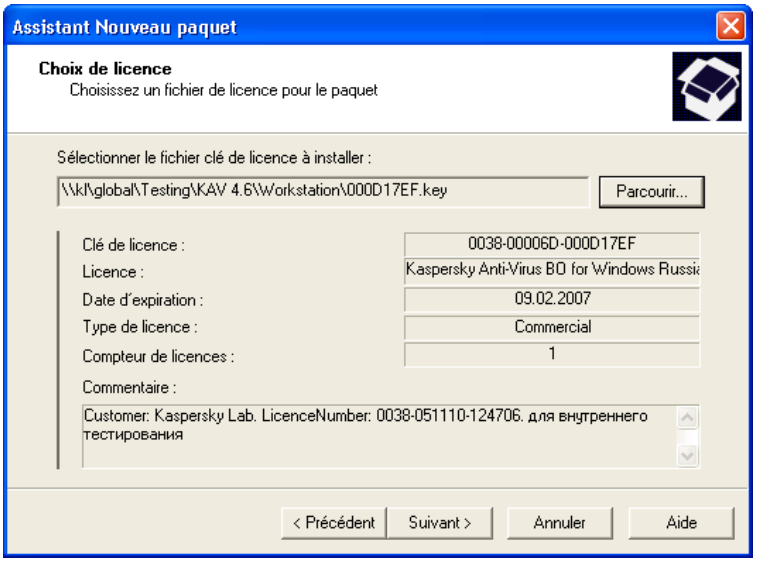

Illustration 65. Création d'un paquet d'installation. Sélection de la clé de licence

Etape 14. Fin de la création du paquet d'installation

Cliquez sur **Suivant >** dans la fenêtre **Téléchargement**.

L'ensemble des fichiers indispensables à l'installation de l'application sur les ordinateurs client est chargé dans le répertoire partagé du Serveur d'administration et le système vérifie si le poste de travail de l'administrateur est équipé du plug in d'administration pour l'application sélectionnée. Si le plug in n'est pas installé ou s'il s'agit d'une version antérieure à celle reprise dans la distribution, le plug sera installé ou mis à jour.

La fenêtre suivante de l'Assistant reprend les informations confirmant la réusste de la création du paquet d'installation. Le paquet ainsi créé sera ajouté au contenu du nœud **Installation distant** et présenté dans le panneau des résultats.

6.1.2. Consultation et modification des paramètres du paquet d'installation

Afin de consulter les valeurs des paramètres du paquet d'installation ou pour les modifier :

1. Dans le dossier **Installation distant**, sélectionnez le paquet d'installation que vous souhaitez modifier.
2. Ouvrez le menu contextuel de la stratégie sélectionnée et choisissez le point **Propriétés**. Cette action entraîne l'ouverture de la boîte de dialogue de configuration de la stratégie pour **Kaspersky Anti-Virus 5.0 for Windows Workstations**. Celle-ci contient plusieurs onglets.

La fenêtre **Propriétés de <Nom du paquet d'installation>** s'ouvre. Elle contient les onglets suivants : **Général**, **Paramètres d'installation**, **Info de licence** et **Redémarrage du S.E.**.

Les onglets **Général**, **Info de licence** et **Redémarrage du S.E.** sont standard pour Kaspersky Administration Kit (pour de plus amples informations, consultez le Manuel de déploiement de Kaspersky Administration Kit 5.0).

L'onglet **Paramètres d'installation** (cf. ill. 66) contient les paramètres de Kaspersky Anti-Virus 5.0 for Windows Workstations:

- **Répertoire d'installation** de l'application sur l'ordinateur client. Si le champ est vide, l'installation s'opère par défaut dans le répertoire : **<Disque>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 5.0 for Windows Workstations**.
- **Technologies de Kaspersky Lab pour la protection des données**. Cochez la case en regard de la technologie que vous souhaitez utiliser.

  

  Si vous décidez de ne pas installer certaines technologies, vous devrez réinstaller l'application sur l'ordinateur client le jour où vous déciderez de les utiliser.

- **Mot de passe pour la supprression** : mot de passe qu'il faudra saisir avant de pouvoir supprimer le logiciel. Saisissez le mot de passe dans le champ adéquat et à nouveau dans le champ **Confirmation du mot de passe**.
- **Mot de passe pour la protection du logiciel** : mot de passe pour permutter entre le mode utilisateur et le mode administrateur. Saisissez le mot de passe dans le champ adéquat et à nouveau dans le champ **Confirmation du mot de passe**.

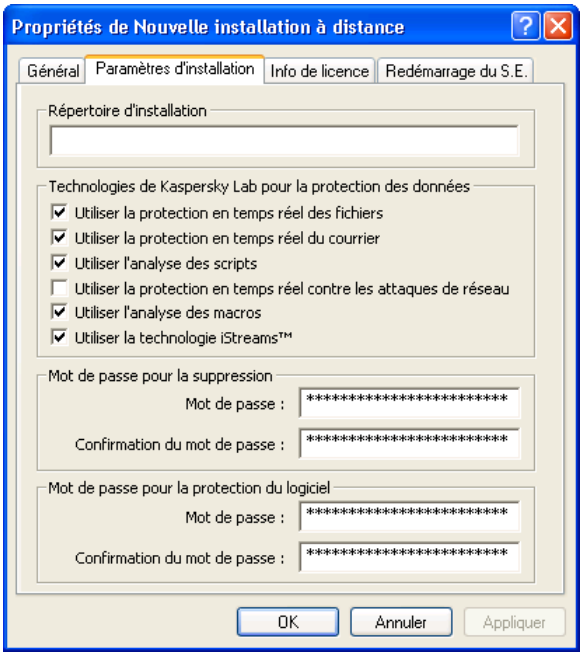

Illustration 66. Propriétés du paquet d'installation. Onglet **Paramètres d'installation**

6.2. Administration des stratégies

Cette rubrique est consacrée à la création et à la configuration de stratégies pour Kaspersky Anti-Virus 5.0 for Windows Workstations. Pour obtenir de plus amples informations sur le concept d'administration des stratégies, consultez le Manuel de l'administrateur de « Kaspersky Administration Kit 5.0 ».

6.2.1. Création d'une stratégie

Afin de créer une stratégie, réalisez les opérations suivantes :

1. Dans l'arborescence du dossier **Groupes**, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez créer la stratégie.
2. Sélectionnez le répertoire **Stratégies** faisant partie du groupe sélectionné, affichez le menu contextuel et sélectionnez

Nouveau→Stratégie… La fenêtre de création d'une nouvelle stratégie apparaîtra à l'écran.

L'interface du programme de création des stratégies se présente sous la forme d'un Assistant 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 quitter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Lors de la création de la stratégie, les paramètres sans lesquels l'application ne pourrait fonctionner sont configurés. Les autres valeurs sont les valeurs par défaut et elles correspondent aux valeurs par défaut en cas d'installation locale de l'application. Il est possible de modifier une stratégie après sa création (cf. point 6.2.2, p. 136).

Lors de la création d'une stratégie (Etape 2 – Etape 5), vous pouvez bloquer la modification des paramètres des stratégies des sous-groupes. Pour bloquer la définition des paramètres, verrouillez-les :  . Les paramètres modifiables sont indiqués par l'icône  .

Etape 1. Saisie des données générales sur la stratégie

Les premières fenêtres de l'Assistant sont destinées à la saisie d'informations. Il est indispensable d'indiquer ici le nom de la stratégie (dans le champ **Nom**) et de sélectionner **Kaspersky Anti-Virus 5.0 for Windows Workstations** dans la liste déroulante **Nom de l'application**. Afin que la stratégie créée fonctionne en tant que stratégie active de l'application, activez-la en cochant la case **Activer la stratégie** dans la fenêtre de l'Assistant.

Il est possible de définir plusieurs stratégie avec différents paramètres dans le groupe pour une stratégie. Ceci étant dit, il ne peut y avoir qu'une seule stratégie active pour l'application. Il est possible d'activer une stratégie qui n'est pas active en fonction des événements, ce qui permet, par exemple, de définir des paramètres de protection antivirus plus stricte lors d'épidémies de virus.

Etape 2. Choix du niveau de protection en temps réel

Sélectionnez à ce stade le niveau de protection antivirus (cf. point 4.2, p. 42) selon lequel la protection en temps réel sera organisée.

Etape 3. Choix du niveau de protection pour l'analyse à la demande

Sélectionnez à ce stade le niveau de protection antivirus (cf. point 4.2, p. 42) selon lequel la protection pour l'analyse à la demande sera organisée ainsi que l'action qui sera exécutée en cas de découverte d'un objet suspect ou infecté (cf. point 5.3.3.2, p. 86).

Le bouton **Configuration…** ouvre une fenêtre qui vous permettra de définir les paramètres de l'analyse à la demande (cf. ill. 71). Si vous modifiez les paramètres de l'un des niveaux prédéfinis, vous passerez automatiquement au mode **Paramètres utilisateur**.

Etape 4. Sélection de l'origine des mises à jours

C'est à cette étape (cf. ill. 67) que vous devez configurer la mise à jour des bases antivirus et des modules de l'application : définir la source de la mise à jour et configurer les paramètres du réseau local dans la fenêtre qui s'ouvre lorsque vous cliquez sur **Paramètres LAN**. Tous les paramètres sont identiques aux paramètres locaux. Pour de plus amples informations, consultez le point 5.1.3 à la page 47.

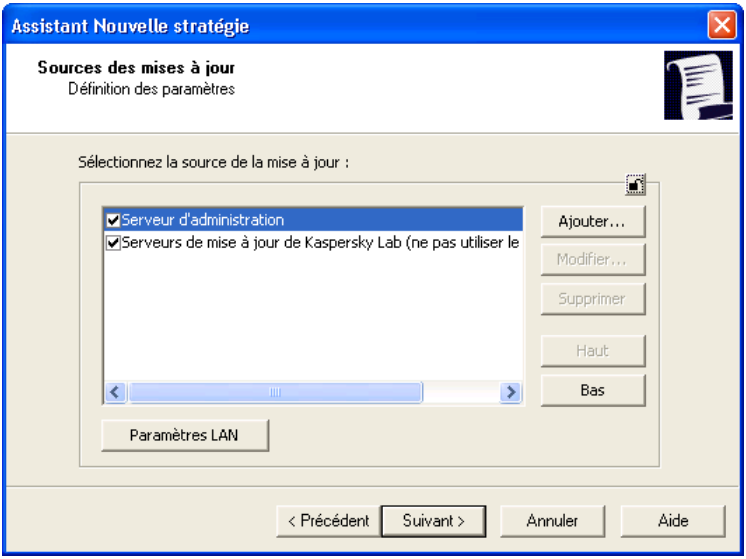

Illustration 67. Sélection de la source des mises à jour

Etape 5. Sélection des paramètres du service de mises à jour

Cette fenêtre (cf. ill. 68) vous permet de définir les paramètres du service des mises à jour des modules l'application. Tous les paramètres sont identiques aux paramètres locaux. Pour de plus amples informations, consultez le point 5.1.3 à la page 47 :

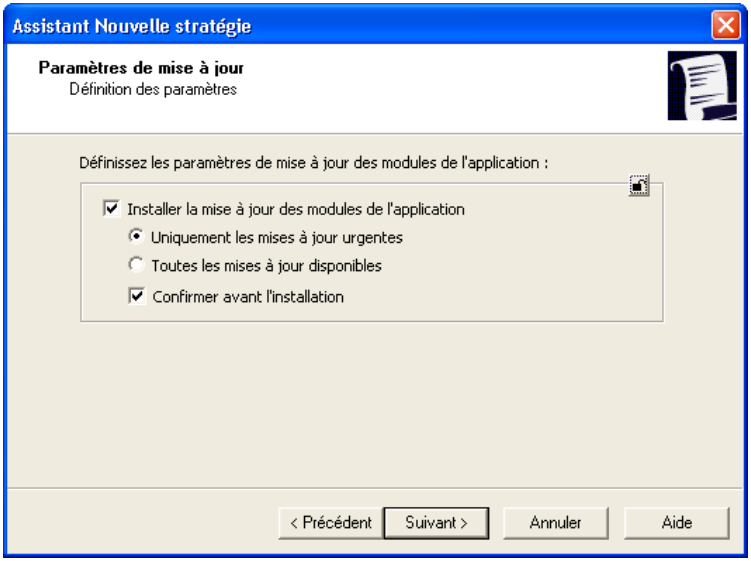

Illustration 68. Sélection des paramètres du service de mise à jour

Etape 6. Fin de la création d'une stratégie

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

Une fois que vous aurez quitté l'Assistant, la stratégie pour l'application sélectionnée sera ajoutée au dossier **Stratégies** du groupe correspondant. Elle apparaîtra également dans le panneau des résultats.

Pour appliquer une stratégie, modifiez ses paramètres et imposez des restrictions quant à la modification des paramètres si cela n'a pas été fait lors de la création de la stratégie. La stratégie sera diffusée sur les ordinateurs client lors de la première synchronisation entre les clients et le serveur d'administration.

L'application de la stratégie s'opère de la manière suivante : si des tâches résidentes (tâches liées à la protection en temps réel) sont exécutées sur

l'ordinateur client, elles seront exécutées selon les nouveaux paramètres. Les tâches exécutées périodiquement (analyse à la demande, mise à jour des bases antivirus) seront toujours exécutées selon les anciens paramètres. Tout nouveau lancement d'une tâche sera réalisé selon les paramètres modifiés.

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 **Action**. Le déplacement peut également être réalisé à l'aide de la souris.

6.2.2. Examen et modification des paramètres de la stratégie

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

Pour interdire la redéfinition des paramètres, il faut les « verrouiller » :  . L'icône  indique les paramètres qui peuvent être modifiés.

Pour examiner la valeur des paramètres de la stratégie et / ou introduire des modifications :

1. Dans l'arborescence du dossier **Groupes**, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez modifier les paramètres.
2. Sélectionnez le dossier **Stratégies** faisant partie de ce groupe. Toutes les stratégies définies pour ce groupe seront reprises dans le panneau des résultats.
3. Dans la liste des stratégies, pointez la souris sur la stratégie définie pour **Kaspersky Anti-Virus 5.0 for Windows Workstations** (le nom de l'application est repris dans le champ **Application**).
4. Ouvrez le menu contextuel pour la stratégie sélectionnée et utilisez la commande **Propriétés**. La fenêtre des paramètres de la stratégie de **Kaspersky Anti-Virus 5.0 for Windows Workstations** apparaîtra à l'écran. Elle reprend plusieurs onglets.

Les onglets **Général**, **Contrôle** et **Traitement des événements** sont standard dans Kaspersky Administration Kit (pour de plus amples informations, consultez le manuel de Kaspersky Administration Kit 5.0).

Les autres onglets contiennent les paramètres de Kaspersky Anti-Virus 5.0 for Windows Workstations. Vous trouverez ci-après une description détaillée de chacun de ces onglets.

Les paramètres de la stratégie pour les composants particuliers de la protection en temps réel sont appliqués uniquement sur les ordinateurs où ces composants sont installés.

6.2.2.1. Examen des renseignements relatifs à la stratégie

L'onglet **Général** (cf. ill. 69) reprend des renseignements d'ordre généraux sur la stratégie :

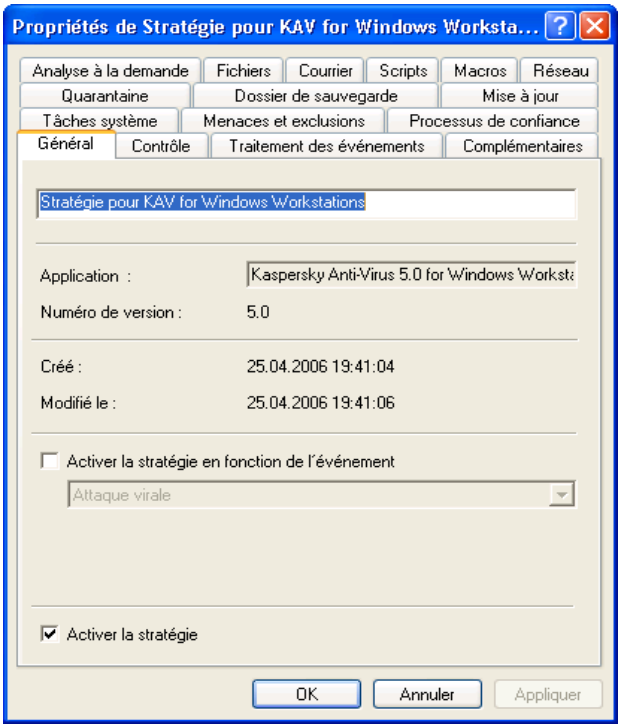

Illustration 69. Onglet **Général**

- Le nom de la stratégie ;
- L'application pour laquelle la stratégie a été définie (**Kaspersky Anti-Virus 5.0 for Windows Workstations**) ;
- La version de l'application ;

- La date et l'heure de création de la stratégie ;
- La date et l'heure de la dernière modification de la stratégie.

Vous pouvez changer le nom de la stratégie.

Si vous souhaitez que la stratégie devienne la stratégie active, cochez la case **Activer la stratégie**. Si vous souhaitez que l'activation d'une stratégie s'opère automatiquement lorsqu'un événement particulier survient, cochez la case **Activer la stratégie en fonction de l'événement** et sélectionnez l'événement en question dans la liste déroulante. Le retour à la stratégie antérieure s'effectue manuellement.

6.2.2.2. Analyse à la demande

L'onglet **Analyse à la demande** (cf. ill. 70) vous permet de configurer la stratégie pour l'analyse à la demande.

Dans la section **Configuration du niveau de protection**, sélectionnez à l'aide du menu déroulant un des trois niveaux de protection antivirus prédéfinis (cf. 4.2, p. 42).

La section **Actions à réaliser sur les objets découverts** permet de définir le type d'action qui sera exécutée en cas de découverte d'objets infectés ou suspects (pour de plus amples informations sur les actions réalisées par Kaspersky Anti-Virus pendant l'analyse à la demande consultez le point 5.3.3.2 à la page 86).

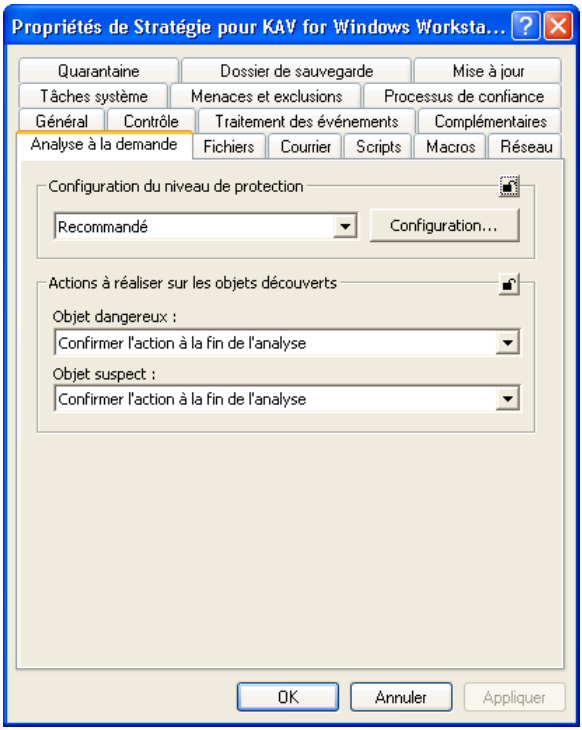

Illustration 70. Onglet **Analyse à la demande**

Le bouton **Configuration…** ouvre une fenêtre qui vous permet de consulter les paramètres correspondant au niveau sélectionné ou de réaliser votre propre configuration sur la base de ceux-ci. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**.

La fenêtre **Configuration de l'analyse à la demande** reprend les onglets **Objets à analyser** et **Complémentaire**.

L'onglet **Objets à analyser** (cf. ill. 71) vous permet de définir les objets à analyser et leur type (pour de plus amples informations, consultez le point 5.3 à la page. 75) ainsi que dresser les listes d'exclusion.

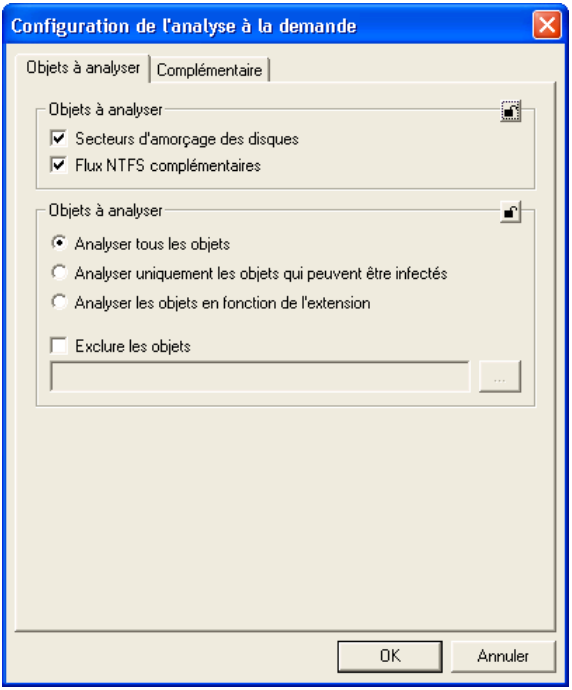

Illustration 71. Onglet **Objets à analyser**

L'onglet **Complémentaire** (cf. ill. 72) vous permet d'activer ou de désactiver l'analyse pour toute une série de fichiers, d'exclure de l'analyse les riskwares de confiance, afficher la fenêtre de saisie du mot de passe lors de l'analyse d'archives protégées ainsi que d'introduire certaines restrictions sur l'analyse.

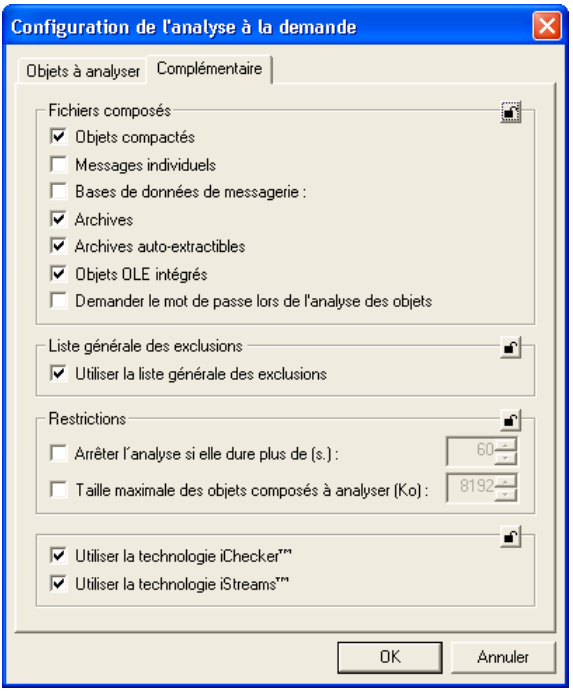

Illustration 72. Onglet **Complémentaire**

6.2.2.3. Protection en temps réel des objets du système de fichiers

Les paramètres de stratégie pour la protection en temps réel des fichiers sont appliqués uniquement sur les ordinateurs où ce composant est installé.

L'onglet **Fichiers** (cf. ill. 73) vous permet de configurer la stratégie pour la protection en temps réel des objets du système de fichiers. La sélection du niveau de protection et le passage à la fenêtre des détails sont identiques à ceux de l'onglet **Analyse à la demande** (cf. point 6.2.2.2, p 138).

Définissez dans la section **Actions à réaliser sur les objets découverts** le type d'action qui sera exécuté en cas de découverte d'objets infectés ou suspects (pour de plus amples informations sur les actions réalisées par Kaspersky Anti-Virus dans le cadre de la protection en temps réel, consultez le point 5.2.1.2 à la page 62.)

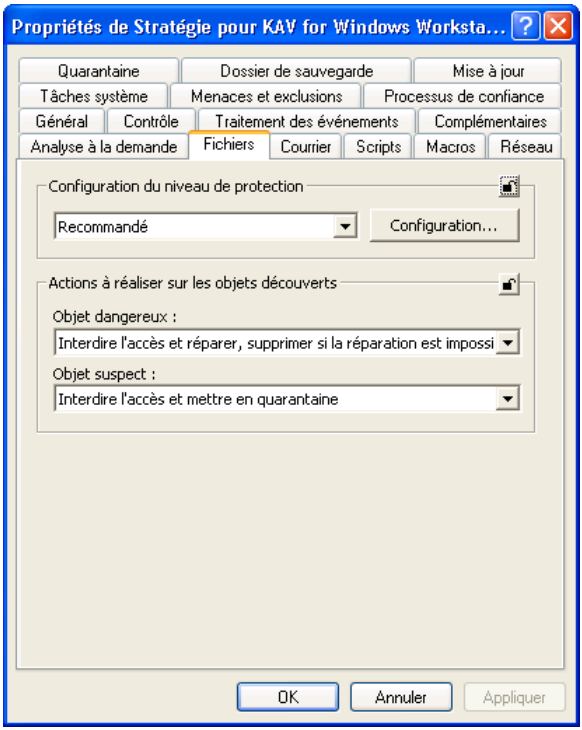

Illustration 73. Onglet **Fichiers**

L'onglet **Objets à analyser** (cf. ill. 74) vous permet de définir les objets à analyser, et de dresser la liste des exclusions. Ces paramètres sont identiques aux paramètres locaux. Pour de plus amples informations, consultez le point 5.2.1 à la page 59.

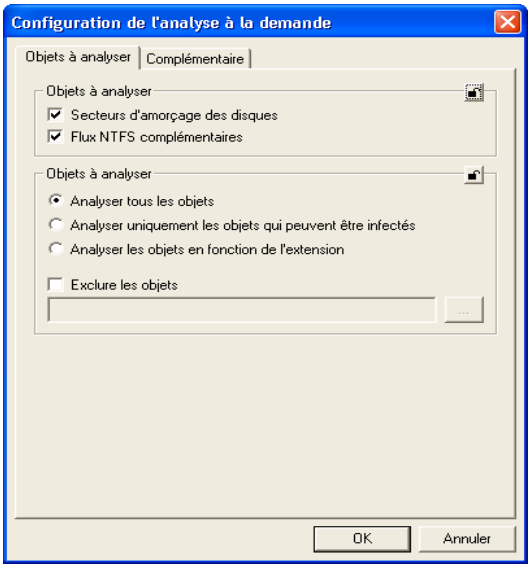

Illustration 74. Onglet **Objets à analyser**

L'onglet **Complémentaire** (cf. ill. 75) vous permet d'activer ou non l'analyse de différents fichiers, d'exclure de l'analyse les riskwares de confiance, de limiter la durée de l'analyse et d'appliquer ou non les technologies iChecker et iStreams (pour de plus amples informations, consultez le point 5.2.1, à la page 59).

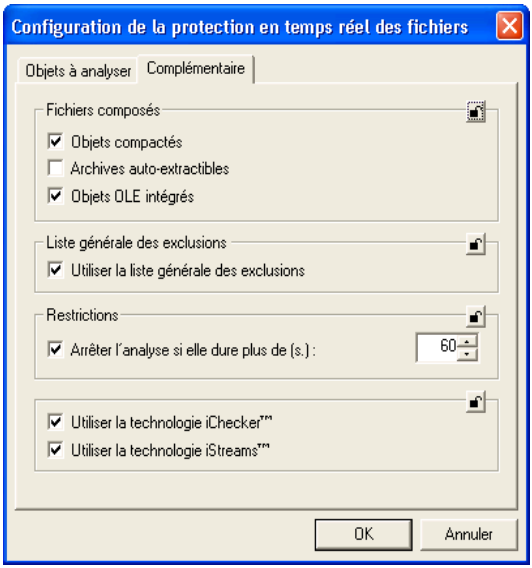

Illustration 75. Onglet **Complémentaire**

6.2.2.4. Menaces et exclusions

L'onglet **Menaces et exclusions** (cf. ill. 76) reprend les bases antivirus qui seront utilisées pendant l'analyse (standard ou étendues). C'est au départ de cet onglet également que vous pouvez composer la liste des exclusions de l'analyse. Ces paramètres sont identiques à ceux de l'interface locale (consultez les points 5.1.3.5 et 5.7 aux pages 55 et 99 pour obtenir de plus amples renseignements).

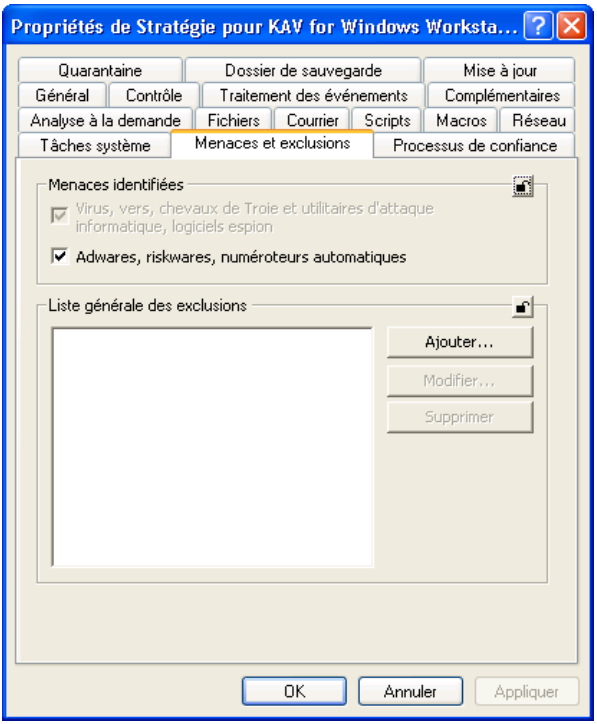

Illustration 76. Onglet **Menaces et exclusions**

6.2.2.5. Contrôle de l'activité des processus logiciels

L'onglet **Processus de confiance** (cf. ill. 77) vous permet de configurer la politique du contrôle antivirus des processus de certains programmes. Ces paramètres sont identiques aux paramètres de l'interface locale (pour de plus amples informations, consultez le point 5.4 à la page 92).

Lors de la saisie du chemin d'accès au fichier, il faut saisir le chemin d'accès au fichier du processus sur l'ordinateur distant.

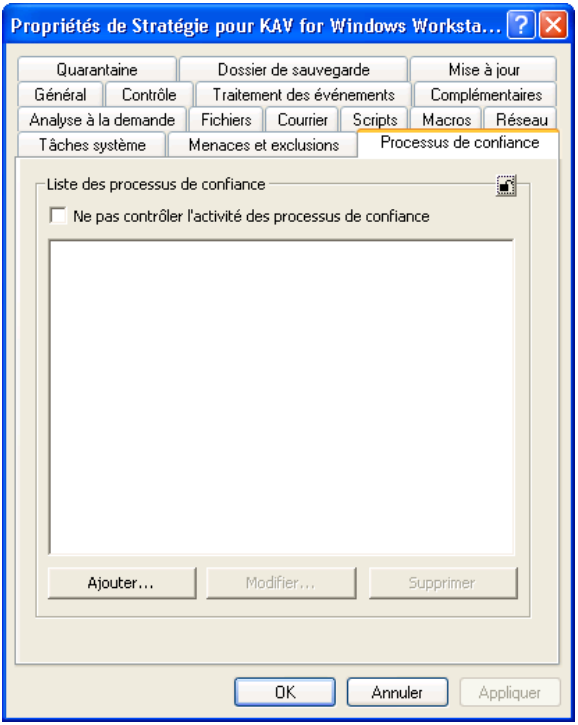

Illustration 77. Onglet **Processus de confiance**

6.2.2.6. Analyse du courrier

Les paramètres de stratégie pour la protection en temps réel du courrier sont appliqués uniquement sur les ordinateurs où ce composant est installé.

L'onglet **Courrier** (cf. ill. 78) vous permet de configurer la stratégie pour l'analyse du courrier entrant et sortant. La sélection du niveau de protection et l'ouverture de la fenêtre de configuration détaillée sont identiques à l'onglet **Analyse à la demande** (cf. point 6.2.2.2, p. 138).

La section **Actions à exécuter sur les objets découverts** permet de définir le type d'action qui sera exécutée en cas de découverte d'objets infectés ou suspects (pour de plus amples informations sur les actions réalisées par Kaspersky Anti-Virus pendant l'analyse du courrier, consultez le point 5.3.3.2 à la page 86).

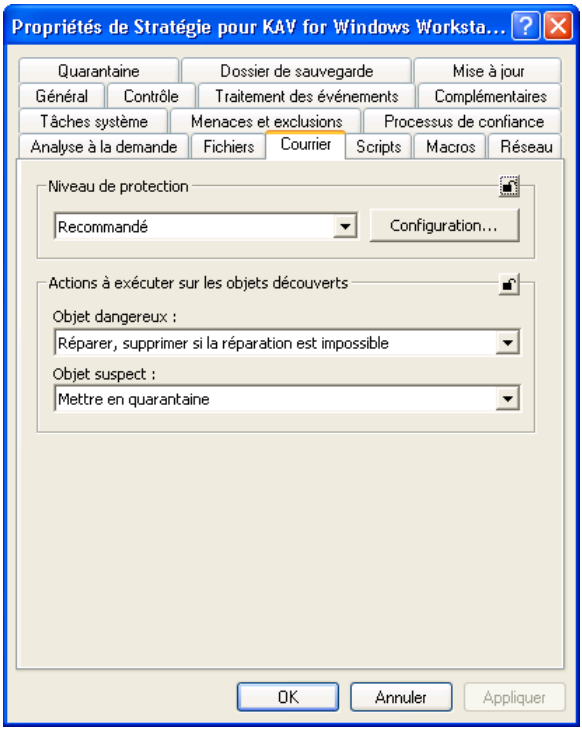

Illustration 78. Onglet **Courrier**

Il est indispensable de sélectionner dans l'onglet **Objets à analyser** (cf. ill. 79) les objets qui seront soumis à l'analyse et de dresser la liste des exclusions de l'analyse du courrier. Ces paramètres sont identiques aux paramètres locaux.(Pour de plus amples informations, consultez le point 5.2.2, p 64).

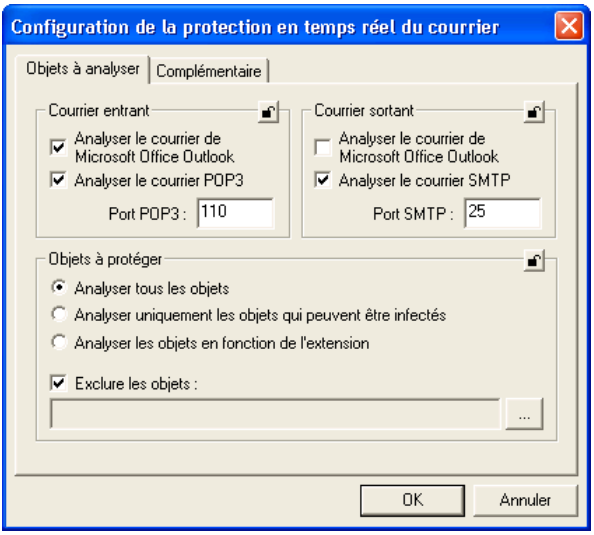

Illustration 79. Onglet **Objets à analyser**

L'onglet **Complémentaire** (cf. ill. 80) vous permet d'autoriser ou non l'utilisation de la technologie iChecker et de définir quelques restrictions pour l'analyse du courrier (pour de plus amples informations, consultez le point 5.2.1, à la page 59).

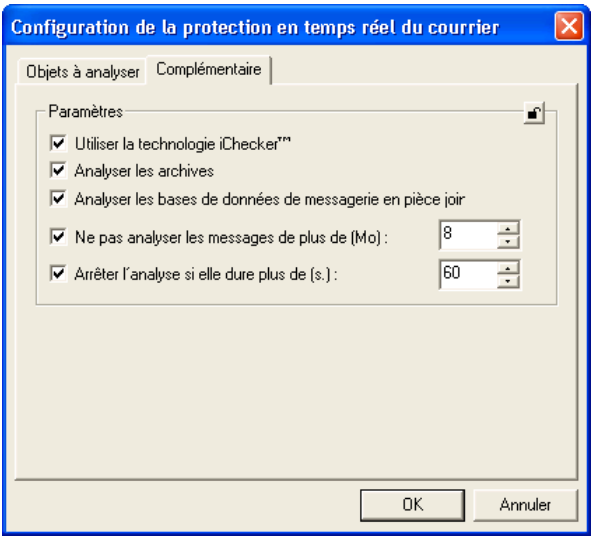

Illustration 80. Onglet **Complémentaire**

6.2.2.7. Analyse des scripts

Les paramètres de stratégie pour l'analyse des scripts sont appliqués uniquement sur les ordinateurs où ce composant est installé.

Dans l'onglet **Scripts** (cf. ill. 81), vous pouvez configurer la stratégie pour la protection en temps réel contre les scripts VBScript et JavaScript qui représentent un danger potentiel. Choisissez l'une des options suivantes :

- **Bloquer l'exécution du script** (option par défaut);
- **Autoriser l'exécution du script;**
- **Confirmer l'action auprès de l'utilisateur.**

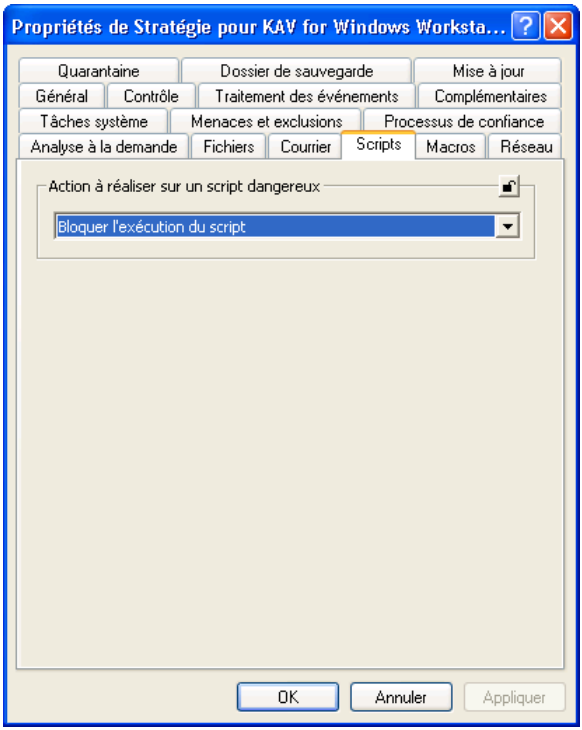

Illustration 81. Onglet **Scripts**

6.2.2.8. Analyse des macros

Les paramètres de stratégie pour l'analyse des macros sont appliqués uniquement sur les ordinateurs où ce composant est installé.

L'onglet **Macros** (cf. ill. 82) vous permet de configurer la stratégie pour l'analyse des macros VBA utilisées dans les applications de bureautique.

La sélection du niveau de protection et le passage à la fenêtre des détails sont identiques à ceux de l'onglet **Analyse à la demande** (cf. point 6.2.2.2, p 138).

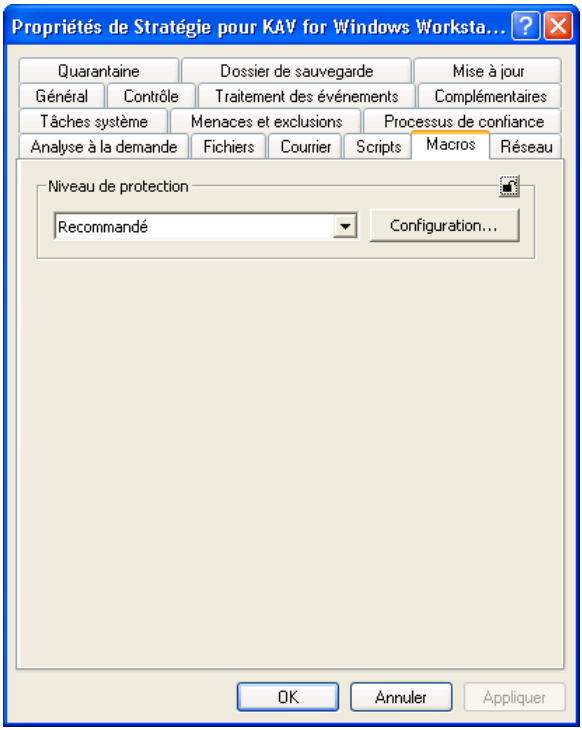

Illustration 82. Onglet **Macros**

Le bouton **Configuration…** entraîne l'ouverture (cf. ill. 83) d'une fenêtre avec plusieurs onglets reprenant les principaux types de macros contrôlées par Kaspersky Anti-Virus.

Les macros ont été réparties en cinq types :

- **Modules** : macros utilisées avec les modules du projet :
    - Copie des modules (OrganizerCopy) ;
    - Suppression des modules (OrganizerDelete);
    - Changement de nom des modules (OrganizerRename) ;
    - Ajout d'un module ;
    - Suppression du module ;
    - Importation des modules ;
    - Exportation des modules.

- **Lignes** : macros pour la modification du code des macros :
    - Création de procédure ;
    - Insertion de ligne de la macro dans le module depuis le fichier ;
    - Ajout d'une ligne à la macro ;
    - Insertion d'une ligne dans la macro ;
    - Remplacement de lignes dans la macro ;
    - Suppression de lignes de la macro.
- **Fichiers** : opérations sur les fichiers :
    - Suppression des fichiers ;
    - Remplacement des attributs du fichier ;
    - Création des dossiers ;
    - Suppression des dossiers ;
    - Ouverture du fichier en mode écriture.
- **ActiveX** : opération sur les objets ActiveX :
    - Création des objets ActiveX ;
    - Création d'un objet ActiveX sur un ordinateur distant ;
    - Accès à l'objet ActiveX.
- **Drivers** : macros diverses
    - Désactiver la demande de confirmation de l'enregistrement de Normal;
    - Copie des feuilles Excel ;
    - Désactivation de la protection antivirus ;
    - Exécution de la commande MacroCopy ;
    - Exécution des commandes Shell;
    - Appel de la fonction API ;
    - Emulation de la frappe du clavier.

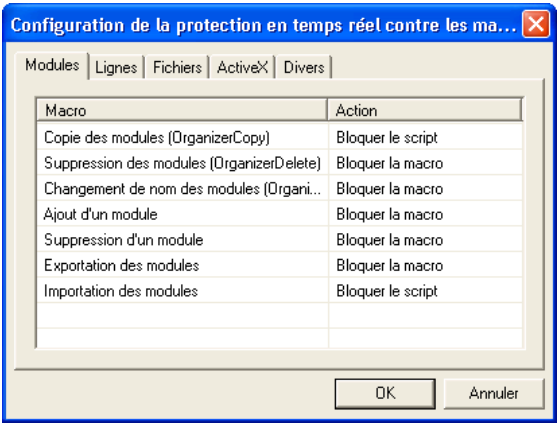

Illustration 83. Liste des macros

Dans la colonne **Action** (cf. ill. 83) en regard du nom de chaque macro, vous trouverez le type d'actions qui sera exécuté par Kaspersky Anti-Virus lors de la découverte de la macro en question. Les actions proposées varient en fonction du niveau de protection sélectionné. Vous avez le choix entre :

- Autoriser la macro.
- Confirmer l'action
- Bloquer la macro.
- *Bloquer le script* : arrêt complet de l'activité de la macro.

Afin de modifier l'action exécutée par Kaspersky Anti-Virus lors de la découverte d'une macro suspecte :

Faites un clic gauche sur le nom de l'action en regard de la commande et sélectionnez une nouvelle valeur dans la liste déroulante.

6.2.2.9. Protection contre les attaques de réseau

Les paramètres de stratégie pour la protection contre les attaques de réseau sont appliqués uniquement sur les ordinateurs où ce composant est installé.

Vous pouvez définir les paramètres de la protection contre les attaques de réseau sur l'onglet **Réseau** (cf. ill. 84). Ces paramètres sont identiques à ceux de

l'interface locale (pour plus de plus amples informations, consultez le point 5.2.6 à la page 73).

Dans la section **Action en cas de redémarrage indispensable**, sélectionnez l'action qui sera exécutée suite à la réception de la mise à jour des bases d'attaques de réseau ou lors de l'activation/désactivation de la protection contre les attaques de réseau (cf. point 5.2.6, p. 73). Choisissez l'une des options suivantes :

- *Confirmer auprès de l'utilisateur*. Dans ce cas, une fenêtre contenant une requête de redémarrage du poste de travail s'affiche.
- *Ne pas confirmer auprès de l'utilisateur, remettre au redémarrage*. Cette action est sélectionnée par défaut.
- *Ne pas confirmer auprès de l'utilisateur, redémarrer immédiatement*. Dans ce cas, le poste de travail sera redémarré directement après la réception de la mise à jour des bases d'attaques de réseau.

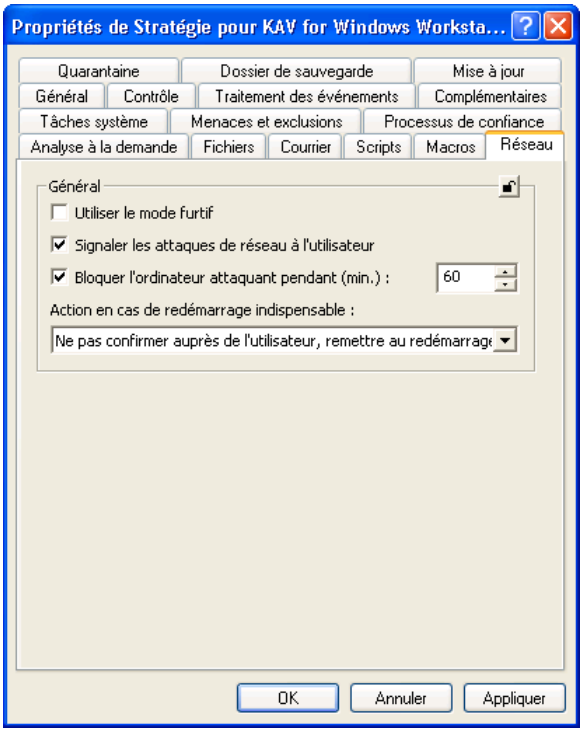

Illustration 84. Onglet **Réseau**

6.2.2.10. Mise à jour des bases antivirus et des modules de l'application

L'onglet **Mise à jour** (cf. ill. 85) vous permet de modifier les paramètres de la mise à jour des bases antivirus et des modules de l'application définis au moment de la création de la stratégie.

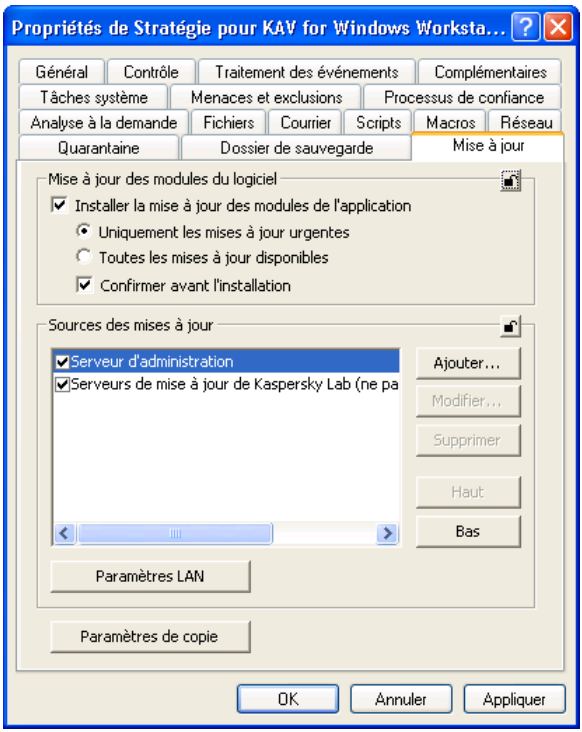

Illustration 85. Onglet **Mise à jour**

L'onglet **Mise à jour** comprend les sections suivantes : **Mises à jour des modules du logiciel** qui permettent de définir les paramètres du service des mises à jour des bases antivirus et de l'application: (cf. Etape 5 à la page 135) et la section **Sources des mises à jour** qui indique l'origine de la mise à jour des bases antivirus et des modules de l'application et ses paramètres (cf. Etape 3 à la page 134).

Le bouton **Paramètres LAN** vous permet de configurer le serveur proxy (pour de plus amples informations, consultez le point 5.1.3.4 à la page 54). Dans le champ **Temps de connexion maximum (s.)**, vous pouvez définir le délai

d'attente de la connexion avec le serveur de mise à jour (en secondes). Une fois ce délai écoulé, la tâche passera à une autre source de mise à jour (dans la liste) ou la mise à jour sera interrompue (lorsqu'aucune autre source de mise à jour n'a été définie).

La fenêtre qui s'ouvre lorsque vous cliquez sur **Paramètres de copie** vous permet d'activer la copie des mises à jour dans la source locale et de la configurer (cf. point 5.1.3, p. 47).

6.2.2.11. Utilisation des tâches systèmes

L'onglet **Tâches systéme** (cf. ill. 86) vous permet d'activer ou de désactiver le lancement automatique des tâches système (cf. point 5.4, p. 92) et des tâches de protection en temps réel sur les postes de travail distant qui font partie du groupe d'administration.

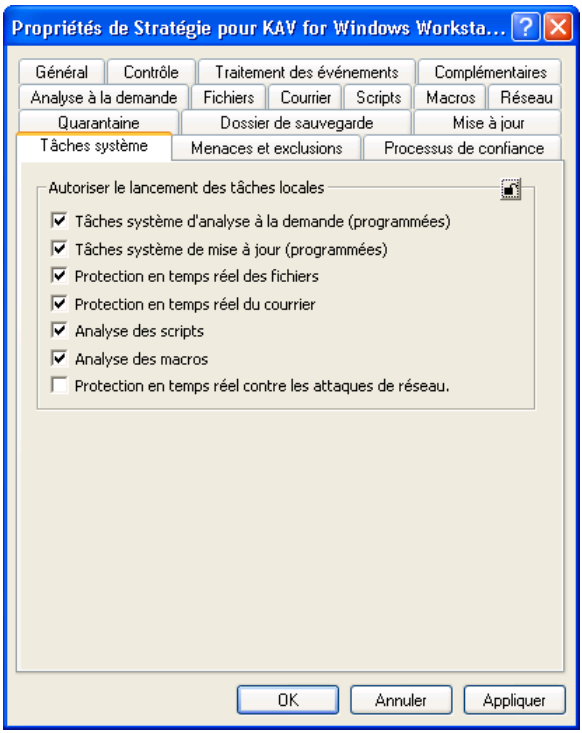

Illustration 86. Onglet **Tâches systéme**

6.2.2.12. Configuration de la quarantaine et du dossier de sauvegarde

Les onglets **Quarantaine** (cf. ill. 87) et **Dossier de sauvegarde** (cf. ill. 88) permettent la configuration de la stratégie appliquée à la quarantaine et au dossier de sauvegarde.

Ces paramètres sont identiques à deux de la quarantaine et du dossier de sauvegarde dans le cadre de l'administration via l'interface locale (cf. point 5.10.1.1, p. 109).

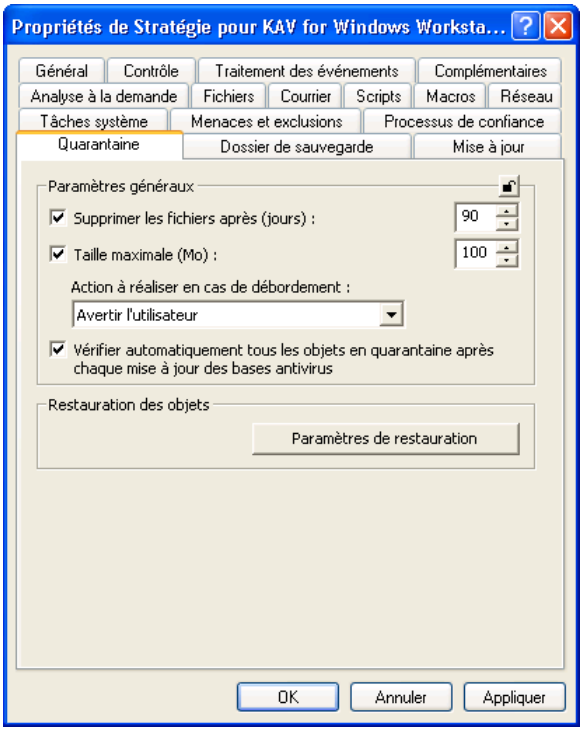

Illustration 87. Onglet **Quarantaine**

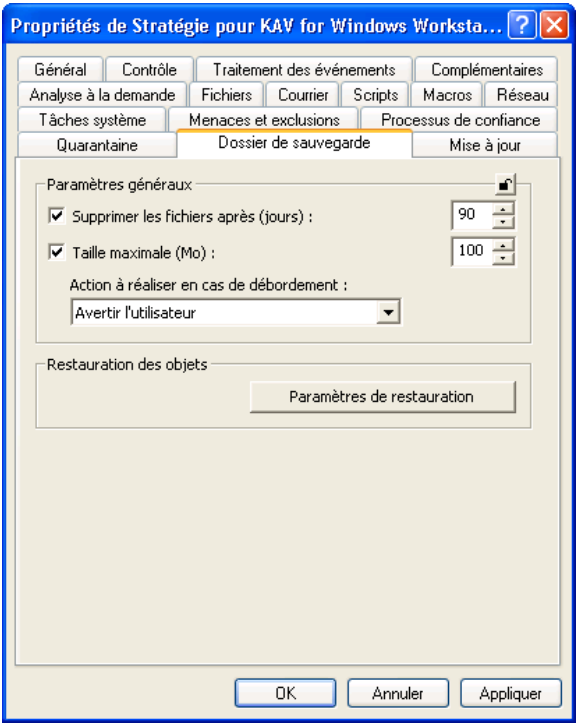

Illustration 88. Onglet **Dossier de sauvegarde**

6.2.2.13. Constitution du rapport sur l'activité de l'application

L'onglet **Traitement des événements** (cf. ill. 89) regroupe les types d'événements qui surviennent pendant l'utilisation de l'application et qui seront consignés dans le rapport ainsi que l'emplacement où sont conservées les données et le mode d'avertissement de l'administrateur et / ou des autres utilisateurs.

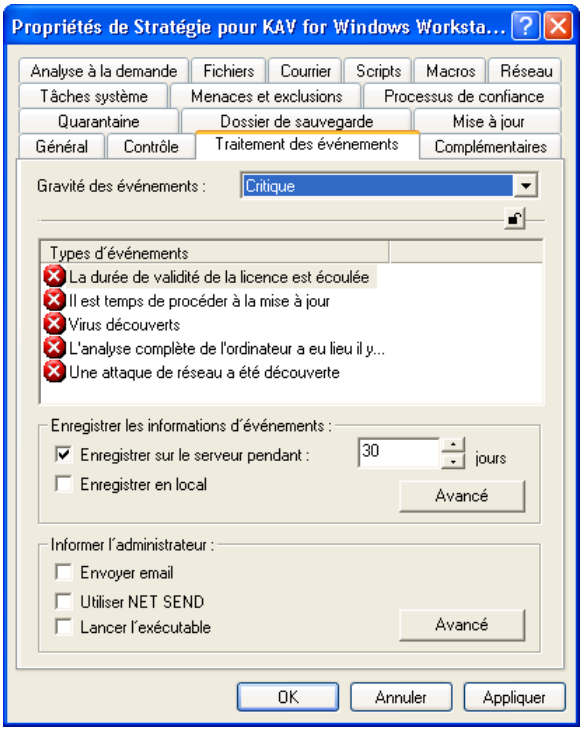

Illustration 89. Onglet **Traitement des événements**

Kaspersky Anti-Virus 5.0 for Windows Workstations génère un ensemble définis d'événements pendant son utilisation (cf. Tableau. 2). Chaque événement est accompagné d'une caractéristique qui reflète son degré d'importance. Il existe quatre degrés :

- **Critique**
- **Erreur**
- **Avertissement**
- **Info**

Les événements d'un même type peuvent avoir différents degrés d'importance en fonction du contexte dans lequel il se sont produits.

Sélectionnez dans la liste déroulante **Gravité des événements** le degré de gravité de l'événement. En dessous de la liste se trouve un champ reprenant les informations sur les types d'événement du degré d'importance que vous avez sélectionné.

Tableau 2. Evénements de l'application

Événement	Degré d'importance
Objet réparé	**Avertissement**
Objet infecté supprimé	**Avertissement**
Modification du niveau de protection en temps réel	**Info**
La licence arrive en fin de validité (deux semaines avant la date limite)	**Avertissement**
La licence est expirée	**Critique**
L'analyse de la licence a échoué	**Erreur**
Découverte d'un objet suspect	**Avertissement**
Erreur de fonctionnement	**Avertissement** **Erreur**
Il est temps de procéder à la mise à jour : - une semaine* - deux semaines*	 **Avertissement** **Evénement critique**
Virus découvert	**Critique**
Une attaque de réseau a été découverte	**Evénement critique**
Erreur interne	**Erreur**
Le système d'exploitation a redémarré	**Avertissement**
L'application a redémarré	**Avertissement**
Découverte d'une archive protégée par un mot de passe	**Avertissement**

Événement	Degré d'importance
Objet non réparé	**Avertissement**
L'analyse complète de l'ordinateur a eu lieu il y a longtemps : - il y a deux semaines* - il y a un mois*	 **Avertissement** **Critique**
L'objet infecté a été bloqué	**Avertissement**
L'objet infecté a été ignoré	**Avertissement**

*Ces valeurs sont définies par défaut. Vous pouvez les modifier dans la fenêtre Avertissement (cf. point 6.2.2.14, page 161).

Pour chaque événement, vous pouvez préciser s'il doit être repris ou non dans le rapport et définir les paramètres d'avertissement de l'administrateur lorsque l'événement survient.

Pour obtenir de plus amples informations sur les autres paramètres de l'onglet **Traitement des événements**, consultez le manuel de Kaspersky Administration Kit 5.0.

6.2.2.14. Options avancées

L'onglet **Complémentaires** (cf. ill. 90) reprend les paramètres de service de Kaspersky Anti-Virus 5.0 for Windows Worskstation. La majorité des paramètres est identique aux paramètres complémentaires décrit au point 5.10.4 à la page 120).

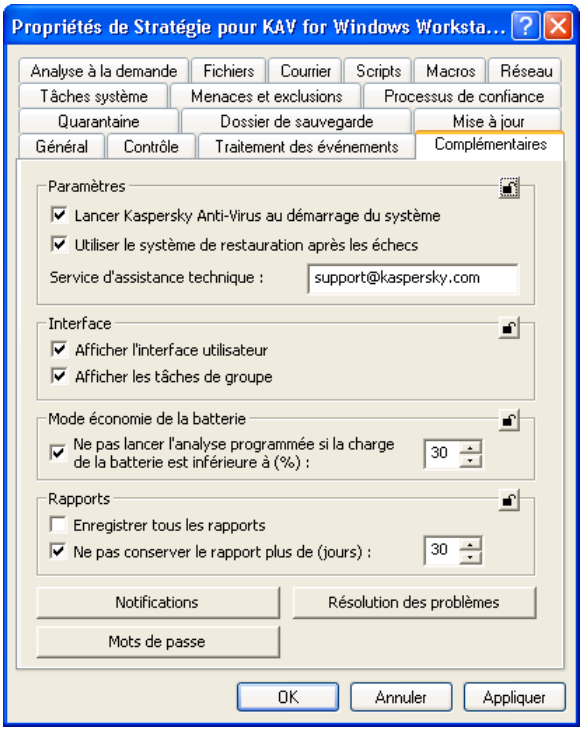

Illustration 90. Onglet **Complémentaires**

La fenêtre qui s'ouvre lorsque vous cliquez sur **Mots de passe** vous permet de définir les mot des passe (cf. ill. 91) suivant :

- Mot de passe pour la permutation entre le mode administrateur et le mode utilisateur (cf. point 5.10.7, p. 126). Pour activer ce mode, cochez la case **Protéger le logiciel avec un mot de passe**;
- Mot de passe requis pour la suppression de Kaspersky Anti-Virus. Cela évitera la suppression non autorisée de Kaspersky Anti-Virus du poste de travail.

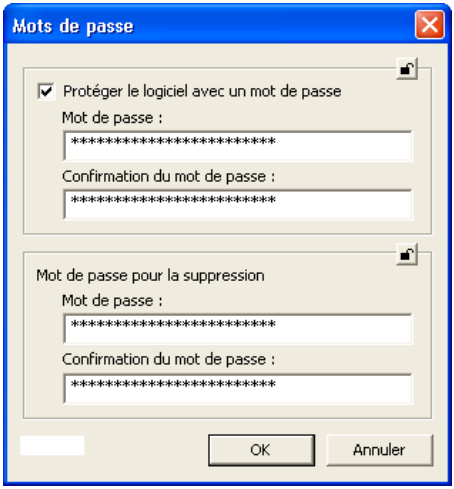

Illustration 91. Fenêtre **Mots de passe**

La fenêtre qui s'ouvre lorsque vous cliquez sur **Notifications** (cf. ill 92) vous permet de configurer l'envoi de différents types de notification:

- **Afficher la notification en cas de découverte d'un objet dangereux** : affiche à l'écran un message qui avertit l'utilisateur qu'un virus a été découvert
- **Afficher les messages informatifs**: autorise l'affichage à l'écran des messages qui accompagnent le fonctionnement de Kaspersky Anti-Virus.
- **Animer l'icône dans la barre des tâches** : anime l'icône de Kaspersky Anti-Virus dans la barre des tâches pendant l'analyse antivirus.
- **Utiliser la sonorisation** : active l'émission d'effets sonores pour avertir l'utilisateur de l'affichage d'un message particulier.

Dans la section **Notifications des événements**, vous pouvez définir les conditions dans lesquelles les notifications relatives à la progression de la mise à jour ou de l'analyse complète de l'ordinateur sont envoyées. Pour chacune de ces tâches, il existe deux niveaux de gravité : **avertissement** et **événement critique**.

Dans le champ situé à droite de chaque événement, saisi la durée (en jours) après laquelle l'utilisateur recevra chaque jour lors du démarrage de Kaspersky Anti-Virus les notifications correspondantes. Cette période commence à compter à partir de la dernière exécution de la tâche en question.

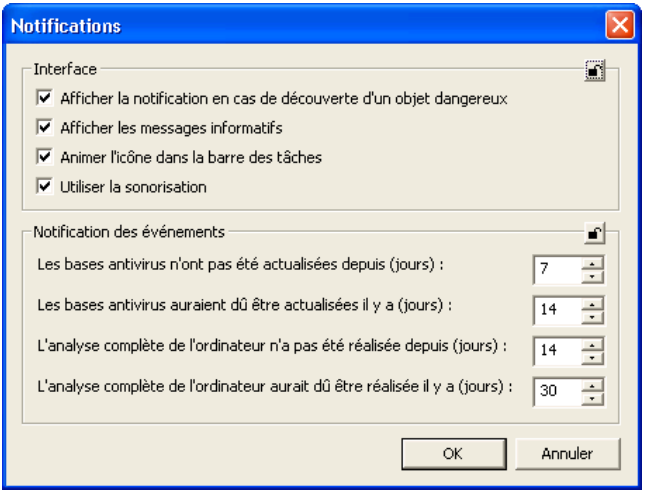

Illustration 92. Fenêtre **Notifications**

La fenêtre qui s'ouvre (cf. ill. 93) lorsque vous cliquez sur **Résolution des problèmes** (cf. ill. 90) permet de configurer les paramètres d'optimisation de l'exécution de l'analyse à la demande. La configuration de ces paramètres est identique à celle effectuée via l'interface locale (Pour de plus amples informations, consultez le point 5.10.4 à la page 120). Vous pouvez :

- **Désactiver l'analyse du courrier lors de l'exécution de la tâche** : désactiver l'analyse du courrier lors de l'exécution de la tâche Analyse de mon poste de travail.
- **Arrêter l'analyse antivirus lorsque la charge du systиme dépasse (%)** : arrête l'analyse à la demande lorsque la charge du système de fichiers est supérieur au niveau indiqué (en %). A l'aide du curseur ou du champ à droite, vous pouvez définir le niveau de charge maximum.

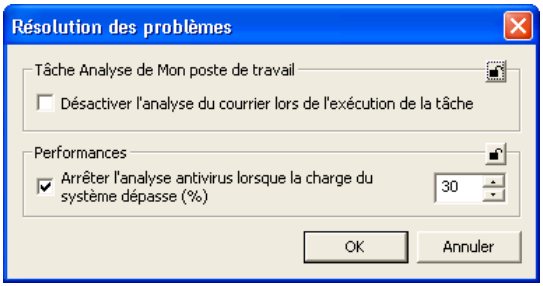

Illustration 93. Fenêtre **Résolutions des problèmes**

6.2.2.15. Examen des résultats de l'application de la stratégie

L'onglet **Contrôle** (cf. ill. 94) contient des informations sur l'application de la stratégie aux ordinateurs du groupe. L'onglet indique également le nombre d'ordinateurs :

- Pour lesquels la stratégie a été définie ;
- Pour lesquels la stratégie est exécutée ;
- Pour lesquels la stratégie n'a pas encore été exécutée ;
- Pour lesquels la stratégie n'a pas pu être appliquée suite à des erreurs.

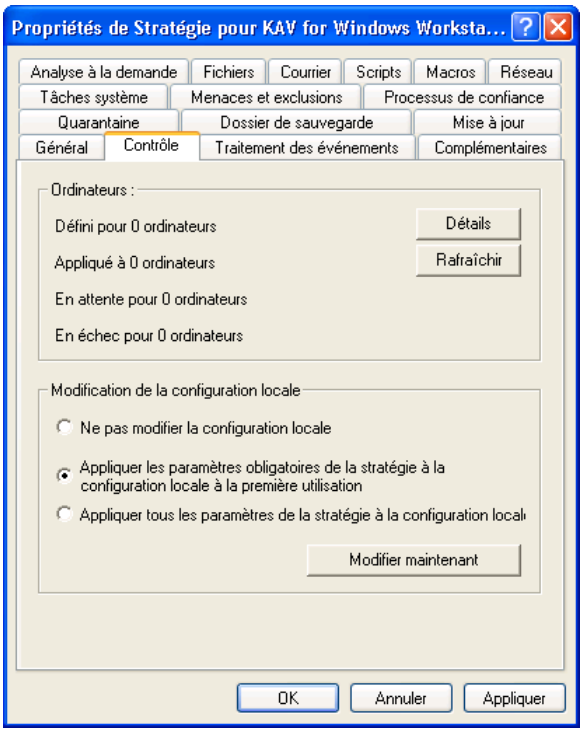

Illustration 94. Onglet **Contrôle**

Il est possible d'obtenir des informations détaillées sur les résultats de la stratégie appliquée à chaque ordinateur client en cliquant sur le bouton **Détails**

(pour de plus amples informations, consulter le manuel de l'administrateur de « Kaspersky Administration Kit 5.0 »).

Dans la section **Modification de la configuration locale**, vous pouvez préciser quels sont les paramètres qui seront modifiés dans les stratégies des groupes intégrés, dans les configurations de l'application et dans les paramètres des tâches sur les ordinateurs clients lors de la première application de la stratégie. Choisissez l'un des options suivantes :

- **Ne pas modifier la configuration locale**. Dans ce cas, les paramètres locaux ne seront pas modifiés.
- **Appliquer les paramètres obligatoires de la stratégie à la configuration locale à la première utilisation**. Dans ce cas, seuls seront modifiés les paramètres locaux accompagnés de l'icône  dans les paramètres de la stratégie. Pour empêcher la modification des paramètres obligatoires par l'utilisateur sur les ordinateurs client, il convient de cliquer sur l'icône avec le bouton gauche de la souris. Il prendra l'apparence suivante :  .
- **Appliquer tous les paramètres de la stratégie à la configuration locale à la première utilisation**. Dans ce cas, tous les paramètres locaux seront modifiés conformément aux paramètres de la stratégie. Comme pour l'option précédent, vous pouvez empêcher la modification des paramètres obligatoires par l'utilisateur.

Les modifications des paramètres locaux ont lieu automatiquement lors de la première application de la stratégie sur l'ordinateur client. Si vous souhaitez appliquer à nouveau la stratégie avec des paramètres actualisés, cliquez sur **Modifier maintenant**.

6.3. Administration des tâches

Cette rubrique est consacrée à la création et à la configuration de tâches pour Kaspersky Anti-Virus 5.0 for Windows Workstations. Pour obtenir de plus amples informations sur le concept d'administration des tâches, consultez le Manuel Kaspersky Administration Kit 5.0.

6.3.1. Création d'une tâche

Suite à l'installation de l'application, une liste de tâches système est créée pour chaque ordinateur. Cette liste (cf. ill. 95) reprend les tâches liées à la protection en temps réel (protection du système de fichiers, du courrier, protection contre les macros et des scripts) et celles liées à l'analyse à la demande (analyse du Poste de travail, analyse automatique lors du lancement de Kaspersky Anti-

Virus, analyse de la quarantaine) ou à la mise à jour (mise à jour des bases antivirus, mise à jour des modules de l'application, annulation des bases).

Les tâches liées à la protection en temps réel sont uniques et sont exécutées en arrière-plan. Un horaire est défini pour l'analyse à la demande et la mise à jour des bases antivirus.

Vous pouvez lancer les tâches systèmes par défaut, configurer les paramètres et les programmer. La suppression de ces tâches est impossible.

Lors de l'utilisation de Kaspersky Anti-Virus via Kaspersky Administration Kit, vous pouvez créer des :

- Tâches locales, définies pour un ordinateur client distinct ;
- Tâches de groupe, pour un groupe d'ordinateurs client ;
- 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**.

Les paramètres de fonctionnement de l'application lors de l'exécution des tâches sur chaque ordinateur client sont définis conformément à la stratégie du groupe, aux paramètres des tâches et aux paramètres de cette application sur l'ordinateur client.

Les tâches sont exécutées conformément à l'horaire établi. Vous pouvez suspendre temporairement certaines des tâches programmées. Dans ce cas la tâche n'est pas supprimée. Elle n'est simplement pas exécutées.

Vous pouvez lancer une tâche, l'arrêter, la suspendre ou la reprendre manuellement grâce aux commandes du menu contextuel **Démarrer/Stopper/Suspendre/Reprendre** ou aux éléments correspondants du menu **Actions**.

6.3.1.1. Création d'une tâche locale

Afin de créer une tâche locale, réalisez les opérations suivantes :

1. Dans le dossier **Groupes**, sélectionnez le dossier portant le nom du groupe dont l'ordinateur client fait partie.

2. Sélectionnez, dans le panneau des résultats, l'ordinateur pour lequel vous devez créer la tâche locale. Utilisez la commande **Propriétés** du menu contextuel ou l'élément correspondant du menu **Actions**. Cette action entraîne l'ouverture de la fenêtre **Propriétés de <Nom de l'ordinateur>** (cf. ill. 95). reprenant les propriétés de l'ordinateur client.

3. Sélectionnez l'onglet **Tâches** (cf. ill. 95). Il reprend toutes les tâches créée pour cet ordinateur client.
   Pour créer une nouvelle tâche locale, cliquez sur **Ajouter**. Cliquez sur **Propriétés** pour modifier les paramètres de la tâche. Vous pouvez supprimer la tâche de la liste en cliquant sur **Supprimer**.

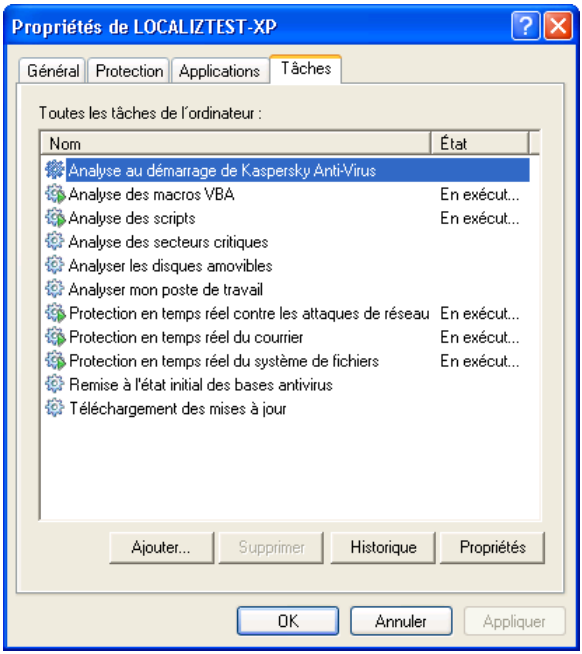

Illustration 95. Création d'une tâche locale.
Onglet **Tâches**

En cliquant sur **Ajouter…**, vous ouvrez la fenêtre de création d'une nouvelle tâche. L'interface du programme de création des tâches se présente sous la forme d'un Assistant 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 le programme à n'importe quel stade, cliquez sur **Annuler**.

Etape 1. Saisie d'informations générales sur la tâche

La première fenêtre de l'Assistant est destinée à la saisie d'informations : Il est indispensable d'indiquer le nom de la stratégie (dans le champ **Nom**).

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

Sélectionnez **Kaspersky Anti-Virus 5.0 for Windows Workstations** dans la liste déroulante **Application**. La sélection du type de tâche s'opère dans la liste déroulante **Type de tâche**. Pour Kaspersky Anti-Virus 5.0 for Windows Workstations, vous avez le choix entre les tâches suivantes :

- **Mise à jour des bases antivirus et des modules de l'application**.
- **Remise des bases antivirus à l'état initial**.
- **Analyse à la demande**.
- **Installation de la clé de licence**.

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.

CONFIGURATION DES PARAMETRES DE LA MISE A JOUR DES BASES ANTIVIRUS ET DES MODULES DE L'APPLICATION

La configuration des paramètres dans les fenêtres qui apparaissent à l'occasion de la configuration de la tâche de la mise à jour des bases antivirus et des modules du logiciel est identique à celle de la création des stratégies (cf. Etape 4–Etape 5 aux pages 134–135). De plus, il est possible de définir les paramètres de copie des mises à jour obtenues (Pour de plus amples informations, consultez le point 5.1.3.2 à la page 51).

CONFIGURATION DES PARAMETRES DE L'ANNULATION DE LA MISE A JOUR DES BASES ANTIVIRUS

L'annulation de la mise à jour des bases antivirus est ne possède pas de paramètres spécifiques. Pour cette raison, dès que vous aurez choisi cette tâche, vous arriverez à la fenêtre de programmation (cf. 5.8 à la page 171).

CONFIGURATION DES PARAMETRES DE L'ANALYSE A LA DEMANDE

Pour l'analyse à la demande, sélectionnez le niveau de protection (cf. point 4.2, p. 42) et précisez l'action qui sera appliquée à l'objet malveillant découvert (cf. point 5.3.3.2, p. 86).

Le bouton **Configuration…** ouvre une fenêtre qui vous permet de consulter les paramètres correspondant au niveau sélectionné ou de réaliser votre propre configuration sur la base de ceux-ci. Dans ce cas, le niveau de protection deviendra **Paramètres utilisateur**.

Dans la fenêtre suivante (cf. ill. 96), composez la liste des objets qui seront soumis. Pour ce faire cliquez sur **Ajouter…**, **Modifier…** ou **Supprimer**.

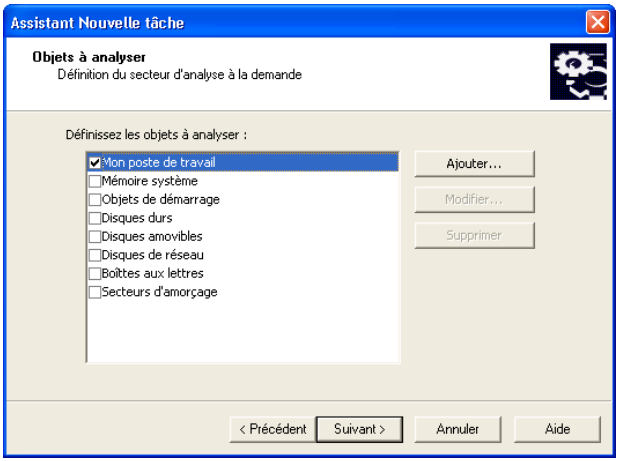

Illustration 96. Liste des objets analysés

CONFIGURATION DES PARAMETRES DE LA TACHE D'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 clé ainsi sélectionnée devienne la clé en cours, cochez la case **Utiliser en tant que clé de licence actuelle**.

Si la clé installée est une clé de réserve, il n'est pas nécessaire de cocher cette case. La clé de licence prendra la place de la clé actuelle dès que cette dernière sera arrivée à échéance.

Etape 4. Configuration du lancement d'une tâche au nom d'un utilisateur sélectionné

Cette étape (cf. Ill. 97) vous offre la possibilité de configurer le lancement de tâches définies sous un autre compte jouissant des privilèges d'accès adéquats à l'objet à analyser ou à la source de la mise à jour (pour de plus amples informations, consultez le point 5.9 à la page 107).

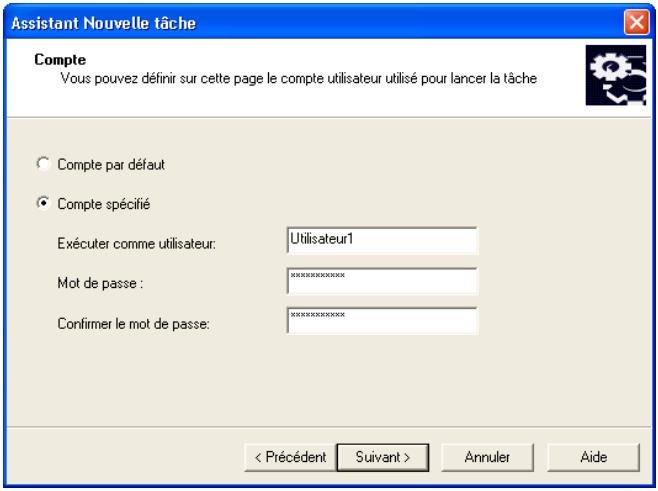

Illustration 97. Configuration du lancement d'une tâche au nom d'un autre compte

Etape 5. Programmation

Une fois que vous aurez configuré le type de tâche sélectionné, l'Assistant passera à la fenêtre **Paramètres de programmation de la tâche** (cf. ill. 98) où il est indispensable de définir l'horaire d'exécution de la tâche.

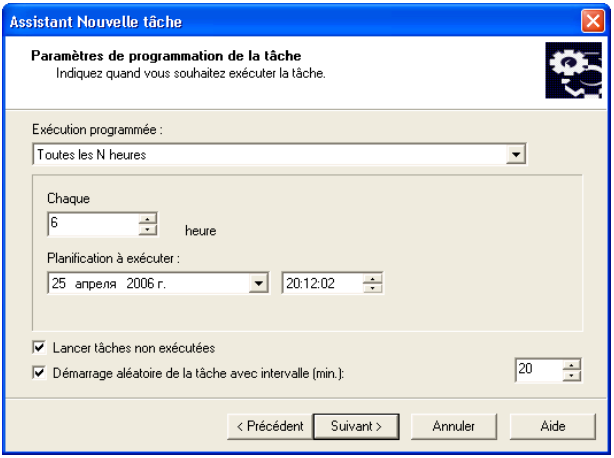

Illustration 98. Programmation de la tâche

Sélectionnez la fréquence de lancement de la tâche dans la liste déroulante **Exécution programmée**. Vous avez le choix entre : *Toutes les N heures, Tous les N jour, Toutes les N semaines et Mode manuel, Au démarrage de l'application.* La partie centrale avec les champs de saisie des données changera en fonction de la fréquence sélectionnée.

L'annulation des mises à jour des bases antivirus et l'installation de la clé de licence peuvent se faire uniquement manuellement.

Pour de plus amples informations sur la programmation du lancement des tâches, veuillez consulter le manuel de Kaspersky Administration Kit 5.0.

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.

6.3.1.2. Création d'une tâche de groupe

Afin de créer une tâche de groupe, réalisez les opérations suivantes :

1. Sélectionnez le groupe pour lequel vous souhaitez créer la tâche dans l'arborescence de la console.
2. Sélectionnez le répertoire **Tâches** qui en fait partie, affichez le menu contextuel et sélectionnez le point **Nouveau→Tâche** ou choisissez l'élément équivalent du menu **Action**. 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 6.3.1.1 à la page 167). Suivez les instructions affichées à l'écran.

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

6.3.1.3. Création d'une tâche globale

Afin de créer une tâche globale, réalisez les opérations suivantes :

1. Sélectionnez le nœud **Tâches** de l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Nouveau→Tâche** ou choisissez l'élément équivalent du menu **Action**.
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 6.3.1.1 à la page 167). 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. Il est possible de sélectionner des ordinateurs de différents répertoires ou des répertoires complets (pour de plus amples informations, consultez le manuel de Kaspersky Administration Kit 5.0).

Les tâches globales sont exécutées uniquement sur le groupe d'ordinateurs sélectionné. 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** de l'arborescence de la console et apparaîtra dans le panneau des résultats.

6.3.2. Examen et modification des paramètres d'une tâche. Suivi de l'exécution de la tâche

Pour vérifier les paramètres d'une tâche et / ou les modifier :

- Pour une tâche locale, sélectionnez, dans le dossier **Groupes,** le dossier portant le nom du groupe dont l'ordinateur client fait partie. Sélectionnez l'ordinateur dans le panneau des résultats et utilisez la commande **Propriétés** du menu contextuel. Ouvrez l'onglet **Tâches** (cf. ill. 95) de la fenêtre **Propriétés de <Nom de l'ordinateur>**. L'examen et la modification des paramètres de la tâche sélectionnée s'opèrent dans la fenêtre qui s'ouvre lorsque vous aurez cliquez sur **Propriétés**.

  L'onglet **Tâches** reprend la liste de toutes les tâches définies pour l'ordinateur local (y compris les tâches globales et de groupe). Les tâches globales et de groupe sont accompagnées d'une icône représentant un « dossier ». Vous pouvez consulter les paramètres de toutes les tâches. Toutefois, vous ne pourrez modifier que ceux des tâches locales.

- Pour les tâches de groupe, sélectionnez le groupe dans l'arborescence de la console et choisissez le dossier **Tâches** qui en fait partie. Ceci entraînera l'affichage dans le panneau des résultats de toutes les tâches définies pour ce groupe. Sélectionnez la tâche qui vous intéresse puis, ouvrez le menu contextuel afin de choisir le point **Propriétés** ou sélectionnez l'élément équivalent dans le menu **Action**.

- Si vous devez absolument modifier les paramètres d'une tâche globale, sélectionnez le nœud **Tâches** dans l'arborescence de la console, sélectionnez la tâche qui vous intéresse dans le panneau des résultats puis, ouvrez le menu contextuel afin de choisir le point **Propriétés** ou sélectionnez l'élément équivalent dans le menu **Action**.

Cela entraînera l'ouverture de la fenêtre **Propriétés de <Nom de la tâche>** avec les onglets suivants : **Général**, **Paramètres**, **Compte**, **Planification** et **Notification**. La fenêtre de configuration de la tâche globale contient également l'onglet intitulé **Ordinateurs cibles** pour lesquels la tâche sera créée.

Ces onglets (à l'exception de l'onglet **Paramètres** et **Compte**) sont des onglets standard pour la configuration des tâches dans Kaspersky Administration Kit 5.0. Ils sont présentés en détail dans le guide de l'administrateur de Kaspersky Administration Kit. L'onglet **Paramètres** reprend les paramètres propres à

Kaspersky Anti-Virus for Windows Workstations. Le contenu de l'onglet varie en fonction du type de tâche sélectionné (pour de plus amples informations, consultez l' Etape 3 à la page 169). L'onglet Compte vous permet de configurer le lancement des tâches sous un autre compte (cf. point 5.9 à la page. 107)

6.3.3. Lancement et arrêt des tâches

Le lancement d'une tâche sur l'ordinateur client est possible uniquement si l'application correspondante est lancée. En cas d'arrêt de l'application, l'exécution de toutes les tâches en cours sera interrompue.

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

Afin de démarrer /stopper/suspendre/continuer manuellement une tâche :

Sélectionnez la tâche qui vous intéresse puis, ouvrez le menu contextuel et choisissez la commande **Démarrer / Stopper / Pause / Continuer** ou utilisez les commandes équivalentes du menu **Action**.

Vous pouvez exécuter des actions similaires au départ de la fenêtre de configuration des tâches (onglet **Général**) à l'aide des boutons qui portent des noms identiques (cf. point 6.3.2, page 174).

6.4. Administration de l'application via les paramètres

La configuration de l'application vous permet de modifier les paramètres de fonctionnement de celle-ci pour des ordinateurs clients distincts dans le groupe. Seuls les paramètres dont la modification n'est pas interdite par la stratégie développée pour cette application peuvent être changés.

Afin de modifier les paramètres de l'application :

1. Dans le dossier **Groupes**, 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 **Propriétés** du menu contextuel ou l'élément correspondant du menu **Actions**.

3. Cette action entraîne l'ouverture dans la fenêtre principale du programme d'une boîte de dialogue intitulée **Propriétés de <Nom de l'ordinateur>** avec quatre onglets. Sélectionnez l'onglet **Applications** (cf. ill. 99). Il reprend toutes les applications de Kaspersky Lab installées sur l'ordinateur client.

4. Sélectionnez l'application **Kaspersky Anti-Virus 5.0 for Windows Workstations** En bas de cette liste se trouvent les boutons **Evénements**, **Statistiques** et **Propriétés** qui remplissent respectivement les fonctions suivantes :

   - Affiche la liste des événements survenus sur l'ordinateur client pendant l'utilisation de l'application et enregistrés sur le serveur d'administration (pour obtenir de plus amples informations sur l'utilisation des rapports, consultez le manuel de Kaspersky Administration Kit 5.0) .

   - Affiche les statistiques actuelles sur l'activité de l'application. .

   - Permet la configuration de l'application. En cliquant sur ce bouton, vous ouvrirez une fenêtre comprenant les onglets suivants : **Général**, **Complémentaire**, **Menaces et exclusions, Processus de confiance**, **Quarantaine**, **Dossier de sauvegarde**, **Objets des dossiers de quarantine et de sauvagarde**, **Licences** et **Traitement des événements**. Vous trouverez ci-après une description détaillée de ces onglets.

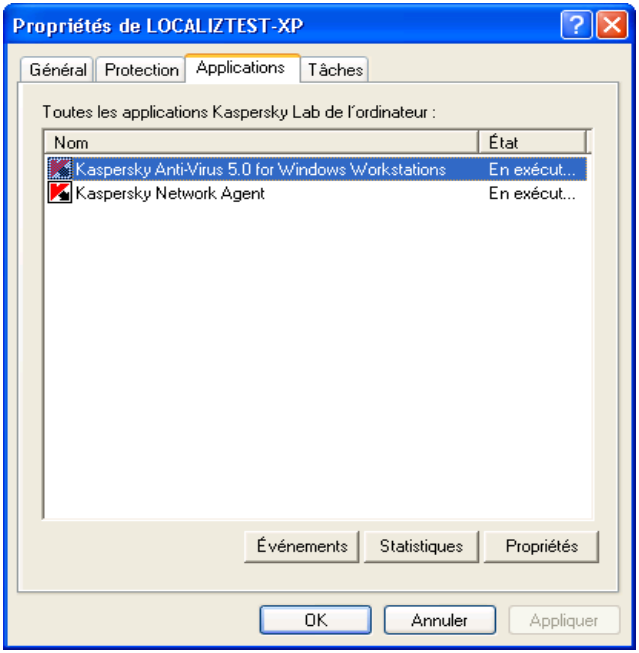

Illustration 99. Fenêtre d'examen des propriétés de l'ordinateur client. Onglet **Applications**

6.4.1. Consultation des renseignements relatifs à l'application

L'onglet **Général** (cf. ill. 100) reprend des informations générales sur Kaspersky Anti-Virus 5.0 for Windows Workstations. Vous pouvez également au départ de cet onglet lancer ou suspendre des tâches.

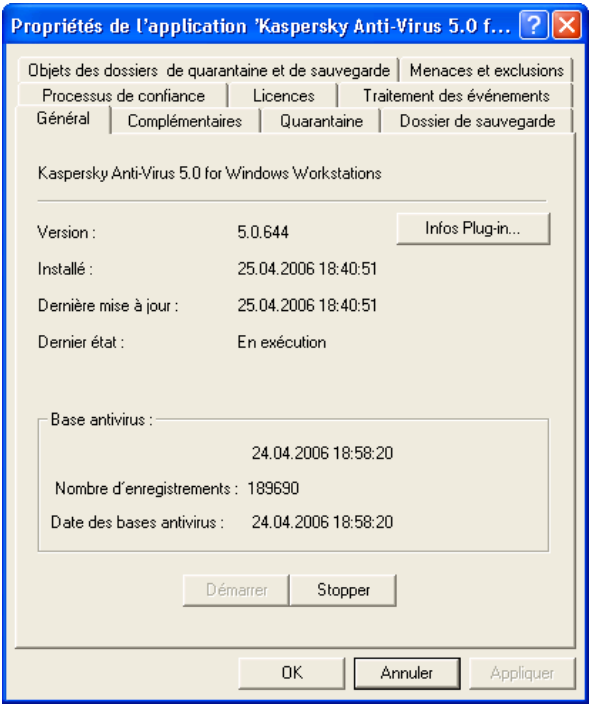

Illustration 100. Fenêtre de configuration des propriétés de l'application. Onglet **Général**

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

Vous pouvez lancer/arrêter l'application à l'aide des boutons correspondant.

Grâce au bouton **Infos Plug-in**, vous pouvez consulter les informations générales sur le plug-in d'administration de Kaspersky Anti-Virus 5.0 for Windows Workstations (cf. Illustration 101).

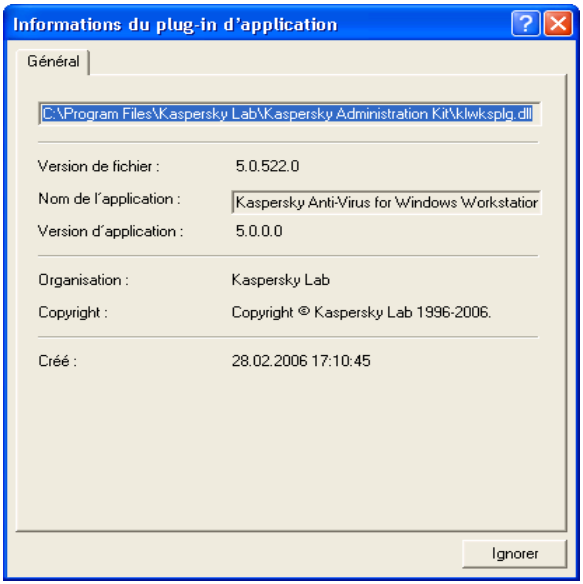

Illustration 101. Informations sur le plug-in d'administration de l'application

6.4.2. Options avancées de l'application

Les onglets **Complémentaires**, **Quarantaine, Riskware, Processus de confiance** et **Dossier de sauvegarde** permettent de configurer Kaspersky Anti-Virus 5.0 for Windows Workstations sur un poste de travail distant.

Ces paramètres sont redondants par rapport aux paramètres de la stratégie du groupe (pour plus de plus amples informations, consultez le point 6.2.2 à la page 136). Dans ce cas, les paramètres de la stratégie sont déterminants pour les paramètres de l'application.

Lors de la configuration des paramètres de l'application sur l'ordinateur local, vous pouvez changer uniquement les valeurs dont la modification est autorisée par la stratégie du groupe.

6.4.3. Utilisation de la quarantaine et du dossier de sauvegarde

Kaspersky Anti-Virus 5.0 for Windows Workstations vous permet de conserver les objets suspects et les copies de sauvegarde dans des dossiers spéciaux.

Il existe pour chaque ordinateur des dossiers de sauvegarde et de quarantaine individuels locaux sur l'ordinateur.

Pour examiner les objets situés dans le dossier de quarantaine ou de sauvegarde de l'ordinateur, utilisez l'onglet **Objets des dossiers de quarantine et de sauvagarde** (cf. ill. 102).

Pour ce faire, cliquez sur **Liste des objets** dans les sections **Quarantaine** ou **Dossier de sauvegarde**.

Si l'application n'est pas en mesure d'établir une connexion avec l'ordinateur client, un message proposant de réessayer ou d'annuler la tentative apparaît à l'écran.

Les fenêtres des deux dossiers se ressemblent (cf. ill. 103). La partie centrale reprend la liste des objets mis en quarantaine ou la liste des copies de sauvegarde. Les informations suivantes accompagnent chaque objet : nom du fichier, état de l'objet, date du placement dans le dossier et chemin d'accès d'origine.

Au-dessus de la liste se trouve le panneau d'administration des objets en quarantaine ou des copies de réserve. Ce panneau est composé des boutons suivants :

 : restaure l'objet. En cliquant sur ce bouton, vous ferez apparaître la fenêtre dans laquelle il faudra saisir le chemin d'accès à l'emplacement souhaité pour la restauration de l'objet.

En cas d'administration à distance à l'aide de Kaspersky Administration Kit, la restauration a lieu uniquement sur l'ordinateur où la *console d'administration* est installée.

 : supprime l'objet du dossier.

 : rafraîchit le contenu du dossier..

 : lance une analyse des objets (uniquement la quarantaine).

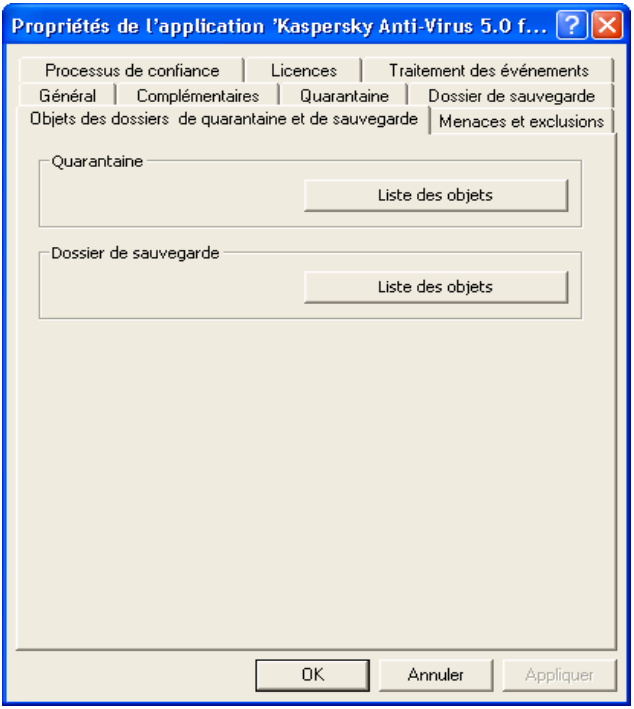

Illustration 102. Onglet **Objets des dossiers**

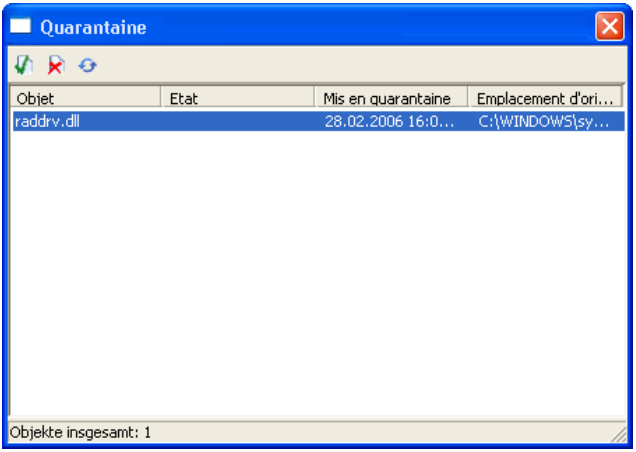

Illustration 103. Dossier de quarantaine

6.4.4. Consultations des informations relatives aux clés de licence

L'onglet **Licences** (cf. ill. 104) est purement informatif. Ces informations portent sur les clés de licence actuelles ou de réserve installées sur cet ordinateur.

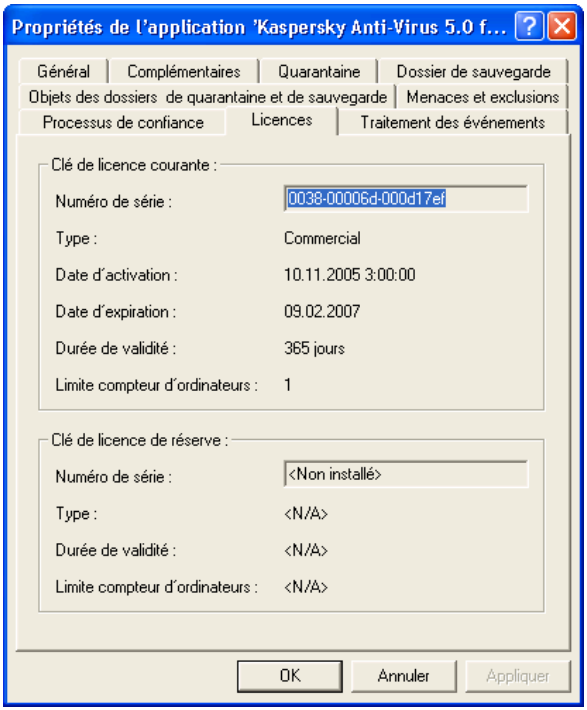

Illustration 104. Onglet **Licences**

6.4.5. Configuration des paramètres de constitution des rapports

L'onglet **Traitement des événements** vous permet de configurer les paramètres pour l'envoi des messages sur l'activité de Kaspersky Anti-Virus depuis l'ordinateur distant.

Cet onglet reprend les mêmes paramètres que ceux de l'onglet du même nom pour la stratégie du groupe (pour plus de plus amples informations, consultez le point 6.2.2.13 à la page 158).

CHAPITRE 7. VERIFICATION DU FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

7.1. Virus d'essai EICAR et ses modifications

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

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

Il NE S'AGIT PAS D'UN VIRUS et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus.

Vous pouvez télécharger le " virus " d'essai depuis le site officiel de l'organisation : http://www.eicar.org/anti_virus_test_file.htm. Si vous n'avez pas accès à Internet, vous pouvez créer ce " virus " d'essai vous-même. Pour ce faire, saisissez la ligne suivante dans n'importe quel éditeur de fichier texte et enregistrez le fichier sous **eicar.com** :

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Le fichier que vous aurez téléchargé depuis le site de **EICAR** ou que vous aurez créé vous-même contient le corps du " virus " d'essai standard. Lorsque l'antivirus le découvre, il lui attribue le statut **Infecté** et exécute l'action que vous avez définie pour les objets de ce type.

Afin de vérifier le comportement de Kaspersky Anti-Virus lors de la découverte d'objets d'un autre type, vous pouvez modifier le contenu du " virus " d'essai standard en ajoutant un des préfixes repris au tableau 1.

Vous pourrez vérifier le bon fonctionnement de Kaspersky Anti-Virus à l'aide du " virus " EICAR modifié uniquement si vous disposez des bases antivirus ultérieures au 24 octobre 2003 (mise à jour cumulée : octobre 2003).

Tableau 3 Modifications du " virus " d'essai

Préfixe	Type d'objet
Pas de préfixe, " virus " d'essai standard	**Infecté.** Une erreur se produit pendant la réparation ; l'objet est supprimé.
CORR–	**Corrompu.**
SUSP-	**Est peut-être infecté par un virus** (code d'un virus inconnu)
WARN-	**Infecté par une modification du virus** (modification du code d'un virus connu).
ERRO-	**Non analysé suite a un échec**.
CURE-	**Infecté**. L'objet sera réparé et le texte du corps du " virus " sera remplacé par CURE.
DELE-	**Infecté**. L'objet sera effacé automatiquement.

La première colonne reprend les préfixes qu'il faudra ajouter au début de la ligne de code du " virus " d'essai standard (par exemple : CORP–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*).

Une fois que vous aurez ajouté le préfixe, enregistrez le fichier sous le nom *eicar_dele.com* par exemple (utilisez la même convention pour toutes les modifications du virus).

La deuxième colonne reprend la description des types d'objet identifiés par l'antivirus suite à l'ajout des différents préfixes. Les actions exécutées sont définies par les différentes configuration de Kaspersky Anti-Virus.

7.2. Vérification du bon fonctionnement du Kaspersky Anti-Virus

Pour vérifier l'exactitude de la configuration et le bon fonctionnement de Kaspersky Anti-Virus 5.0 for Windows Workstation :

- Créez un nouveau répertoire dans lequel vous enregistrerez tous les virus d'essai que vous avez créés.
- Créez et configurez une tâche utilisateur (cf. point 5.6 , p. 97) :
    - Dans la liste des objets analysés lors de cette tâche, ajoutez le dossier reprenant les virus d'essai créés.
    - Parmi les actions proposées en cas de découverte d'objets infectés ou suspects, sélectionnez *Confirmer l'action auprès de l'utilisateur*.
- Cochez la case **Enregistrer tous les rapports** dans la fenêtre **Options avancées** (cf. point 5.10.3, p. 120). Cette étape est indispensable si vous voulez consigner dans le rapport les données relatives aux objets endommagés qui n'ont pu être analysés suite à un échec.
- Lancez la tâche.

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, le message suivant apparaîtra suite à la découverte d'un objet avec le préfixe SUSP- :

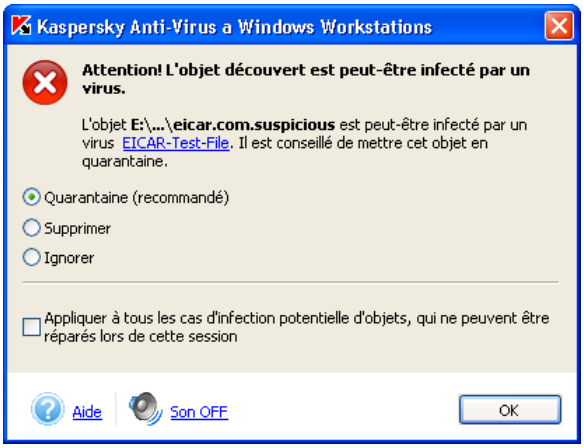

Illustration 105. Attention ! Un objet suspect a été découvert

De cette manière, vous pourrez vérifier la réaction du logiciel lors de la découverte de différents types d'objets infectés en sélectionnant différents scénarios de traitement.

Les résultats complets de l'analyse seront repris dans le rapport (cf. ill. 106).

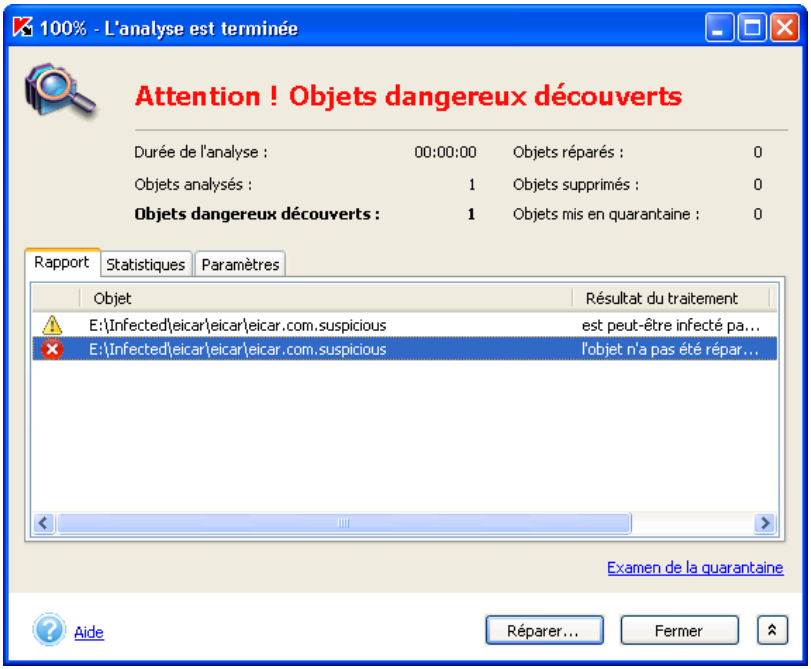

Illustration 106. Rapport d'analyse du dossier contenant les virus d'essai

CHAPITRE 8. GESTION DES CLES DE LICENCE

Vous pouvez utiliser Kaspersky Anti-Virus uniquement après avoir installé la *clé de licence* livrée avec le logiciel.

Kaspersky Anti-Virus for Windows Workstations NE PEUT FONCTIONNER sans la clé de licence !

A la fin de la période de validité de la licence, Kaspersky Anti-Virus continue à fonctionner mais la mise à jour des bases antivirus n'est plus possible. Les bases antivirus qui étaient d'actualité à la date d'expiration de la licence sont celles qui seront utilisées pour l'analyse antivirus de l'ordinateur et du courrier ainsi que pour la réparation des objets dangereux. Par conséquent, la protection contre les nouveaux virus qui apparaîtraient après la fin de validité de la licence n'est pas garantie.

Pour éviter que votre ordinateur ne soit infecté par de nouveaux virus, il est recommandé de renouvelé la licence d'utilisation de Kaspersky Anti-Virus.

Deux semaines avant la date d'expiration, Kaspersky Anti-Virus vous signalera qu'il est bientôt temps de renouveler la licence. Ce message apparaîtra à chaque démarrage du logiciel pendant cette période de deux semaines.

Pour renouveler la licence, vous devez absolument acheter et activer une nouvelle licence d'utilisation de Kaspersky Anti-Virus. Pour ce faire :

1. Contactez le distributeur chez lequel vous avez acheté le logiciel et demandez une prolongation de la licence d'utilisation de Kaspersky Anti-Virus 5.0 for Windows Workstations.

Ou :

Achetez une nouvelle clé de licence directement chez Kaspersky Lab en cliquant sur le lien Renouvellement de la licence dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 4) ou en cliquant **Renouveler** dans la boîte de dialogue **Gestion des clés de licence** (cf. ill. 107). Remplissez le formulaire requis sur notre site Internet. Une fois le paiement effectué, vous recevrez à l'adresse électronique spécifiée lors de la commande une référence qui vous permettra de télécharger la clé de licence

2. Activez la clé de licence. Pour obtenir de plus amples informations sur l'utilisation des clés de licence via l'interface locale de la clé de

licence, consultez le point 8.1 à la page 190 et via l'interface de Kaspersky Administration Kit, consultez le point 8.2 à la page 193).

Vous pouvez activer deux clés : une clé actuelle et une clé de réserve. La clé actuelle est celle qui fonctionne en ce moment. Il ne peut pas y avoir plus de deux clés « actuelles » activées. La clé de réserve entre en action dès la fin de validité de la clé actuelle.

8.1. Manipulation des clés de licence via l'interface locale

Afin de prolonger la licence d'utilisation via l'interface locale de Kaspersky Anti-Virus 5.0 for Windows Workstations, réalisez les opérations suivantes :

1. Achetez une clé de licence (voir plus haut pour les détails).
2. Activez la clé de licence. Pour ce faire :
   a. Cliquez sur Clés de licence dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 4).
   b. Cliquez sur **Ajouter…** dans la boîte de dialogue **Gestion des clés de licence** (cf. ill. 107) et sélectionnez la nouvelle clé de licence.
   c. Dans la fenêtre de sélection, ouvrez le répertoire qui contient la clé de licence (fichier **.key**). Sélectionnez la clé nécessaire puis, cliquez sur **Ouvrir**
   d. Dans la fenêtre **Activation de la clé** (cf. ill. 108), lisez les informations relatives à la clé ajoutée puis cliquez sur **Activer** pour utiliser cette clé.

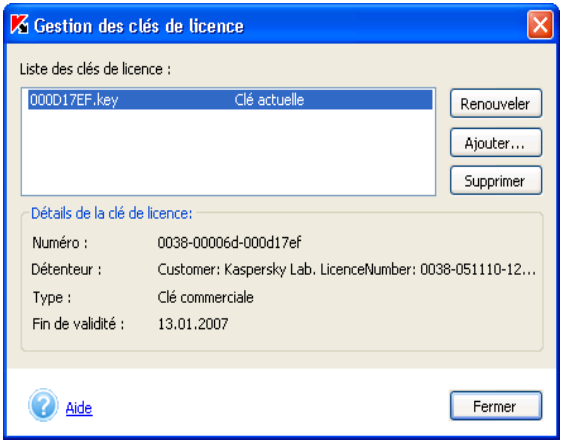

Illustration 107. Fenêtre d'administration des clés de licence

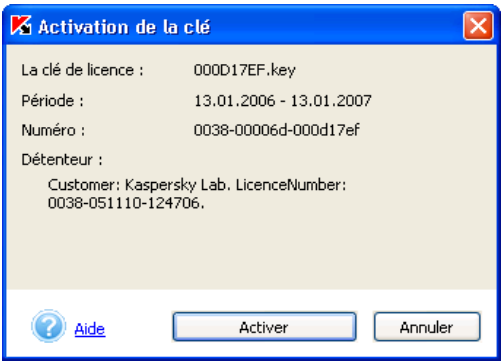

Illustration 108. Fenêtre d'activation de la clé

ou:

a. Dans le menu **Démarrer** → **Programmes**, sélectionnez le groupe Kaspersky Anti-Virus et dans le menu déroulant, sélectionnez le point **Activation de la clé de licence**.

a. Cliquez sur **Parcourir…** dans la fenêtre qui s'ouvre et passez au répertoire qui contient la clé de licence.

b. Sélectionnez la clé de licence nécessaire puis, cliquez sur **Ouvrir**.

c. Dans la partie inférieure de la fenêtre (cf. ill. 109), cochez la case en regard de l'application pour laquelle vous souhaitez installer la clé de licence. Cliquez sur **OK**.

Si la liste de la partie inférieure de la fenêtre est vide, cela signifie que la clé choisie ne convient à aucune des applications de Kaspersky Lab installées sur l'ordinateur.

Sélectionnez un autre fichier de clé de licence.

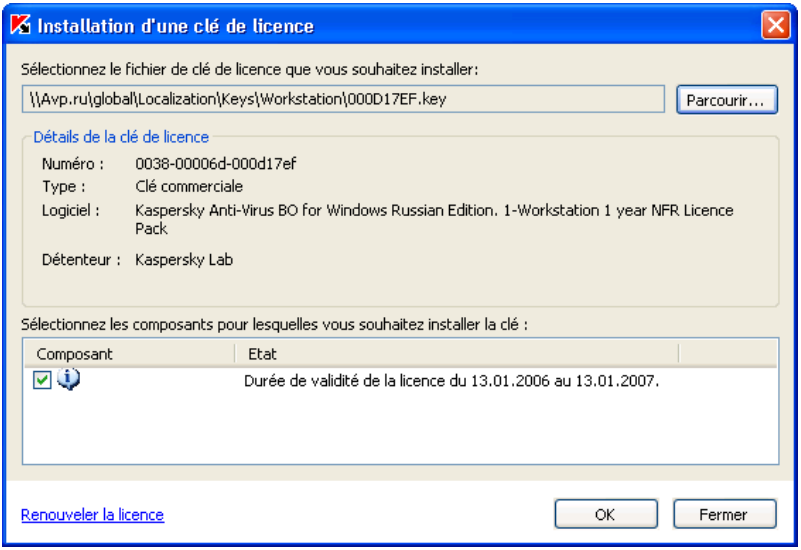

Illustration 109. Fenêtre **Installation de la clé de licence**

d. Dans la fenêtre **Activation de la clé** (cf. ill. 108), lisez les informations relatives à la clé ajoutée puis, cliquez sur **Activer** pour utiliser la clé.

Si vous souhaitez activer une nouvelle clé alors que la clé actuelle est toujours valide, vous aurez le choix entre deux options :

- Donner le statut de clé de réserve à la nouvelle clé (recommandé). Dans ce cas, la clé est ajoutée à la liste avec le statut *réserve*. Dès la fin de validité de la clé actuelle, la nouvelle clé la remplacera.
- Écraser la clé actuelle avec la nouvelle. Dans ce cas, la nouvelle clé est ajoutée à la liste et prend le statut « actuelle ».

N'oubliez pas que la suppression de la clé de licence actuelle s'accompagne automatiquement de la suppression de la clé de réserve installée !

8.2. Manipulation des clés de licence via l'interface de Kaspersky Administration Kit

Kaspersky Administration Kit vous permet de renouveler la licence de deux manières :

- *Ajout groupé de licence* : le renouvellement de la licence pour Kaspersky Anti-Virus s'opère simultanément pour les ordinateurs sélectionnés ou pour un groupe d'ordinateurs clients grâces aux tâches globales ou de groupe (pour de plus amples informations, consultez le Manuel de Kaspersky Administration Kit 5.0).
- *Ajout individuel d'une licence* : renouvellement de la licence de Kaspersky Anti-Virus de l'ordinateur sélectionné.

Pour renouveler la licence sur une poste de travail particulier, vous devez absolument acheter et activer une nouvelle licence d'utilisation de Kaspersky Anti-Virus. Pour ce faire :

1. Achetez une clé de licence (cf. Chapitre 8, page 189).
2. Créez une tâche locale pour l'activation de la clé de licence (cf. point 6.3.1.1, p. 167).

L'onglet **Licenses** vous permet de consulter les informations relatives aux clés de licence (actuelles ou de réserve) installées sur un ordinateur particulier (pour de plus amples informations, consultez le point 6.4.4 à la page 182)).

CHAPITRE 9. ADMINISTRATION DE L'APPLICATION VIA LA LIGNE DE COMMANDE

Kaspersky Anti-Virus peut être administré via la ligne de commande grâce à l'utilitaire **kavshell.exe** qui est livré avec le logiciel. Après l'installation de Kaspersky Anti-Virus, cet utilitaire se place dans la racine du répertoire d'installation du programme. Lors du lancement de l'utilitaire au départ de la ligne de commande, les fonctions suivantes sont accessibles en fonction des commandes utilisées :

SCAN	Analyse des objets sélectionnés
FULLSCAN	Analyse complète de l'ordinateur
UPDATE	Mise à jour des bases antivirus et des modules de l'application
ROLLBACK	Annulation de la dernière mise à jour réalisée des base antivirus
RTP	Administration du mode d'analyse en temps réel de l'ordinateur
START	Lancement de Kaspersky Anti-Virus
STOP	Arrêt de Kaspersky Anti-Virus
TASK	Administration des tâches de Kaspersky Anti-Virus
IMPORT	Importation des paramètres de Kaspersky Anti-Virus depuis un fichier
EXPORT	Exportation des paramètres de Kaspersky Anti-Virus dans un fichier

ADDKEY	Ajout d'une clé de licence

Si l'utilisation des modes utilisateur et administrateur a été desactivée dans Kaspersky Anti-Virus (cf. point 5.10.7, p.126), les commandes qui requièrent un mot de passe ne seront pas exécutée. Un message d'erreur s'affichera.

Pour étudier la syntaxe des commandes, utilisez :

```
KAVSHELL HELP [commande] [6]
KAVSHELL [commande] /?
```

Si la clé **commande** n'est pas définie, la liste de toutes les commandes disponibles sera affichée.

Exemple:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

9.1. Analyse des objets sélectionnés

Syntaxe de la commande :

```
KAVSHELL SCAN [objets] [/L[!]:fichier_objet] [/F(A|E|C)]
[/NP] [/ASK|/DISINFECT|/DELETE]
[/W[A][!]:fichier_de_rapport]
```

Si une de ces clés n'est pas définie, l'aide relative à la syntaxe de la commande sera affichée.

L'analyse est réalisée selon les paramètres recommandés par les experts de Kaspersky Kab.

Argument	Signification
objets	Dresse la liste d'un ou de plusieurs fichiers, répertoires, d'objets prédéfinis ou

[6] La valeur entre crochets est une variable.

	fichiers, répertoires, d'objets prédéfinis ou de problèmes distincts. Parmi les objets prédéfinis, citons : • **/MEMORY** : mémoire système. • **/STARTUP** : objet de démarrage. • **/MAIL:** les boîtes aux lettres Microsoft Office Outlook et Microsoft Outlook Express ; • **/REMDRIVES** : les disques amovibles; • **/FIXDRIVES** : disques système. • **/NETDRIVES** : disques de réseau Remarques : • Mettre le nom de l'objet entre guillemets s'il contient un espace; • Il est possible d'avoir recours aux masques pour analyser plusieurs fichiers (des exemples de masque sont repris au point 5.7 à la page 99); • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/L[!]:fichier_objet	Définit le fichier au format **.txt** qui contient la liste des objets à analyser (fichiers, répertoires, objets prédéfinis). Le nom de chaque objet dans le fichier doit être écrit à la ligne. Le symbole **!** détermine la suppression du fichier de la liste après l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/F(A|E|C) **/FA**	Type de fichiers analysés : • Analyser tous les fichiers.

/FC **/FE**	• Analyser les fichiers qui peuvent être infectés selon le format. • Analyser les fichiers qui peuvent être infectés selon l'extension.
/NP	Ignore les objets protégés par un mot de passe.
[/ASK | /DISINFECT | /DELETE] • **/ASK** • **/DISINFECT** • **/DELETE**	Action à exécuter sur les objets infectés : • Confirmer l'action auprès de l'utilisateur • Réparer, supprimer si la réparation est impossible • Supprimer. Remarques : • Si aucune action n'est définie, l'objet sera ignorée et les informations à son sujet seront reprises dans le rapport. • Les objets composés ne seront pas supprimés.
/W[A][!]:fichier_de_rapport **/W:fichier_de_rapport** **/WA:fichier_de_rapport**	Consigne les événements dans le fichier journal. • uniquement les événements importants; • tous les événements. Le caractère **!** indique l'écrasement du rapport après chaque lancement de la tâche. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace

Exemples:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
```

```
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt /ASK
```

9.2. Analyse complète

Syntaxe de la commande :

```
KAVSHELL FULLSCAN [/W[A][!]:fichier_de_rapport] [/D]
```

Si une de ces clés n'est pas définie, l'aide relative à la syntaxe de la commande sera affichée.

L'analyse est réalisée selon les paramètres recommandés par les experts de Kaspersky Kab.

Argument	Signification
/W[A][!]:fichier_de_rapport **/W:fichier_de_rapport** **/WA:fichier_de_rapport**	Consigne les événements dans le fichier journal. • uniquement les événements importants; • tous les événements. Le caractère **!** indique l'écrasement du rapport après chaque lancement de la tâche. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/D	Annule l'analyse si cette tâche a déjà été réalisée avec succès aujourd'hui.

Exemples:

```
KAVSHELL FULLSCAN /WA:fullscan.log
```

9.3. Lancement de la mise à jour

Syntaxe de la commande :

```
KAVSHELL UPDATE [source_de_mise_à_jour]
[/W[A][!]:fichier_de_rapport] [/APP]
```

Si une de ces clés n'est pas définie, l'aide relative à la syntaxe de la commande sera affichée.

Argument	Signification
[**source_de_mise_à_jour**]	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Si le chemin n'est pas indiqué, la source de la mise à jour sera celle reprise dans la configuration de la tâche d'actualisation des bases antivirus et des modules de l'application.
/W[A][!]:fichier_de_rapport **/W:fichier_de_rapport** **/WA:fichier_de_rapport**	Consigne les événements dans le fichier journal. • uniquement les événements importants; • tous les événements. Le caractère **!** indique l'écrasement du rapport après chaque lancement de la tâche. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
/APP	Mise à jour des modules du logiciel.

Exemples:

```
KAVSHELL UPDATE ftp://ftp.kaspersky.ru/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP
```

9.4. Annulation de la dernière mise à jour

Syntaxe de la commande :

```
KAVSHELL ROLLBACK [/W[A][!]:fichier_de_rapport]
```

Si une de ces clés n'est pas définie, l'aide relative à la syntaxe de la commande sera affichée.

Argument	Signification
/W[A][!]:fichier_de_rapport **/W:fichier_de_rapport** **/WA:fichier_de_rapport**	Consigne les événements dans le fichier journal. • uniquement les événements importants; • tous les événements. Le caractère **!** indique l'écrasement du rapport après chaque lancement de la tâche. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace

Exemples:

```
KAVSHELL ROLLBACK /WA:rollback.log
```

9.5. Mode de protection en temps réel

Syntaxe de la commande :

```
KAVSHELL RTP [taskid] { /START /PWD:mot de passe | /STOP
/PWD:mot de passe }
```

Si une de ces clés n'est pas définie, l'aide relative à la syntaxe de la commande sera affichée.

Argument	Signification
/START	Active la protection en temps réel ou l'un de ses composants particuliers.
/STOP	Arrête la protection en temps réel ou l'un de ses composants particuliers..
taskid	Identifiant du composant de la protection en temps réel. Si l'identifiant (taskid) n'est pas repris, toutes les commandes sont appliquées à toutes les tâches de la protection en temps réel. Valeurs possibles : • on-access : protection en temps réel des fichiers • mail-checker : protection en temps réel du courrier; • outlook-plugin : protection en temps réel du courrier sur Microsoft Office Outlook; • script-checker : analyse en temps réel des scripts • office-guard : analyse des macros VBA.
/PWD:mot de passe	Saisie du mot de passe de l'administrateur indispensable pour exécuter la commande.

Exemples:

```
KAVSHELL RTP /START /PWD:mot_de_passe
KAVSHELL RTP on-access /START /PWD:mot_de_passe
KAVSHELL RTP /STOP script-checker /PWD:mot_de_passe
```

9.6. Lancement de l'application

Syntaxe de la commande :

```
KAVSHELL START
```

9.7. Arrêt de l'application

Syntaxe de la commande :

```
KAVSHELL STOP /PWD:mot_de_passe
```

Argument	Signification
/PWD:mot_de_passe	Saisie du mot de passe de l'administrateur indispensable pour exécuter la commande.

Exemple:

```
KAVSHELL STOP /PWD:mot_de_passe
```

9.8. Administration des tâches

Syntaxe de la commande :

```
KAVSHELL TASK [ taskid {/START
[/W[A][!]:fichier_de_rapport]|
                /STOP |
                /PAUSE |
                /RESUME [/W[A][!][: fichier_de_rapport]]|
                /DELETE } ] /PWD:mot de passe
```

Si aucune des clés n'est définie, la liste de toutes les tâches accessibles avec leur identifiant unique apparaîtra, ainsi que le statut de chaque tâche.

Argument	Signification
/START	Lance la tâche correspondant à l'identifiant spécifié.
/W[A][!]:fichier_de_rapport **/W:fichier_de_rapport** **/WA:fichier_de_rapport**	Consigne les événements dans le fichier journal. • uniquement les événements importants; • tous les événements. Le caractère **!** indique l'écrasement du rapport après chaque lancement de la tâche. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace

/STOP	Arrête la tâche correspondant à l'identifiant spécifié. Le mot de passe est indispensable à l'arrêt des tâches de la protection en temps réel ! Il s'agit de : • Protection en temps réel des fichiers; • Protection en temps réel du courrier; • Analyse des scripts en temps réel; • Analyse des macros VBA; • Protection contre les attaques de réseau.
/PAUSE	Suspend l'exécution de la tâche correspondant à l'identifiant spécifié.
/RESUME	Reprend l'exécution de la tâche correspondant à l'identifiant spécifié.
/DELETE	Supprime la tâche correspondant à l'identifiant spécifié.
taskid	Identifiant unique de la tâche. Les tâches système peuvent être administrées via les identifiants standard suivants : • scan-computer : analyse complète de l'ordinateur; • scan-removable : analyse des disques amovibles; • scan-quarantine : analyse de la quarantaine; • scan-critical : analyse des secteurs de démarrage des disques, de la mémoire et des objets de démarrage • update-bases : mise à jour des bases antivirus; • update-app : mise à jour des modules de l'application;

	• rollback : annulation de la dernière mise à jour des bases antivirus; • on-access : protection en temps réel des fichiers • mail-checker protection en temps réel du courrier; • script-checker : analyse en temps réel des scripts • office-guard - analyse des macros VBA; • ids : protection contre les attaques de réseau.
/PWD:mot de passe	Saisie du mot de passe de l'administrateur indispensable pour exécuter la commande.

Exemples:

```
KAVSHELL TASK /PWD:mot_de_passe
KAVSHELL TASK update-app /START /WA:fullscan.log
/PWD:mot_de_passe
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE /PWD:mot_de_passe
```

9.9. Importation/exportation des paramètres

Syntaxe de la commande :

```
KAVSHELL IMPORT fichier_de_configuration /PWD:mot de passe
KAVSHELL EXPORT fichier_de_configuration /PWD:mot de passe
```

Argument	Signification
fichier_de_configuration	Nom du fichier du profil au départ duquel ou vers lequel les paramètres de Kaspersky Anti-Virus sont importés ou exportés. Pour obtenir de plus amples informations, consultez le point 5.10.3 à la page 119.
/PWD:mot_de_passe	Saisie du mot de passe de l'administrateur indispensable pour exécuter la commande.

Exemples:

```
KAVSHELL IMPORT c:\kav50settings.xml /PWD:mot_de_passe
KAVSHELL EXPORT c:\kav50settings.xml /PWD:mot_de_passe
```

9.10. Ajout d'une clé de licence

Syntaxe de la commande :

KAVSHELL ADDKEY fichier [/R] /PWD:mot de passe

Argument	Signification
fichier	Nom du fichier de clé de licence
[/R]	Remplacement de la clé de licence actuelle par une nouvelle clé.
/PWD:mot_de_passe	Saisie du mot de passe de l'administrateur indispensable pour exécuter la commande.

Exemple:

```
KAVSHELL ADDKEY c:\00A531D2.key /R /PWD:mot_de_passe
```

CHAPITRE 10. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquemment posées par les utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Anti-Virus. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : l'utilisation simultanée de Kaspersky Anti-Virus avec des logiciels antivirus d'autres éditeurs est-elle possible ?

Afin d'éviter tout risque de conflit, nous vous conseillons de supprimer les logiciels antivirus d'éditeurs tiers avant d'installer Kaspersky Anti-Virus.

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

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

Et cela, grâce aux nouvelles technologies iChecker et iStreams. Ces technologies reposent sur l'utilisation d'une base de données des sommes de contrôle des objets et la conservation des sommes de contrôle dans les flux NTFS complémentaires.

Question : Pourquoi Kaspersky Anti-Virus entraîne-t-il une baisse des performances de mon ordinateur et surcharge le processeur ?

La détection des virus est avant tout une tâche mathématique liée à l'analyse de la structure, de la somme de contrôle et des données mathématiques. Pour cette raison, la principale ressource utilisée par tout logiciel antivirus est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse. C'est le prix à payer pour garantir la fiabilité et la sécurité des données.

A la différence d'autres logiciels antivirus qui réduisent la durée de l'analyse en éliminant des bases antivirus les virus les plus complexes à identifier ou les plus rares (à l'endroit où est basé l'éditeur), ainsi que les fichiers les plus difficiles à analyser (comme les fichiers PDF), Kaspersky Lab estime que la tâche attendue de tout antivirus est de garantir une véritable protection de l'utilisateur contre les virus. Il ne peut être question de protection partielle. Qui plus est, la " protection

partielle " est pire que l'absence de protection (dans ce cas au moins, l'utilisateur adopte lui-même des mesures de prévention).

Kaspersky Anti-Virus confère à l'utilisateur un sentiment de protection totale. Il va de soi que Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer la vitesse de l'analyse au détriment du niveau global de sécurité grâce à l'exclusion de toute une série de différents fichiers. Toutefois, nous ne vous conseillons pas d'agir ainsi si vous souhaitez vous sentir vraiment en sécurité.

Signe de la protection maximale qu'il assure aux utilisateurs, Kaspersky Anti-Virus reconnaît plus de 1 200 formats de fichiers archivés ou compressés et répare 6 formats. Ceci est très important au niveau de la sécurité antivirus car chacun des formats reconnus ci-dessus peut contenir un code malicieux exécutable. Néanmoins, il convient de remarquer que chaque nouvelle version du logiciel est plus rapide que la précédente, malgré l'augmentation quotidienne du nombre de virus identifiés par Kaspersky Anti-Virus et l'augmentation constante des formats pris en charge. Tout ceci est rendu possible grâce aux nouvelles technologies développées par Kaspersky Lab comme i-Checker™ et i-Stream™. Ces technologies permettent de rechercher d'éventuels virus dans les fichiers une seule fois, lors de la première analyse. Si ce fichier n'a pas été modifié depuis la dernière analyse, il ne sera pas repris dans l'analyse suivante. Autrement dit, les performances du logiciel antivirus sont nettement accrues après la première analyse du fichier.

Question : A quoi sert la clé de licence? *Mon antivirus fonctionnera-t-il sans elle ?*

Kaspersky Anti-Virus ne peut fonctionner sans la clé de licence.

Si vous n'avez pas encore décidé d'acheter Kaspersky Anti-Virus, vous pouvez télécharger une version d'évaluation sur le site dans la rubrique **Téléchargements → Versions d'évaluation** La version d'évaluation fonctionnera pendant 15 jours. Passé ce délai, la clé sera bloquée.

Question : Que se passe-t-il lorsque la licence d'utilisation du logiciel arrive à échéance ?

Lorsque la licence est parvenue à échéance, Kaspersky Anti-Virus continue à fonctionner mais il n'est plus possible de procéder aux mises à jour des bases antivirus. Le programme continuera à réparer les objets infectés en utilisant les vieilles bases antivirus.

Lorsque cette situation se présente, vous devez contacter votre administrateur de système ou la société où vous avez acheté Kaspersky Anti-Virus ou Kaspersky Lab directement.

Question : à quoi servent les mises à jour quotidiennes ?

Il y a encore quelques années, les virus étaient transmis via disquette et afin de protéger l'ordinateur, il suffisait d'installer un logiciel antivirus et de procéder de temps à autre à la mise à jour des bases antivirus. Les épidémies les plus récentes se sont répandues à travers le monde entier en quelques heures uniquement et dans ces conditions, un logiciel antivirus équipé d'anciennes bases antivirus est impuissant face aux nouvelles menaces. Afin de ne pas devenir victime de la prochaine épidémie de virus, il est indispensable de mettre à jour les bases antivirus quotidiennement.

Chaque année, Kaspersky Lab augmente la fréquence de mise à jour des bases antivirus. Actuellement, les mises à jour sont diffusées toutes les heures.

La mise à jour des modules de l'application est une fonction supplémentaire. Ces mises à jour corrigent les défauts et apportent de nouvelles possibilités.

Question : qu'est-ce qui a changé dans le service de mise à jour de la version 5.0 ?

La nouvelle gamme de produits de la version 5.0 offerte par Kaspersky Lab présente un nouveau service de mise à jour. Le développement de cette nouvelle fonction s'est fondé sur les remarques des utilisateurs et sur les impératifs du marketing. De plus, il fallait renforcer le degré technologique de l'ensemble de la procédure de mise à jour, depuis la préparation chez Kaspersky Lab jusque l'actualisation des fichiers chez l'utilisateur.

Voici les avantages du nouveau système de mise à jour :

- Fin du téléchargement des fichiers en cas de déconnexion : désormais, il n'est plus nécessaire de télécharger à nouveau les données obtenues avant la déconnexion.
- *Réduction de moitié de la taille de la mise à jour cumulée.* La mise à jour cumulée contient toute la base antivirus, ce qui explique pourquoi la taille de la mise à jour cumulée est de loin supérieur à la taille de la mise à jour traditionnelle. Le nouveau service introduit une nouvelle technologie qui permet d'utiliser

les bases antivirus qui existent déjà pour la mise à jour cumulée.

- *Accélération du téléchargement depuis Internet.* Kaspersky Anti-Virus sélectionne le serveur de mise à jour situé dans votre région. De plus, la charge du serveur est répartie en fonction de ses performances. Autrement dit, vous ne serez pas connecté à un serveur surchargé pendant qu'un autre n'est pas sollicité.

- *Application des « listes noires » des clés.* Ceci permet d'exclure des mises à jour les utilisateurs qui ne disposent pas de la licence d'utilisation de Kaspersky Anti-Virus. Ainsi, les utilisateurs qui possèdent une licence ne sont pas pénalisés à cause de serveurs surchargés.

- Les logiciels destinés aux entreprises autorisent la création d'un répertoire local pour la mise à jour des bases antivirus. Cette fonction est prévue pour les entreprises où les ordinateurs, protégés par les applications de Kaspersky Lab, sont regroupés au sein d'un réseau. N'importe quel ordinateur peut jouer le rôle de serveur de mise à jour. C'est lui qui recevra les mises à jour depuis Internet. Elles seront enregistrées dans un répertoire local accessible aux autres ordinateurs du réseau.

Question : *une personne mal intentionnée pourrait-elle remplacer les bases antivirus ?*

Chaque base antivirus dispose d'une signature unique que Kaspersky Anti-Virus vérifie lorsqu'il consulte ces bases. Si la signature ne correspond pas à celle octroyée par Kaspersky Lab et que la date de la base de données est postérieure à la date d'expiration de la licence, Kaspersky Anti-Virus n'utilisera pas cette base.

Question : comment configurer la mise à jour pour un ordinateur via Internet afin qu'il devienne ensuite le serveur de mise à jour pour les autres ordinateurs du réseau ?

Le serveur sera l'ordinateur mis à jour via Internet tandis que les autres ordinateurs du réseau seront les clients de ce serveur.

Il est possible de configurer la mise à jour via le réseau local de l'une des manières suivantes :

- Activer l'utilisation de la source de mise à jour locale sur le serveur Kaspersky Administration Kit 5.0.

  Kaspersky Administration Kit est équipé d'un outil de diffusion des mises à jour via le réseau de l'entreprise. Il peut, selon

l'horaire défini, mettre à jour les ressources d'accès commun et lancer la mise à jour des autres ordinateurs. Kaspersky Administration Kit veillera à ce que le volume de données téléchargées ne dépasse les besoins des applications installées. Il est possible de voir sur le serveur la liste des correctifs disponibles. La procédure de configuration est décrite en détail dans le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

- Activer l'utilisation de la source de mise à jour locale dans l'un des logiciels de Kaspersky Lab.

  Cette méthode doit être suivie lorsque l'utilisation de Kaspersky Administration Kit est impossible ou lorsqu'il faut obtenir une structure du réseau des serveurs de mise à jour plus complexe. Pour ce faire :

  - Sélectionnez les ordinateurs qui serviront de serveur de mise à jour. La version 5.07 des applications de Kaspersky Lab devront être installées sur cet ordinateur.
  - Il faut absolument créer sur chaque ordinateur sélectionné une ressource de réseau qui servira à la diffusion de la mise à jour. Il peut s'agir d'un répertoire de réseau sur un ordinateur Microsoft Windows, un serveur FTP ou un serveur HTTP. Les privilèges d'accès à ce répertoire devront être définis correctement.
  - Créez la tâche de mise à jour ou modifiez la tâche existante. Activez l'utilisation de la mise à jour depuis la source locale et indiquez le chemin d'accès au répertoire.
  - Précisez le répertoire de source locale de la mise à jour du serveur sur tous les ordinateurs qui devront être mis à jour au départ de ce serveur.

Question : j'utilise un serveur proxy et la mise à jour ne fonctionne pas. Que faire ?

L'échec de la réception des mises à jour en cas d'utilisation d'un serveur proxy peut provenir de l'une des causes suivantes :

- Configuration incorrecte des paramètres du réseau.

[7] Autre que Kaspersky Anti-Virus 5.0 Personal et Kaspersky Anti-Virus 5.0 for Microsoft ISA Server

Lors de la configuration du service de mise à jour, il est possible de configurer les paramètres du réseau de deux manières : soit en utilisant les paramètres de Microsoft Internet Explorer, soit en utilisant des paramètres individuels. Le service de mise à jour n'utilise pas toujours correctement les paramètres de Microsoft Internet Explorer, surtout dans les cas suivants :

- La connexion Internet n'est pas configurée sur l'ordinateur ;
- Les paramètres de Microsoft Internet Explorer ne sont pas accessibles lorsqu'aucun utilisateur n'est enregistré dans le système d'exploitation.
- Le serveur proxy requiert une autorisation.

Dans tous ces cas, il est nécessaire de définir les paramètres du réseau directement dans les paramètres du service de mise à jour.

- Utilisation d'un serveur proxy qui n'est pas compatible avec le service de mise à jour de Kaspersky Anti-Virus.

  Le service de mise à jour ne fonctionne pas avec Kerio WinRoute car WinRoute ne résout pas entièrement le protocole http 1.0. Dans ce cas, nous vous recommandons d'utiliser n'importe quel autre serveur proxy.

  De même, le service de mise à jour ne fonctionne pas via le protocole FTP avec Microsoft ISA Server. Dans ce cas, il est conseillée de procéder à la mise à jour au départ des serveurs de Kaspersky Lab via le protocole HTTP.

Question : *j'ai perdu ma connexion au réseau/à Internet après l'installation de Kaspersky Anti-Virus. Que faire* ?

Cela signifie qu'il y a eu un conflit entre le module de protection contre les attaques de réseau de Kaspersky Anti-Virus et le pare-feu installé sur votre ordinateur.

Pour rétablir la connexion au réseau local/à Internet, il faut désactiver la protection contre les attaques de réseau. Pour ce faire :

- Ouvrez la fenêtre principale de Kaspersky Anti-Virus for Windows Workstations et passez à l'onglet **Paramètres** (cf. ill. 3)
- Ouvrez, à l'aide du lien Protection en temps réel, la fenêtre **Configuration de la protection en temps réel** et sélectionnez l'onglet **Réseau** (cf. ill. 24)
- Désélectionnez la case **Activer la protection en temps réel contre les attaques de réseau** et cliquez sur **OK**.

Pour que les paramètres que vous avez sélectionnés entrent en vigueur, vous devez redémarrer l'ordinateur. Pour ce faire, cliquez sur **Oui** dans la fenêtre adéquate. Si vous souhaitez redémarrer l'ordinateur plus tard, cliquez sur **Non**.

Question : *depuis l'installation de Kaspersky Anti-Virus, l'ordinateur a un comportement bizarre (« écran bleu », redémarrage constant, etc.) Que faire ?*

Cette situation est rare mais elle peut se produire en cas de conflit entre Kaspersky Anti-Virus et une application installée sur l'ordinateur.

Pour rétablir le bon fonctionnement de votre système d'exploitation, suivez les instructions ci-après :

1. Appuyez sur **F8** au tout début du démarrage de l'ordinateur jusqu'à ce que le menu de sélection du mode de démarrage apparaisse.
2. Sélectionnez le point **Mode sans échec** et chargez le système d'exploitation.
3. Lancez Kaspersky Anti-Virus
4. Ouvrez l'onglet **Paramètres** de la fenêtre principale et cliquez sur le lien Options avancées.
5. Dans la fenêtre **Options avancées** qui s'ouvre, ouvrez l'onglet **Sécurité** (cf. ill. 61) et désélectionnez la case **Lancer Kaspersky Anti-Virus au démarrage du système**. Cliquez sur **Ok**.
6. Redémarrer le système d'exploitation en mode normal.

Ensuite, contactez le service d'assistance technique via le site Internet de Kaspersky Lab (rubrique **Services → Centre de support → Résoudre un problème**). Décrivez avec le plus de précision possible le problème et les conditions dans lesquelles il survient.

Il faudra joindre à la demande le fichier du tampon complet de la mémoire du système d'exploitation Microsoft Windows. Pour ce faire, suivez ces instructions :

1. Cliquez avec le bouton droit de la souris sur l'icône **Poste de travail** et sélectionnez **Propriétés** dans le menu contextuel qui s'affiche.
2. Dans la fenêtre **Propriétés du système**, sélectionnez l'onglet **Avancé** et dans la section **Démarrage et récupération**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Démarrage et récupération**, sélectionnez **Image mémoire complète** dans la liste déroulante de la section **Ecriture des informations de débogage**.

Par défaut le fichier de l'image est sauvegardé dans le répertoire système *memory.dmp*. Vous pouvez modifier l'emplacement de sauvegarde en modifiant le nom du répertoire dans le champ correspondant.

4. Reproduisez le problème qui entraîne le gel de Kaspersky Anti-Virus.
5. Assurez-vous que l'image mémoire complète a bien été enregistrée.

ANNEXE A. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Kaspersky Anti-Virus vous permet de contacter le Service d'assistance technique de Kaspersky Lab dans les cas suivants :

- Vous avez l'impression que le logiciel ne fonctionne pas normalement ou de nombreuses erreurs se produisent.
- Kaspersky Anti-Virus a découvert un objet potentiellement infecté par un virus ou l'une de ses variantes et l'accès à cet objet contenant des données importantes est bloqué. Vous souhaiteriez pouvoir continuer à travailler avec ce fichier.

Si des problèmes surviennent pendant l'utilisation de Kaspersky Anti-Virus, assurez-vous que la solution n'est pas proposée dans ce manuel et plus particulièrement dans le chapitre consacrée aux **Questions fréquemment posée** (cf. Chapitre 10, p. 206) ou dans la rubrique **Services/ FAQs/Solutions** du site de Kaspersky Lab (www.kaspersky.com/fr).

Si vous ne trouvez pas la solution à votre problème dans ces sources, contactez le service d'assistance technique de Kaspersky Lab.

Pour les questions urgentes, composez le numéro de téléphone repris dans la rubrique C.2 à la page 235. L'assistance technique par téléphone est offerte 24h/24 en russe, en anglais, en français et en allemand. N'oubliez pas que pour pouvoir bénéficier de l'assistance, vous devez être un utilisateur enregistré et vous devrez transmettre votre numéro d'inscription à l'opérateur (en cas d'achat du logiciel dans une boîte) ou les informations relatives à votre commande (en cas d'achat en ligne).

Pour envoyer un message au Service d'assistance technique de Kaspersky Lab au sujet d'échec dans le fonctionnement du logiciel :

Cliquez sur le lien Envoi d'une requête au service d'assistance technique situé dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 4) de la fenêtre principale du logiciel.

Cette action entraînera l'ouverture automatique d'une page Web reprenant un formulaire de contact du Service d'assistance technique. Vous devez remplir ce formulaire. La première fenêtre vous invite à saisir les données relatives au problème rencontré et à la licence de Kaspersky Anti-Virus :

- Sélectionnez le **Type de requête** dans la liste déroulante en indiquant le problème qui survient pendant l'utilisation de Kaspersky Anti-Virus Personal.
- Sélectionnez **Kaspersky Anti-Virus Personal** parmi les logiciels de Kaspersky Lab et décrivez en détails le problème que vous rencontrez dans le champ **Informations détaillées de la requête**.
- Sélectionnez le type d'enregistrement du programme en choisissant **Clé de licence** si vous avez achetez le logiciel dans un magasin ou si vous avez installé la licence depuis une disquette ou **commande en ligne** si vous avez acheté le logiciel en ligne.
- Saisissez le numéro de série de votre clé dans le champ **Numéro de sérié de la licence ou commande en ligne**. Ces informations figurent dans le champ **Numéro** de la fenêtre **Administration des clés de licence** (cf. ill. 107).
- Saisissez votre adresse électronique dans le champ **Adresse électronique.**
- Cliquez sur **Suivant**.

La page suivante vous invite à décrire la configuration matériel et logiciel de l'ordinateur et les périphériques utilisés. Vous pouvez saisir ces informations manuellement ou utilisez le service de collecte automatique de ces informations. Pour ce faire, assurez-vous que votre navigateur accepte les objets Active-X puis cliquez sur **Saisir**. Fournissez également les informations suivantes:

- Si le problème est survenu pendant l'utilisation conjointe de Kaspersky Anti-Virus et d'un autre programme, veuillez saisir son nom dans le champ **Incompatibilités identifiées**.
- Saisissez vos coordonnées dans la rubrique **Coordonnées** afin que nous puissions vous contacter pour vous aider à résoudre le plus vite possible le problème.
- Saisissez le code numérique spécial affiché dans la section **Protection contre l'enregistrement automatique** puis cliquez sur **Envoyer**.

Lorsque Kaspersky Anti-Virus met en quarantaine un fichier potentiellement infecté, vous pouvez tenter de le réparer après avoir mis les bases antivirus à jour (pour de plus amples informations, consultez le point 5.10.1.2 à la page 111). Toutefois, lorsque la réparation de l'objet est impossible et que vous devez absolument le réparer le plus vite possible, vous pouvez l'envoyer à Kaspersky Lab en vue d'un examen. Il se peut en effet que ce fichier est infecté par un virus encore inconnu ou qu'il s'agisse simplement d'une fausse alerte.

Attention ! Vous pouvez envoyer les fichiers suspects à Kaspersky Lab uniquement s'ils ont été analysés avec les bases antivirus actualisées le jour de l'envoi.

Pour envoyer vos demandes au service d'assistance technique via le système de traitement automatique des requêtes des clients :

Cliquez sur Commentaires, dans la partie gauche de l'onglet Assistance technique (cf. ill. 4) de la fenêtre principale.

Cette action entraînera l'ouverture de MS Internet Explorer à un formulaire situé sur le site de Kaspersky Lab. Saisissez les informations requises et formulez votre demande. Les opérateurs du service d'assistance technique tenteront de la traiter le plus rapidement possible.

Pour envoyer un fichier à Kaspersky Lab en vue d'un examen :

Sélectionnez le fichier dans la fenêtre **Quarantaine** (cf. point 5.10.1.2, p. 111) puis cliquez sur **Envoyer**.

Cette action entraînera l'ouverture automatique du client de messagerie installé sur votre ordinateur, par exemple Microsoft Outlook Express, et la composition d'un nouveau message qui reprendra en pièce jointe l'objet potentiellement infecté. Envoyez le message. Les experts de Kaspersky Lab étudieront attentivement le fichier reçu et tenteront de restaurer les données qu'il contient. Quels que soient les résultats de l'examen, vous recevrez une réponse exhaustive.

Nous attirons votre attention sur le fait que vous pouvez envoyer à Kaspersky Lab un maximum de trois fichiers par jour. De plus, chacun de ces fichiers doit avoir été analysé par Kaspersky Anti-Virus au plus tard trois jours avant l'envoi.

Il peut arriver que Kaspersky Anti-Virus n'identifie pas lors de l'analyse des fichiers potentiellement infectés alors que vous êtes convaincu qu'un ou plusieurs fichiers de votre ordinateur sont infectés par un nouveau type de virus. Vous pouvez envoyer ces fichiers également à Kaspersky Lab en vue d'un examen.

Pour envoyer à Kaspersky Lab les fichiers que vous pensez être infectés en vue d'un examen :

Cliquez sur le lien Envoi d'un fichier pour examen dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 4). Dans la boîte de dialogue qui apparaît, sélectionnez les fichiers sur lesquels portent vos soupçons.

La marche à suivre pour l'envoi d'un courrier électronique à Kaspersky Lab est entièrement identique à celle décrite pour l'envoi de fichiers potentiellement infectés depuis la quarantaine.

ANNEXE B. GLOSSAIRE

Ce manuel reprend des termes et des notions propres à la lutte contre les virus informatiques. Ce glossaire vise à vous offrir une définition de ces différents termes. Les termes sont présentés par ordre alphabétiques.

A

Administrateur (sécurité) : personne qui assure l'administration du fonctionnement de l'application. Il peut travailler soit à distance à l'aide de la *console d'administration*, soit via l'interface locale.

Administrateur du réseau logique : personne chargée de l'administration du fonctionnement de Kaspersky Anti-Virus via Kaspersky Administration Kit 5.0, le système d'administration centralisée.

Administration centralisée de l'application : administration de l'application à l'aide des services d'administration proposés par Kaspersky Administration Kit 5.0.

Adware : programme introduit dans des applications à l'insu de l'utilisateur et dont l'objectif est d'afficher des publicités. Ces programmes sont diffusés gratuitement. Les publicités s'affichent sur l'interface de travail. Bien souvent, ces programmes recueillent des données personnelles sur l'utilisateur et les transmettent à l'auteur du programme, modifient les paramètres du navigateur (page d'ouverture, paramètres de sécurité, etc.) et créent un trafic non contrôlé par l'utilisateur. Tout ceci peut entraîner une violation de la sécurité, voire des pertes financières.

Agent d'administration : application spéciale garantissant l'interaction entre le serveur d'administration et les applications faisant partie des solutions pour entreprises de Kaspersky Lab. Il fait partie de Kaspersky Administration Kit.

Analyse complète : mode de fonctionnement qui permet à l'utilisateur de sécurité de rechercher quand il le souhaite la présence d'éventuels virus dans tout l'ordinateur et de réparer ou de supprimer les objets suspects ou infectés découverts.

Analyser les fichiers infectés en fonction de l'extension : l'extension du fichier est prise en compte pour l'analyse.

Analyser les fichiers infectés en fonction du format : l'analyse porte sur les fichiers en fonction du format, c'est-à-dire que le contenu du fichier est analysé, à savoir l'identificateur de format dans l'entête.

B

Bases antivirus : il s'agit des bases de données développées par les experts de Kaspersky Lab. Elles reprennent une description détaillée de tous les virus connus à l'heure actuelle ainsi que des méthodes utilisées pour les identifier et réparer les dégâts qu'ils causent. Elles sont

actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouveaux virus apparaissent. Afin d'accroître l'efficacité de la découverte des virus, nous vous recommandons de procéder à la mise à jour régulière des bases antivirus.

Bases antivirus étendues : bases standard augmentées de complémentaires qui permettent au logiciel de découvrir les riskwares sur votre ordinateur.

Bases antivirus standard : bases antivirus qui permettent de découvrir tous les programmes malveillants connus à ce jour et de réparer les objets et les fichiers endommagés.

Bases de données de messagerie électronique : bases de données qui reprennent les messages électroniques sauvegardés sur votre ordinateur. Chaque message entrant/sortant est repris dans la base après son envoi ou sa réception. Ces bases sont couvertes par la protection en temps réel de votre ordinateur.

Bloquer l'objet : empêcher les applications externes d'accéder à l'objet. L'objet bloqué ne peut être ni lu, ni exécuté, ni modifié, ni supprimé.

C

Clé de licence actuelle : clé de licence installée et utilisée actuellement par Kaspersky Anti-Virus. Elle définit la durée de validité de la licence et la politique de licence par rapport au logiciel. Il ne peut pas y avoir plus de deux clés « actuelles » activées.

Clé de licence de réserve : clé de licence installée, mais pas encore activée pour Kaspersky Anti-Virus. La clé de licence de réserve entrera en vigueur dès la fin de la période de validité de la clé de licence actuelle.

Clé de licence : fichier avec une extension **.key* qui représente votre clé personnelle, indispensable à l'utilisation de Kaspersky Anti-Virus. La clé de licence est reprise dans le pack logiciel lorsque vous achetez celui-ci chez un revendeur Kaspersky Lab. Par contre, elle vous sera envoyée par courrier électronique si vous achetez le logiciel en ligne. Kaspersky Anti-Virus NE PEUT FONCTIONNER sans la clé de licence.

Console d'administration : composant de l'application Kaspersky Administration Kit 5.0 qui constitue l'interface utilisateur pour l'administration de Kaspersky Anti-Virus. Fait partie de Kaspersky Administration Kit 5.0.

Copie de sauvegarde : création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et mise de cette copie dans le dossier de sauvegarde.

D

Disques virtuels (Disques RAM) : secteur de la mémoire vive (RAM) de l'ordinateur personnel qui émule et qui se comporte comme un disque physique normal de l'ordinateur.

Dossier de sauvegarde : dossier spécial prévu pour accueillir pendant un laps de temps défini les copies de sauvegarde des fichiers avant leur réparation ou leur suppression.

Durée de validité de la licence : période pendant laquelle vous pouvez utiliser toutes les fonctions de Kaspersky Anti-Virus. Cette durée est définie par la clé de licence et est égale à une année calendaire à partir de l'activation de la clé. Lorsque la licence est arrivée à échéance, les fonctions du logiciel sont réduites : il n'est plus possible de mettre les *bases antivirus à jour et des modules de l'application*.

E

Etat de la protection antivirus : état actuel de la protection antivirus, caractérisé par le niveau de protection de l'ordinateur.

Exclusions : ensemble de paramètres qui permettent d'exclure certains objets de l'analyse. Vous pouvez configurer ces exclusions aussi bien pour la *protection en temps réel* que pour *l'analyse complète*. Par exemple, vous pouvez exclure les *archives* de l'analyse complète de votre ordinateur ou définir les masques des fichiers que vous ne souhaitez pas analyser.

F

Fichier de configuration : fichier contenant les paramètres de base du logiciel. Il est possible d'exporter les paramètres de configuration dans un fichier (sauvegarde) ou de les importer au départ d'un fichier (chargement).

Flux NTFS complémentaires (flux NTFS) : flux de données du disque en provenance du système de fichier NTFS qui viennent en complément du flux principal où se trouve son contenu.

G

Groupe d'administration : groupe d'ordinateurs réunis pour la facilité de l'administration du groupe. Le groupe est administré comme un tout. Il est possible de lui appliquer une stratégie de groupe, de l'inclure dans d'autres groupes et d'appliquer des commandes d'administration.

H

Hack Tools : programme utilisé par des personnes malveillantes pour s'introduire dans l'ordinateur d'autrui. Cette catégorie comprend les dispositifs de balayage, les programmes de déchiffrage de mot de passe et tout autre programme qui vise à pénétrer dans les ressources d'un réseau.

J

Jokeware : logiciels qui n'infligent aucun dégât direct à l'ordinateur mais qui affiche des messages signalant que l'ordinateur est déjà endommagé ou qu'il sera endommagé sous certaines conditions. Ces messages portent souvent sur des menaces fictives, par exemple le formatage du

disque (alors qu'aucun formatage n'a eu lieu), signalent des virus dans des fichiers sains.

K

Kaspersky Administration Kit 5.0 : application faisant partie des logiciels Kaspersky Business Optimal et Kaspersky Corporate. Elle sert à l'exécution centralisée des principales tâches d'administration pour la gestion du système de protection antivirus du réseau de l'entreprise utilisant les solutions de Kaspersky Lab.

L

Liste noire : base de données reprenant les informations relatives aux clés de licence dont les détenteurs ont violé les conditions d'utilisation ou aux clés qui ont été livrées mais qui pour une raison quelconque n'ont pas été vendues. Le contenu de la « liste noire » est mis à jour chaque jour en même temps que les bases antivirus et sans celui-ci, Kaspersky Anti-Virus ne fonctionnera pas.

M

Masque de fichier : il s'agit de la représentation du nom et de l'extension d'un fichier à l'aide de caractères généraux. Les deux principaux caractères utilisés à cette fin sont * et ? (* représente une chaîne de caractères quelconques et ? représente un caractère quelconque. Ces caractères permettent de représenter n'importe quel fichier. N'oubliez que le nom du fichier et son extension sont toujours séparés par un point.

Mise à jour : procédure de remplacement/d'ajout de nouveaux fichiers (bases antivirus ou modules logiciels de l'application) depuis les serveurs de mises à jour de Kaspersky Lab.

Mise en quarantaine des objets : mode de traitement d'un objet *suspect* qui consiste à bloquer l'accès et à le mettre en quarantaine pour la suite du traitement.

Mises à jour disponibles : Service Packs contenant l'ensemble des mises à jour urgentes recueillies sur une certaine période ainsi que les modifications apportées à l'architecture de l'application.

Mises à jour urgente : mises à jour critiques des modules de l'application.

Modules de l'application : fichiers faisant partie de la distribution de Kaspersky Anti-Virus for Windows Workstations et responsables de l'exécution des principales fonctions de l'application. A chaque tâche exécutée par Kaspersky Anti-Virus (protection en temps réel, analyse à la demande et mise à jour) correspond un module exécutable distinct. En lançant la tâche depuis la fenêtre principale de l'application, vous lancez le module correspondant à cette application.

N

Niveau recommandé : niveau de protection antivirus qui repose sur les paramètres recommandés par les experts de Kaspersky Lab et qui assure la protection optimale de votre ordinateur. Ce niveau est sélectionné par défaut.

O

Objet infecté : objet qui renferme un code malicieux. Nous vous conseillons vivement de ne pas travailler avec de tels objets car cela pourrait entraîner une infection de votre ordinateur.

Objet OLE : objets ou documents intégrés à d'autres fichiers via la technologie OLE.

Objet suspect : objet dont le code renferme une modification du code d'un virus connu ou d'un code qui évoque celui d'un virus qui n'a pas encore été découvert par Kaspersky Lab.

Objets exécutés au démarrage du système d'exploitation : ensemble des programmes indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont lancés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter de tels objets, ce qui peut par exemple bloquer le lancement du système d'exploitation.

P

Plug-in d'administration de l'application : composant spécial servant d'interface pour l'administration à distance de l'utilisation de l'application via la console d'administration. Le plug-in d'administration est propre à chaque application et fait partie de toutes les applications de Kaspersky Lab qui peuvent être administrées par Kaspersky Administration Kit 5.0.

Pornware : programme établissant une connexion par modem vers un site Internet payant, généralement à contenu pornographique.

Processus de confiance : liste des processus logiciels dont l'activité sur les fichiers n'est pas contrôlée par Kaspersky Anti-Virus en mode de protection en temps réel. Autrement dit, tous les objets exécutés, ouverts et enregistrés par le processus de confiance ne sont pas analysés.

Protection en temps réel : mode de fonctionnement pendant lequel l'application se trouve en permanence dans la mémoire vive de l'ordinateur et surveille les requêtes adressées aux objets des systèmes de fichiers. Avant d'autoriser l'accès à l'objet, l'application vérifie que l'objet est exempt de virus. S'il en détecte un, il propose soit de réparer l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction des paramètres définis).

Q

Quarantaine : dossier spécial prévu pour l'isolation des objets suspects et infectés.

R

Réparation des objets : ensemble des moyens de traitement appliqués aux *objets infectés* qui débouchent sur une restauration complète ou partielle des données ou sur un constat d'incapacité à réparer l'objet en question La réparation des objets s'opère sur la base des enregistrements contenus dans les *bases antivirus*. Lorsque la réparation est la première action prévue pour un objet (autrement dit, la première action exercée sur cet objet directement après sa découverte), une *copie de sauvegarde* de l'objet sera créée avant de procéder à la réparation. En effet, une partie des données peut être endommagée pendant la réparation. La copie vous donne la possibilité de restaurer l'objet à l'état antérieur à la réparation.

Réparation des objets au redémarrage : mode de traitement des objets infectés, utilisés par d'autres applications au moment de la réparation. Ce mode consiste à créer une copie du fichier infecté, à réparer la copie et remplace, au redémarrage, le fichier original infecté par la copie réparée. Dans les systèmes d'exploitation MS Windows 9x, les grands noms d'objet sont remplacés au redémarrage par des noms raccourcis, ce qui peut entraîner un mauvais fonctionnement des applications qui utilisent les objets réparés.

Restauration : rétablissement de l'objet en *quarantaine* ou dans le *dossier de sauvegarde* vers le répertoire de restauration ou le répertoire d'origine, c'est-à-dire le répertoire où il se trouvait avant sa mise en quarantaine, sa réparation ou sa suppression.

Riskware : ces logiciels ne sont pas des virus mais ils représentent néanmoins une menace. Dans certains cas, la présence de tels logiciels sur votre ordinateur expose vos données à des risques. Cette catégorie reprend les programmes d'administration à distance et les dialers qui vous connectent à des sites Internet payants via le modem, etc.

Rootkit: ces utilitaires servent à dissimuler les activités malveillantes. Ils cachent les programmes malveillants afin qu'ils ne soient pas identifiés par les logiciels antivirus. Les rootkits peuvent également modifier le système d'exploitation et changer ses fonctions fondamentales afin de dissimuler sa présence et les actions exécutées par l'individu mal intentionné sur votre ordinateur.

S

Sécurité maximale : niveau de protection de l'ordinateur correspondant au niveau de protection maximum, au détriment d'un léger recul des performances du système.

Serveur d'administration : application spéciale assurant les fonctions de centre d'informations centralisé sur les applications de Kaspersky Lab installées sur les machines du réseau de l'entreprise et permettant de les administrer. Il fait partie de Kaspersky Administration Kit 5.0.

Serveurs de mises à jour de Kaspersky Lab : listes des sites http et ftp de Kaspersky Lab à partir desquels Kaspersky Anti-Virus copie les bases antivirus et les modules de l'application sur votre ordinateur.

Spyware : programme qui vise à accéder de manière illicite aux données de l'utilisateur, de suivre les actions réalisées avec l'ordinateur et de recueillir les informations stockées sur le disque dur. Ce type de programme permet non seulement à son auteur de recueillir des informations, mais également de prendre les commandes des ordinateurs. Les spywares sont diffusés au sein d'applications gratuites et sont installés à l'insu de l'utilisateur. Les programmes de suivi de frappe de clavier, les programmes de déchiffrage de mot de passe et les programmes qui recueillent les informations confidentielles (comme les numéros de carte de crédit) appartiennent à cette catégorie.

Stratégie de groupe : ensemble de paramètres de fonctionnement de l'application dans le groupe d'administration en cas de gestion via Kaspersky Administration Kit 5.0.

Suppression d'un objet : mode de traitement d'un objet qui consiste à le supprimer de votre ordinateur. Ce traitement doit être appliqué aux objets infectés. Lorsque la suppression est la première action prévue, le logiciel crée d'abord une copie de *sauvegarde de l'objet*. Cette copie vous permettra de restaurer l'objet original.

T

Tâche : action exécutée par l'application de Kaspersky Lab.

Technologie iChecker™ : technologie permettant d'exclure de l'analyse les objets qui n'ont pas été modifiés depuis la dernière analyse. Cette technologie repose sur l'utilisation de bases de données avec les sommes de contrôle des objets.

Technologie iStreams™ : cette technologie exclut de l'analyse les fichiers situés sur le disque avec un système de fichiers NTFS et qui n'ont pas changé depuis la dernière analyse. Cette technologie repose sur la technologie de conservation des sommes de contrôle des fichiers dans les flux complémentaires NTFS.

V

Virus inconnu : nouveau virus au sujet duquel il n'existe aucune information dans les *bases antivirus*. En règle générale, les virus inconnus peuvent être malgré tout identifiés par Kaspersky Anti-Virus grâce à *l'analyse heuristique* et ces objets reçoivent le statut de *suspects*

Vitesse maximale : niveau de protection de l'ordinateur correspondant à la vitesse maximale de fonctionnement, au détriment d'un léger recul du nombre d'objets analysés.

ANNEXE C. KASPERSKY LAB

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

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

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

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

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

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

C.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Microsoft Windows 98/ME, 2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (riskware). Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Le système unique d'analyse heuristique des données neutralise efficacement les virus inconnus. Le logiciel peut fonctionner dans l'un des modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :

- La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
- **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

Kaspersky Anti-Virus® Personal ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une **nette augmentation de la rapidité d'exécution de l'application**.

Le logiciel représente donc un obstacle de taille pour les virus qui tenteraient d'infecter l'ordinateur via le courrier électronique. Kaspersky Anti-Virus® Personal analyse et répare automatiquement tous les messages entrants et sortants via les protocoles POP3 et SMTP. Il décèle également avec efficacité les virus dans les bases de données de messagerie.

Le logiciel est compatible avec plus de 700 formats de fichiers archivés ou compressés et assure l'analyse antivirale automatique de leur contenu. Il peut également supprimer tout code malveillant des fichiers archivés au format **ZIP, CAB, RAR, ARJ, LHA** et **ICE**.

La simplicité de la configuration du logiciel est assurée grâce à l'existance de trois niveaux prédéfinis : **Sécurité maximale**, **Recommandé** et **Vitesse maximale**.

Les bases de données antivirus sont actualisées toutes les trois heures. Leur distribution est garantie même en cas de coupure ou de modification de la connexion.

Kaspersky Anti-Virus® Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Microsoft Windows 98/ME, Microsoft Windows 2000/NT, et Microsoft Windows XP, ainsi que des applications Microsoft Office. Kaspersky Anti-Virus® Personal Pro dispose d'un outil intégré de mise à jour pour le téléchargement des bases de données antivirus et des modules de programmes. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Ce système d'analyse heuristique de seconde génération parvient à neutraliser les virus inconnus. L'utilisateur peut facilement configurer l'application à travers une interface simple et facile.

Kaspersky Anti-Virus® Personal Pro possède les caractéristiques suivantes :

- **Analyse à la demande** des unités locales ;
- **Protection automatique en temps réel** de tous les fichiers, contre les virus;
- **Filtre de courrier** qui analyse et désinfecte automatiquement tout le trafic de messagerie entrant et sortant de n'importe quel client de messagerie utilisant les protocoles POP3 et SMTP et détecte efficacement les virus dans les bases de données de messagerie ;
- **Bloqueur de comportements** qui assure une protection maximale des applications MS Office contre les virus ;
- **Analyseur de fichier compressés –** Kaspersky Anti-Virus prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirale automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les fichiers au format **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** ou **ICE**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Microsoft Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite est une suite logicielle conçue pour organiser la protection intégrée des ordinateurs personnels tournant sous Microsoft Windows. Cette solution bloque l'intrusion des programmes malveillants et des riskwares via toutes les sources d'infection possible, vous protège contre l'accès non-autorisés à vos données et lutte contre le courrier indésirable.

Kaspersky® Personal Security Suite possède les fonctions suivantes :

- Protection des données de votre ordinateur contre les virus.
- Protection des utilisateurs des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express contre le courrier indésirable.
- Protection de l'ordinateur contre l'accès non-autorisé aux données ainsi que contre les attaques de pirates informatiques réalisées depuis le réseau local ou Internet.

Kaspersky Lab News Agent

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

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;

- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

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

Kaspersky OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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

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

Kaspersky Anti-Virus 6.0

Kaspersky Anti-Virus 6.0 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 6.0 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 normaux.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.
- **Bloquer les macros Visual Basic for Applications dangereuses** dans les documents Microsoft Office.
- **Restaurer le système** après les actions malveillantes des logiciels espion : 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 6.0

Kaspersky® Internet Security 6.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espion. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés (Microsoft Office Outlook, Microsoft Outlook Express et The Bat!)

- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système arpès une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer.

Kaspersky® Internet Security 6.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif (**technologie SmartStealth™**) empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé,toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

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

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

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[8] intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications

[8] En fonction du type de livraison

utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- *Postes de travail* sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition ;
- *Ordinateurs de poche* sous Microsoft Windows CE et Palm OS et téléphones intelligents tournant sous Microsoft Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

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

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

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

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie.

C.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 D. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN OUVRANT LE BOÎTIER DU CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL.

CONFORMÉMENT À LA LÉGISLATION, LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) ACHETÉS EN LIGNE VIA INTERNET CHEZ KASPERSKY LAB BÉNÉFICIENT D'UN DÉLAI DE RÉTRACTATION DE 7 JOURS FRANCS À COMPTER DE LA RÉCEPTION DES BIEN ACHETÉS, SI CES LOGICIELS N'ONT PAS ÉTÉ DESCELLÉS.

CONCERNANT LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) NON ACHETÉS EN LIGNE VIA INTERNET, ILS NE SERONT NI REPRIS NI ÉCHANGÉS SAUF DISPOSITIONS CONTRAIRES PROPRES AU PARTENAIRE CHEZ QUI LE PRODUIT A ÉTÉ ACHETÉ. DANS CE CAS, KASPERSKY LAB N'EST EN AUCUN CAS ENGAGÉ PAR LES CLAUSES DES PARTENAIRES.

LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel ("Fichier Clé d'Identification") qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser une copie de 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 une copie du Logiciel sur un ordinateur, poste de travail, assistant digital personnel, ou tout autre appareil électronique pour lequel le Logiciel a été conçu (un "Système Client"). Si le Logiciel est inscrit en tant que suite ou paquet avec plus d'un seul Logiciel, cette licence s'applique à tous les Logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée sur le tarif en vigueur ou l'emballage du produit qui concerne chacun de ces Logiciels.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un Système Client ou par plus d'un utilisateur à la fois, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un Système Client 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 ce Système Client. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez le Système Client sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur ("Serveur") dans un environnement multi-utilisateurs ou en réseau ("Mode-Serveur") uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est exigée pour chaque Système Client ou "siège" pouvant se connecter au Serveur à tout moment, indifféremment du fait que de tels Systèmes Clients inscrits ou sièges sont connectés en même temps au Logiciel, y accèdent ou l'utilisent. L'utilisation d'un logiciel ou de matériel réduisant le nombre de Systèmes Clients ou sièges qui accèdent au Logiciel ou l'utilisent directement (e.g., un logiciel ou matériel de "multiplexage" ou de "regroupement") ne réduit pas le nombre de licences exigées (i.e., le nombre requis de licences égalerait le nombre d'entrées distinctes au logiciel ou matériel de multiplexage ou de regroupement frontal). Si le nombre de Systèmes Clients ou sièges pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. Cette licence vous permet d'effectuer ou de télécharger autant de copies de la Documentation que le réseau compte de Systèmes Clients ou sièges possédant une licence d'utilisation du Logiciel, et pourvu que chaque copie contienne les notes de propriété de la Documentation.

1.3 Licences de volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en oeuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous permet d'effectuer ou de télécharger une copie de la Documentation pour chaque copie additionnelle autorisée par la licence de volume, pourvu que chaque copie contienne toutes les notes de propriété de la Documentation.

2. *Durée*. Ce Contrat est valable pour la période indiquée dans le Fichier Clé d'Identification (Ce fichier est unique et est nécessaire à l'activation complète du Logiciel, voir Aide/ sur Logiciel ou " à propos de ", pour les versions Unix/Linux du Logiciel voir les notifications sur la date d'expiration du Fichier Clé) à moins

que celle-ci n'arrive à terme avant pour l'une des raisons notées ci-après. Ce contrat se terminera automatiquement si vous n'en respectez les termes, limites ou conditions décrites. Au-delà du terme ou expiration de ce Contrat, vous devez immédiatement détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez mettre un terme à ce Contrat à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. Assistance technique.

(i) Kaspersky Lab vous fournira une assistance technique ("Assistance Technique") comme décrit ci-dessous pour une période d'un an à condition que:

(a) le paiement des frais de l'assistance technique en cours ait été fait; et

(b) le Formulaire d'Inscription à l'Assistance Technique fourni avec ce Contrat ou disponible sur le site web de Kaspersky Lab ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Lab avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Lab de juger si vous remplissez les conditions nécessaires pour un accès aux services d'Assistance Technique.

(ii) L'Assistance technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Politique de Confidentialité de Kaspersky Lab déposée sur www.kapersky.com/privacy, et vous consentez explicitement au transfert de données vers d'autres pays que le votre en accord avec les termes de la Politique de Confidentialité.

(iv) "Assistance Technique" signifie:

(a) Mises à jour quotidiennes des bases antivirus;

(b) Mises à jour gratuites du logiciel, incluant des mises à niveau de versions;

(c) Assistance Technique étendue par E-mail et assistance téléphonique fournie par votre Vendeur et/ou Distributeur;

(d) Mises à jour de détection et désinfection de virus sous 24 heures.

4. *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.

5. *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.

6. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de six (6) mois suivant le téléchargement ou l'installation du logiciel, acheté de manière physique, ce dernier fonctionnera correctement 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 répondront à ces besoins et que leur utilisation sera exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaîtra tous les virus connus ou n'affichera 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).

7. *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, le Fournisseur 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.

8. (i) 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. En dehors des situations prévues dans les termes des paragraphes (ii) – (iii) ci-dessous, vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat ("Fausse Représentation") et Kaspersky Lab ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé expressément dans ce Contrat.

(i) Rien dans ce Contrat n'engagera la responsabilité de Kaspersky Lab pour toute Fausse Représentation faite en connaissance de cause.

(ii) La responsabilité de Kaspersky Lab pour Fausse Déclaration quant à une question fondamentale pour la capacité du créateur à exécuter ses engagements envers ce Contrat, sera sujette à la limitation de responsabilité décrite dans le paragraphe 7 (iii).