KASPERSKY LAB

Kaspersky Anti-Virus®
Mobile 6.0 Enterprise Edition

GUIDE DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS® MOBILE 6.0
ENTERPRISE EDITION

Guide de l'utilisateur

http://www.kaspersky.com/fr

Date de révision : Octobre 2007

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

Kaspersky Anti-Virus® Mobile Enterprise Edition (désigné en tant que **Kaspersky Anti-Virus**) est conçu pour protéger des périphériques mobiles sous Microsoft Windows Mobile contre les logiciels malveillants ou les messages indésirables, et dispose des fonctionnalités suivantes :

- **Mode de protection en temps réel** du système de fichiers du périphérique – interception et analyse de :
  - tous les objets entrants, transmis au moyen de connexions sans fil (port infrarouge, Bluetooth), les messages EMS et MMS, lors de la synchronisation avec un ordinateur personnel ou du chargement de fichiers par un navigateur ;
  - fichiers ouverts sur le périphérique mobile ;
  - programmes installés depuis l'interface du périphérique.
- **Analyses à la demande ou planifiées** des objets du système de fichiers, présents sur le périphérique mobile ou sur des cartes d'extension mémoire.
- **Mise en sécurité des objets infectés** en quarantaine.
- **Mise à jour des bases de Kaspersky Anti-Virus** utilisée pour détecter les applications dangereuses et supprimer les objets suspects.
- **Interdiction des messages SMS indésirables**.

Kaspersky Anti-Virus ne peut être installé qu'avec l'aide des outils de Kaspersky Administration Kit, qui offrent également à l'administrateur les possibilités suivantes avec Kaspersky Anti-Virus :

- réception d'informations sur l'état de la protection ;
- réception d'informations sur les paramètres courants de l'application ;
- modification des paramètres de l'application au moyen de stratégies ;
- réception d'informations sur les événements significatifs.

À la différence des autres produits Kaspersky Lab, Kaspersky Anti-Virus **ne permet pas** de réaliser les actions suivantes à l'aide des outils de Kaspersky Administration Kit :

- télécharger les mises à jour des bases anti-virus ;
- créer des tâches de groupe, globales ou locales ;
- prolonger la durée de validité de la clé de licence ;
- désinstaller l'application à distance.

L'utilisateur peut personnaliser la configuration de Kaspersky Anti-virus, surveiller l'état courant de la protection et afficher le rapport d'activité de l'application.

Le logiciel possède un menu facile d'emploi et une interface conviviale permettant à l'utilisateur de contrôler les paramètres de Kaspersky Anti-Virus (pour ceux dont la modification est autorisée par la stratégie), d'afficher l'état courant de la protection anti-virus et le journal où sont consignées les actions du programme.

Lors de la détection d'une application dangereuse, Kaspersky Anti-Virus peut réparer l'objet infecté (si cela est possible), le supprimer ou le placer en quarantaine. Aucun copie d'un objet supprimé n'est conservée.

1.1. Spécifications matérielles et logicielles

Kaspersky Anti-Virus peut être installé sur des périphériques mobiles sous l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 2003, 2003SE
- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0.

1.2. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-virus Mobile Enterprise Edition par Internet, qui permet le téléchargement du programme d'installation et de la documentation en format électronique. Vous pouvez également obtenir Kaspersky Anti-virus Mobile Enterprise Edition auprès des opérateurs de services mobiles. Pour plus de détails sur son acquisition, prenez contact avec votre opérateur mobile.

CHAPITRE 2. KASPERSKY ANTI-VIRUS POUR MICROSOFT WINDOWS MOBILE

Ce chapitre décrit le fonctionnement de Kaspersky Anti-virus Mobile Enterprise Edition sur des périphériques mobiles exploités sous l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 2003, 2003SE,
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

2.1. Installation de Kaspersky Anti-Virus

L'installation de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition s'effectue à distance avec Kaspersky Administration Kit.

- Création du paquet d'installation comprenant le fichier de distribution du produit, l'outil d'installation, la clé de licence, le fichier de configuration.
- Copie du paquet d'installation sur le poste distant ; l'outil d'installation est alors démarré sur l'ordinateur et reste en attente jusqu'à la connexion du périphérique mobile.
- Installation de Kaspersky Anti-Virus sur le périphérique mobile qui se connecte à l'ordinateur.

Pour installer Kaspersky Anti-Virus Mobile Enterprise Edition, procédez de la manière suivante :

1. Dans le dossier **Installation distante** de l'explorateur de console, créez un paquet d'installation utilisé pour l'installation à distance de l'application sur les périphériques mobiles (voir Figure 1).

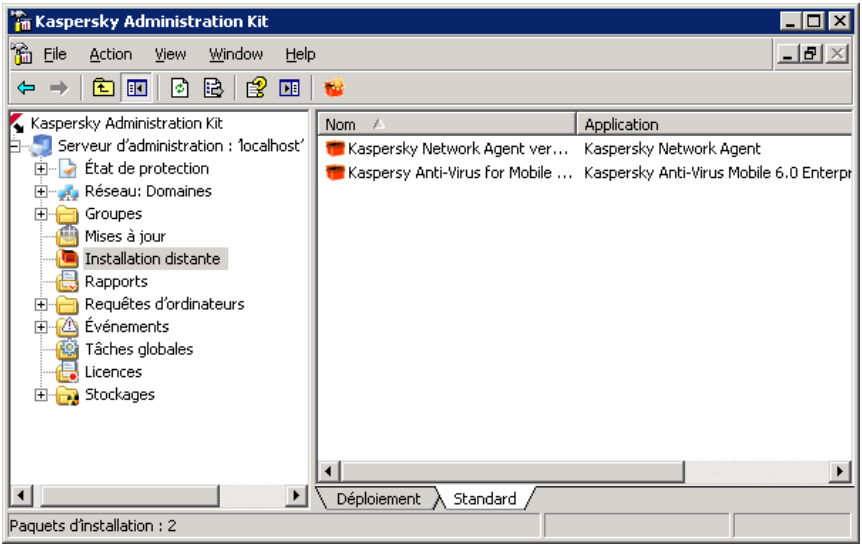

Figure 1. Sélection du paquet d'installation

Pour plus de détails sur la création et l'utilisation de paquets d'installation, voir le Guide de référence de Kaspersky Administration Kit.

2. Ouvrez le menu contextuel du paquet sélectionné puis choisissez **Installer**.

   L'installation du paquet d'installation est conçue comme un Assistant de Microsoft Windows, avec une suite de boîtes de dialogue (ou étapes) qu'il est possible de parcourir avec les boutons **Précédent** et **Suivant** et de conclure avec le bouton **Terminer**. Pour quitter l'Assistant à n'importe quelle étape, utilisez le bouton **Annuler**.

   Attention !

   Le paquet d'installation contient la clé de licence qui sera installée sur un périphérique mobile en même temps. En l'absence de clé de licence dans le paquet d'installation, l'Application ne sera pas activée et ne pourra pas fonctionner.

   Tout autre procédé d'installation de la clé de licence n'est pas pris en charge.

3. À la fin des opérations réalisées par l'Assistant, l'outil **Kav Mobile EE Installer** sera installé sur l'ordinateur ou sur le groupe d'ordinateurs

sélectionné ; cet outil servira à compléter l'installation de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

4. Quand un périphérique mobile se connecte à l'ordinateur, Kav Mobile EE Installer suggère à l'utilisateur d'y installer Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition (voir Figure 2).

> **Attention !**
>
> Pour installer Kaspersky Anti-Virus 6.0 Enterprise Edition sur un périphérique mobile, il faut utiliser Microsoft Active Sync, dans le cas contraire, l'outil **Kav Mobile EE Installer** ne pourra pas détecter les périphériques connectés.

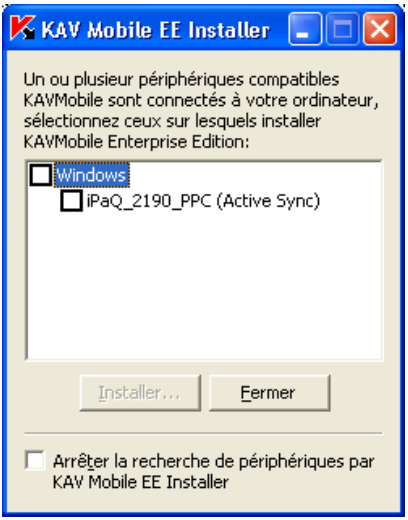

Figure 2. Sélection d'un périphérique mobile

5. Choisissez un périphérique dans la liste de suggestions et cliquez sur **Installer**. Le processus d'installation de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition sur le périphérique mobile sélectionné démarre ensuite.

6. Lisez le texte du contrat de licence sur le périphérique mobile. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir Figure 3)[1].

Figure 3. Contrat de licence

2.2. Utilisation de l'application

Cette section décrit la configuration de l'anti-virus et de la protection en temps réel, le filtrage des messages SMS, l'analyse anti-virus du périphérique mobile ainsi que les mises à jour de l'application.

2.2.1. Lancement de l'application

Pour lancer Kaspersky Anti-virus Mobile Enterprise Edition, procédez de la manière suivante :

1. Ouvrez le menu **Applications** sur votre périphérique mobile.
2. Sélectionnez l'icône *KAV Mobile* et lancez l'application.

Après le démarrage de l'application, le périphérique mobile affiche une fenêtre décrivant l'état des composants principaux de Kaspersky Anti-virus (voir Figure 4).

[1] Toutes les captures d'écran de ce document correspondent à un smartphone modèle I-mate K-JAM smartphone. Sur d'autres modèles de smartphones, l'interface de l'application peut varier.

- **P.T.R** – état de la protection en temps réel. Pour plus de détails, voir section 2.2.3 à la page 11).
- **Dernière analyse complète** – date et heure de la dernière analyse anti-virus du smartphone.
- **Date de la base de données** – date de publication des bases de Kaspersky Anti-Virus utilisées par l'application.

> **Attention !**
>
> Attention. Si l'analyse antivirus d'un périphérique mobile n'a pas été réalisée ou qu'elle date de deux semaine, l'icône correspondante à l'élément change à ⚠. Cette icône apparaît également si le mode de protection en temps réel ou le module Anti-Spam sont désactivés.

- **L'antipourriel est** – Mode d'exploitation du composant Anti-Spam utilisé pour filtrer les messages SMS.

> **Attention !**
>
> Le composant Anti-Spam n'est pas disponible pour le modèle PDA.

Figure 4 Fenêtre d'état des composants de l'application

2.2.2. Interface graphique utilisateur

L'interface graphique contient cinq onglets disponibles depuis le **Menu** (voir Figure 6) :

- L'onglet **Analyser** permet d'effectuer une analyse anti-virus du périphérique mobile, de modifier les paramètres de l'analyse anti-virus et

de la protection en temps réel et de configurer la planification de l'analyse automatique.

- L'onglet **Antipourriel** permet de filtrer les messages SMS et MMS entrants.
- L'onglet **Mittre à jour** permet de mettre à jour la base anti-virus, de modifier les paramètres et de planifier la mise à jour.
- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.
- L'onglet **Info** permet d'afficher les rapports d'activité des composants de l'application ; des informations générales sur l'application et la base anti-virus utilisée, ainsi que de modifier les paramètres généraux de l'application.

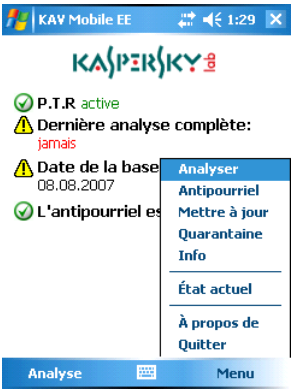

Figure 6. Menu de l'application

Pour revenir à la fenêtre d'état des composants de l'application, sélectionnez **État actuel**.

Pour quitter l'application choisissez **Quitter**.

2.2.3. Analyse et protection antivirus

L'onglet **Analyser** permet d'effectuer une analyse anti-virus du système de fichiers complet et de la mémoire du périphérique mobile ou seulement d'un fichier ou d'un répertoire individuel. Vous pouvez également modifier la configuration de l'analyse et du mode de protection anti-virus, afficher un rapport avec les résultats de l'analyse, ou planifier le démarrage automatique de l'analyse.

2.2.3.1. Protection en temps réel et analyse à la demande des fichiers

La protection en temps réel est un mode de fonctionnement dans lequel une partie de Kaspersky Anti-Virus reste résident dans la mémoire RAM du périphérique mobile, afin de surveiller toutes ses données.

La protection en temps réel démarre au moment où le périphérique est allumé, et reste en exécution jusqu'à son arrêt (si le paramètre correspondant à ce mode est activé).

En outre, Kaspersky Anti-Virus permet de faire une analyse complète du système de fichiers du périphérique mobile.

Les résultats d'activité de la protection en temps réel et de l'analyse à la demande sont conservés dans un rapport. Pour afficher le rapport, sélectionnez l'onglet **Rapport d'analyse**. Le rapport est aussi disponible sur l'onglet **Info** (voir section 2.2.7 à la page 20).

Pour activer le mode de protection en temps réel procédez de la manière suivante :

1. Sélectionnez **Params analyse** sur l'onglet **Analyser**.
2. Activez ou désactivez le mode de la protection en temps réel en définissant la valeur correspondante du paramètre **Protection en temps réel**.

Pour modifier la configuration de l'analyse à la demande, procédez comme suit :

1. Sélectionnez **Params analyse** sur l'onglet **Analyser**.
2. Spécifiez la couverture de l'analyse dans la section **Scan Params** en sélectionnant les types de fichier à analyser, de la manière suivante :
   - **Analyser les archives** – analyse les fichiers comprimés dans des archives;
   - **Executables uniquement** – analyse uniquement les fichiers exécutables.
3. Dans la section **Action antivirus**, spécifiez l'action que l'application doit réaliser quand elle détecte un objet infecté. Pour faire en sorte que Kaspersky Anti-Virus tente de neutraliser l'objet infecté, cochez la case **Tenter de réparer**. Si aucune désinfection n'est nécessaire, sélectionnez une action possible en spécifiant l'une des valeurs suivantes du paramètre **Échec de réparation** :
   - **Quarantaine** – place en quarantaine les objets infectés détectés

- **Demander** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté, de le placer en quarantaine ou de l'ignorer.
- **Supprimer** – supprime les objets infectés détectés
- **Ignorer** – ne réalise aucune action sur les objets infectés

Vous pouvez aussi spécifier l'une des actions suivantes au cas où la réparation de l'objet infecté échouerait. Pour ce faire, cochez la case **Tenter de réparer** et sélectionnez l'action requise dans la liste **Si non réparé**.

Pour lancer une analyse anti-virus :

1. Lancez Kaspersky Anti-virus (voir section 2.2.1 à la page 9).
2. Ouvrez l'onglet **Params analyse**.
   - Spécifiez la couverture de l'analyse dans la section **Scan Params** en sélectionnant les types de fichier à analyser (voir plus haut).
   - Sélectionnez les actions exécutées lors de la découverte d'un objet infecté (voir plus haut).
3. Sélectionnez **Analyse compléte** sur l'onglet **Analyse** (voir Figure 7) si vous souhaitez analyser le système de fichiers complet du périphérique mobile ou **Analyser dossier** pour analyser un dossier individuel.

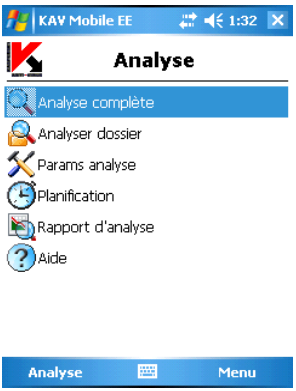

Figure 7. Onglet **Analyse**

Quand l'option **Analyser dossier** est sélectionnée, une fenêtre présente alors le système de fichiers du périphérique mobile. Pour lancer l'analyse sur un dossier, déplacez le curseur vers le dossier concerné et appuyez sur **Analyse**.

Après le démarrage, une fenêtre affiche l'état courant, le nombre d'objets analysés et le chemin de chaque objet en cours d'analyse (voir Figure 8).

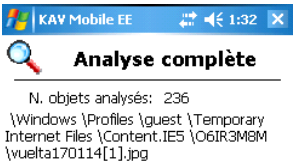

Figure 8. Fenêtre d'**analyse**

Figure 9. Notification de détection de virus

Une fois l'analyse terminée, l'application présente des statistiques générales sur les objets malveillants détectés et supprimés.

2.2.3.2. Planification de l'analyse

Kaspersky Anti-virus permet de planifier des analyses automatiques, qui seront lancés à une heure spécifique. L'analyse sera effectuée en arrière-plan. En cas de détection d'un objet infecté, l'application exécute l'action spécifiée par les paramètres d'analyse (voir section **Params analyse**).

L'analyse programmée est désactivée par défaut.

Pour configurer une analyse planifiée, procédez de la manière suivante :

Ouvrez la page **Analyser**, sélectionnez **Planification** et configurez les paramètres d'analyse (voir Figure 10) :

- **Quotidien** – l'analyse s'exécutera tous les jours. L'heure d'analyse est déterminée par le paramètre **Heure**.
- **Hebdomadaire** – l'analyse s'exécutera chaque semaine. Le jour et l'heure d'analyse sont déterminés par les paramètres **Jour de la semaine** et **Heure**.
- **Désactiver** – l'analyse est lancée manuellement par l'utilisateur uniquement.

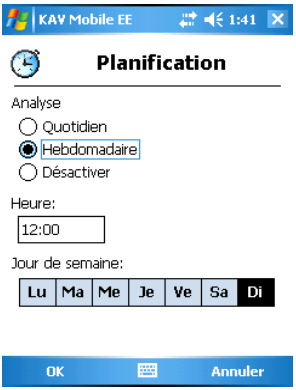

Figure 10. Le menu **Planification**

2.2.4. Utilisation de la quarantaine

Les objets infectés placés en quarantaine ne sont pas en mesure d'endommager votre périphérique mobile et peuvent être supprimés ou restaurés par la suite.

Le logiciel peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Si vous souhaitez configurer l'application pour placer automatiquement en quarantaine les objets infectés, ouvrez la page **Analyse**, sélectionnez **Params analyse** puis choisissez la valeur **Quarantaine** pour le paramètre **Si non réparé** dans la section **Action antivirus**. Si l'objet ne peut être réparé, cochez la case **Tenter de réparer** et sélectionnez **Quarantaine** dans la liste **Si non réparé**.

Si vous avez choisi l'action **Demander**, lors de la détection d'un objet infecté, Kaspersky Anti-virus vous proposera son effacement ou son déplacement en quarantaine.

La page **Quarantaine** permet d'afficher le contenu de la quarantaine (voir Figure 12).

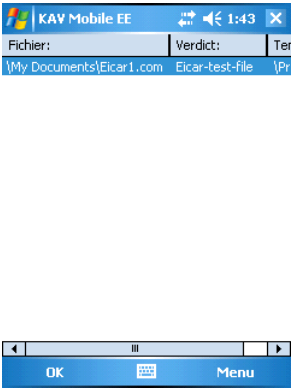

Figure 12. **Quarantaine**

Le menu de la fenêtre Quarantaine permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Détails**).
- Analyse antivirus d'un fichier en quarantaine (**Analyser)**.
- Supprimer l'objet courant (**Supprimer fichier**).
- Réparer un objet en quarantaine (**Réparer)**.
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer**).
- Purger la quarantaine en supprimant tous les objets conservés (**Tout supprimer**).

2.2.5. Utilisation du composant Anti-Spam

Le composant Anti-Spam est une autre caractéristique nouvelle introduite par Kaspersky Anti-virus Mobile 6.0. Il est destiné à protéger le périphérique mobile contre les messages SMS indésirables.

Attention !

Le composant Anti-Spam n'est pas disponible pour le PDA.

Le principe utilisé pour filtrer les messages fait appel aux listes dites noire et blanche. Le composant Anti-Spam permet de bloquer les messages entrants provenant de numéros de téléphone ajoutés à votre liste noire. Les messages provenant de numéros ajoutés à la liste blanche ne seront pas bloqués.

Pour modifier la configuration du composant Anti-Spam :

1. Sélectionnez **Paramètres** sur l'onglet **Antipourriel**.
2. Activer ou désactiver le composant Anti-Spam avec la case à cocher **Activer Antipourriel**.
3. Spécifiez si vous autorisez la réception de messages SMS provenant de numéros de téléphone qui n'appartiennent à aucune des listes en cochant **Recevoir SMS: d'expéditeurs inconnus**.
4. Spécifiez si vous autorisez la réception de messages SMS provenant de numéros de téléphone de votre liste de contacts en cochant **Recevoir SMS: de ma liste de contacts**.

2.2.5.1. Modification des listes blanche et noire

La liste « noire » contient des numéros de téléphone dont la réception de messages SMS est bloquée par le composant Anti-Spam.

La liste « blanche » contient des numéros de téléphone dont la réception de messages SMS est autorisée.

Pour pouvoir modifier la liste noire ou blanche, ouvrez la page **Antipourriel** (voir Figure 13) et sélectionnez la liste souhaitée.

Figure 13. **Menu Anti-Spam**

Pour modifier la liste utilisez le **Menu** :

- **Ajouter** – ajoute un nouvel enregistrement à la liste sélectionnée.
- **Supprimer** – supprime l'enregistrement courant de la liste.
- **Modifier** – modifie l'enregistrement sélectionné dans la liste.

Après sélectionner **Ajouter enregistrement**, spécifiez le numéro de téléphone que vous souhaitez ajouter à la liste. Le numéro peut commencer par un chiffre ou par le signe "+" et ne peut contenir que des chiffres.

Après avoir modifié la liste, appuyez sur **OK** pour revenir à la page **Antipourriel**.

2.2.5.2. Actions appliquées aux messages

Quand vous recevez un message SMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, et en supposant que vous avez autorisé la réception de messages provenant de numéros inconnus (voir section 2.2.5 à la page 16), le composant Anti-Spam affichera un avertissement sur l'écran du périphérique (voir Figure 14).

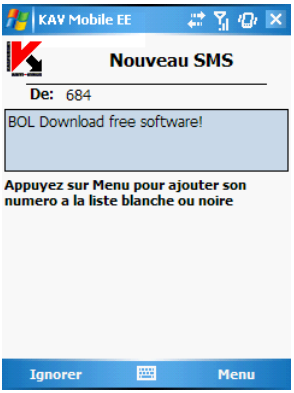

Figure 14. Avertissement du composant Anti-Spam

Utilisez **Menu** pour appliquer l'une des actions suivantes sur le message :

- **Ajouter à la liste blanche** – autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.
- **Ajouter à la liste noire** – bloque la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.

Pour autoriser la réception du message, appuyez sur **Ignorer**. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Des informations sur les messages bloqués sont ajoutées au rapport de l'application. Pour examiner le rapport, ouvrez l'onglet **Antipourriel** et sélectionnez **Rapport** ou cliquez sur **Anti-Spam Rapport** sur le même onglet. Le rapport est aussi disponible sur l'onglet **Info** (voir section 2.2.7 à la page 20).

2.2.6. Mise à jour des bases antivirus

Kaspersky Anti-virus détecte les virus grâce aux enregistrements de ses bases antivirus qui contiennent la description de tous les logiciels malveillants connus. Il est extrêmement important de protéger la sécurité de votre smartphone en mettant à jour fréquemment les bases antivirus.

Vous pouvez mettre à jour la base manuellement ou planifier l'opération. Pour configurer et démarrer la mise à jour, utilisez l'onglet **Mettre à jour** (voir Figure 15). La mise à jour peut se faire par Internet depuis les serveurs de Kaspersky Lab.

Figure 15. Onglet **Mise à jour**

Les informations de mise à jour de la base sont enregistrées dans le rapport. Pour examiner le rapport, ouvrez l'onglet **Mettre à jour** et sélectionnez **Mise à jour rapport**. Le rapport est aussi disponible sur l'onglet **Info** (voir section 2.2.7 à la page 20).

Pour lancer la mise à jour manuelle des bases antivirus depuis les serveurs de Kaspersky Lab :

1. Lancez Kaspersky Anti-virus (voir section 2.2.1 à la page 9) et ouvrez l'onglet **Mettre à jour**.
2. Sélectionnez **Mise à jour** pour lancer l'opération de mise à jour.

Pour planifier une mise à jour automatique des bases antivirus :

1. Lancez Kaspersky Anti-virus (voir section 2.2.1 à la page 9) et ouvrez l'onglet **Mettee à jour**.
2. Sélectionnez **Planification** pour modifier la configuration de mise à jour automatique.
3. Spécifiez la fréquence des mises à jour en modifiant la valeur du paramètre **Mise à jour automatique** :
   - **Tous les jours** – exécute la mise à jour tous les jours. En outre, spécifiez l'**Heure** des mises à jour à réaliser.
   - **Toutes les semaines** – l'analyse est exécutée chaque semaine. En outre, spécifiez le **Jour de la semaine** et l'**Heure** des mises à jour à réaliser.
   - **Désactiver** – l'analyse est lancée manuellement par l'utilisateur uniquement.

L'onglet **Info** vous informe de la date de publication des bases antivirus actuellement installées sur le périphérique mobile et du nombre de signatures de virus. Pour ce faire, sélectionnez **Info base AV** sur l'onglet.

2.2.7. Réception de rapports sur le fonctionnement de l'application

Les rapports sur l'activité de l'application sont regroupés dans la section **Rapports** de l'onglet **Infor**. Un rapport peut être obtenu sur n'importe quelle tâche effectuée par Kaspersky Anti-Virus :

- analyse antivirus ;
- activité du composant anti-spam ;
- mise à jour des bases antivirus.

Par exemple, pour afficher un rapport sur les résultats de l'analyse anti-virus, procédez comme suit :

1. Lancez Kaspersky Anti-virus (voir section 2.2.1 à la page 9).
2. Sélectionnez **Rapports** dans l'onglet **Infor** (voir Figure 16).
3. Sélectionnez un rapport sur la protection en temps réel dans la fenêtre ouverte.

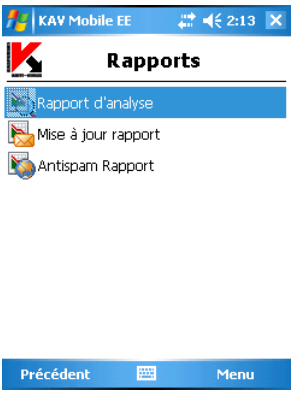

Figure 16. Onglet **Rapports**

2.3. Suppression de l'application

Pour supprimer Kaspersky Anti-Virus :

1. Désactivez l'autoprotection (voir 2.2.3 à la p. 11 pour plus de détails) ;

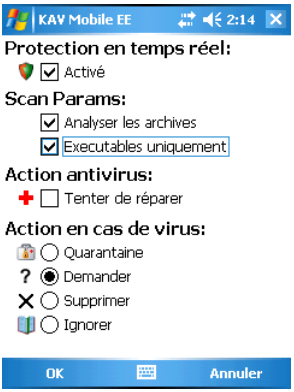

Figure 17. Désactiver l'autoprotection

2. Quittez Kaspersky Anti-Virus. Pour ce faire, sélectionnez **Quitter** dans le menu du programme (voir Figure 18).

Figure 18. Sortie du logiciel

3. Supprimez le programme. Pour ce faire :

   - Cliquez de nouveau sur **Démarrer**, choisissez **Paramètres** puis **Suppression de programme** (voir Figure 19) :

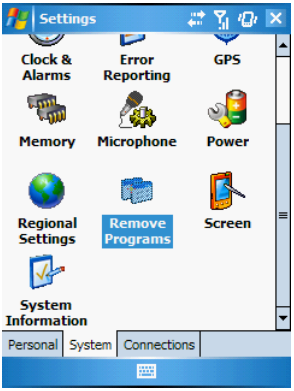

Figure 19. Démarrage de la suppression du logiciel

   - Sélectionnez **Kaspersky Anti-Virus Mobile** dans la liste des applications installées puis cliquez sur **Supprimer** (voir Figure 20).

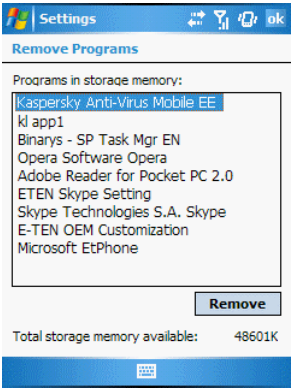

Figure 20. Sélection de programme

- Pour confirmer la suppression, cliquez sur **Oui** (voir Figure 21).

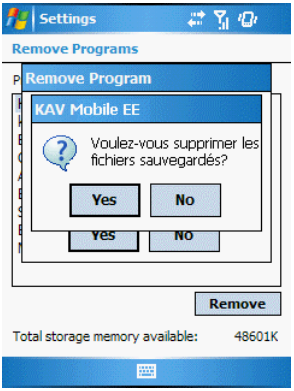

Figure 21. Confirmation de la suppression du programme

CHAPITRE 3. ADMINISTRATION DU LOGICIEL VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit est un système gestionnaire centralisé des tâches administratives liées au système de sécurité de périphériques mobiles.

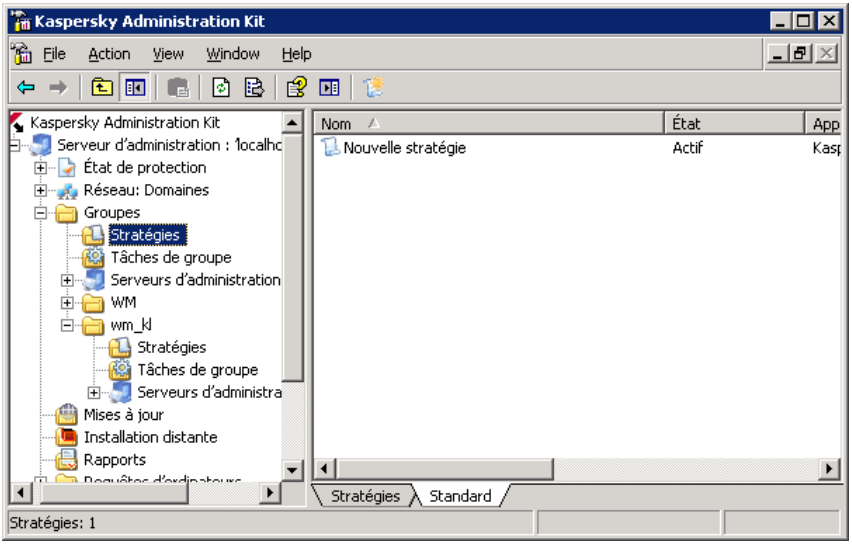

Figure 22. Console d'administration de Kaspersky Administration Kit

Quand il utilise le gestionnaire centralisé Kaspersky Administration Kit, l'administrateur définit les paramètres des stratégies et de l'application. La protection mise en place s'appuie sur ces paramètres.

Une particularité de la gestion centralisée est l'organisation des périphériques mobiles à l'intérieur de groupes, dont les paramètres sont définis moyennant la création et la gestion de stratégies de groupes.

Une stratégie est un ensemble de paramètres Kaspersky Anti-Virus associés à un groupe du réseau logique. Les multiples paramètres qui composent une

stratégie permet de gérer le fonctionnement de l'application Kaspersky Anti-Virus.

Une stratégie peut également prévoir un ensemble de restrictions à la modification de paramètres spécifiques, dans la configuration de l'application. Ces restrictions sont définies depuis l'interface de Kaspersky Administration Kit par un utilisateur disposant de privilèges administrateur.

Remarque :

Pour déplacer le périphérique mobile dans le groupe d'administration, ouvrez la **Console d'administration**, ouvrez le conteneur **Réseau** et configurez-le pour qu'il reflète les domaines..

Pour vous assurer que Kaspersky Administration Kit détecte les périphériques mobiles, cochez la case **Port pour les périphériques mobiles**, sur l'onglet **Paramètres** des propriétés du serveur d'administration.

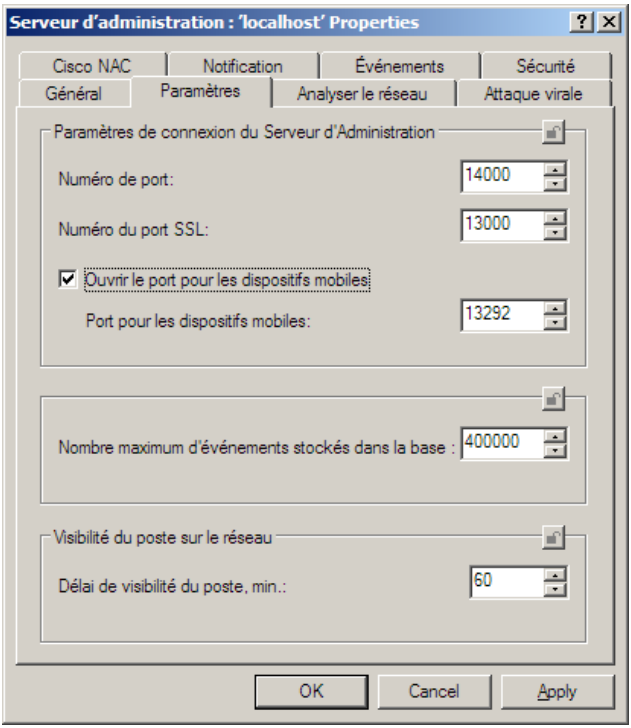

Figure 23. Onglet **Paramètres**

.

3.1. Administration des stratégies

Cette section explique la création et la configuration de stratégies pour Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

3.1.1. Création d'une stratégie

Pour créer une stratégie, procédez de la manière suivante :

1. Dans l'arborescence de console, choisissez le groupe de périphériques mobiles pour lequel vous allez créer une stratégie, dans le dossier **Groupes**.
2. Sélectionnez le dossier **Stratégies** faisant partie du groupe sélectionné, affichez le menu contextuel et sélectionnez la commande **Créer→Stratégie**.

L'outil de création d'une stratégie est conçu comme un Assistant de Microsoft Windows, avec une suite de boîtes de dialogue (ou étapes) qu'il est possible de parcourir avec les boutons **Précédent** et **Suivant** et de conclure avec le bouton **Terminer**. Pour quitter l'Assistant à n'importe quelle étape, utilisez le bouton **Annuler**.

Attention !

À chaque étape de la création d'une stratégie, vous pouvez verrouiller les paramètres avec le bouton  . Si le verrou est fermé, les nouvelles valeurs de la stratégie s'appliqueront plus tard sur les périphériques mobiles.

Etape 1. Saisie des données générales sur la stratégie

La première étape de l'Assistant est une introduction. La première fenêtre de l'Assistant permet de spécifier le nom de la stratégie (champ **Nom**), dans la seconde fenêtre, sélectionnez l'application **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition** dans la liste déroulante **Nom d'application**. Pour appliquer les paramètres de stratégie immédiatement après leur définition, cochez la case **Activer la stratégie** dans la section **État de la stratégie** de la troisième fenêtre.

Etape 2. Définition des paramètres d'analyse antivirus

Au cours de cette étape, vous devez définir les paramètres de l'analyse antivirus du périphérique mobile : couverture et planification de l'analyse. Vous devez aussi définir si le mode de protection en temps réel doit être activé.

Pour exploiter le périphérique mobile dans le mode de protection en temps réel, cochez la case **Activer la protection en temps réel** (voir Figure 24). La protection en temps réel sera alors activée au démarrage du périphérique jusqu'à son arrêt.

Vous pouvez utiliser la section **Analyse à la demande** pour sélectionner les types de fichiers compris dans la couverture d'analyse et pour spécifier les tentatives de réparation appliquées aux objets infectés :

- **Analyser les exécutables uniquement** – analyse les fichiers de programmes exécutables.
- **Analyser les archives** – analyse les fichiers comprimés dans des archives.
- **Tenter de réparer** : essaie de réparer un objet infecté. Tous les objets ne sont pas réparables.

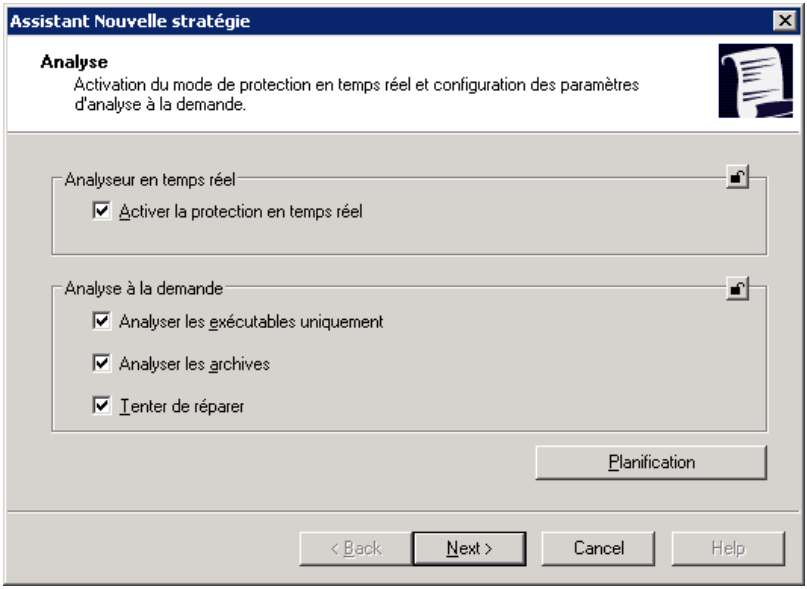

Figure 24. Configuration des paramètres d'analyse antivirus

Pour programmer l'exécution d'une analyse à la demande, cliquez sur **Planification**. Ceci ouvrira une boîte de dialogue vous permettant de spécifier la fréquence d'analyse :

- **Manuellement** - l'action est lancée manuellement par l'utilisateur.

- **Tous les jours** - l'action s'exécutera tous les jours. Spécifiez l'heure de l'analyse dans le groupe de champs **Heure de début**.
- **Toutes les semaines** - l'action s'exécutera certains de jours de la semaine. Dans le groupe de champs **Heure de début** spécifiez l'heure et sélectionnez un jour de la semaine pour exécuter l'analyse à la demande.

Etape 3. Sélection de la source des mises à jour

Au cours de cette étape, vous devez définir l'origine et planifier l'exécution des mises à jour.

Dans le champ associé de la section **Source des mises à jour** (voir Figure 25) spécifiez l'adresse de la source des mises à jour. Seuls les serveurs de mise à jour de Kaspersky Lab peuvent être utilisés.

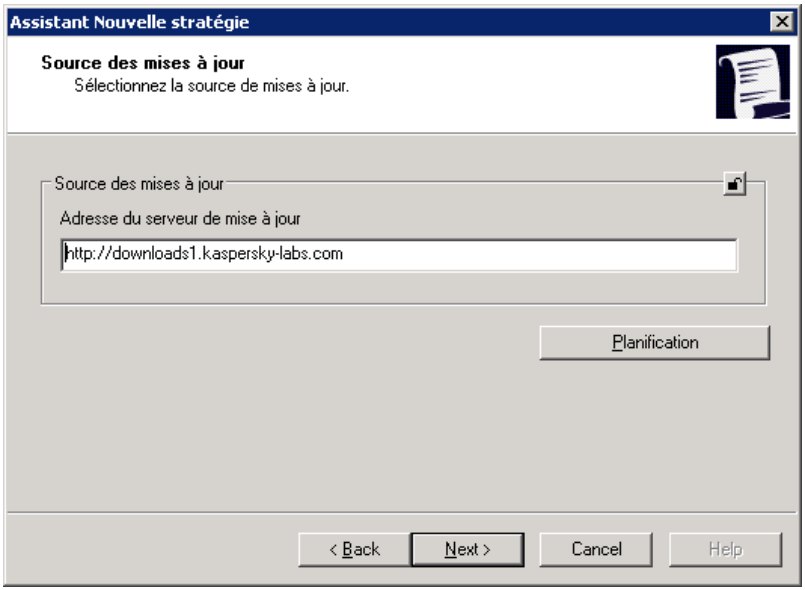

Figure 25. Sélection de la source des mises à jour

Vous pouvez aussi planifier le téléchargement des mises à jour. Pour ce faire, cliquez sur **Planification**. Ceci ouvrira une boîte de dialogue vous permettant de spécifier la fréquence d'analyse :

- **Manuellement** - l'action est lancée manuellement par l'utilisateur.

- **Tous les jours** - l'action s'exécutera tous les jours. Spécifiez l'heure de l'analyse dans le groupe de champs **Heure de début**.
- **Toutes les semaines** - l'action s'exécutera certains de jours de la semaine. Dans le groupe de champs **Heure de début** spécifiez l'heure et sélectionnez un jour de la semaine pour exécuter l'analyse à la demande.

Etape 4. Spécification de paramètres avancés

Au cours de cette étape, vous pouvez spécifier les paramètres du module Anti-Spam et de la période de synchronisation avec le serveur d'administration.

Configurez le module Anti-Spam dans la section **Anti-Spam** (voir Figure 26). Si vous cochez la case **Activer la protection Anti-Spam**, le module Anti-Spam détectera les messages indésirables en fonction des critères suivants :

- **Réception de messages de numéros dans la liste des contacts** - le critère utilisé est la présence des numéros dans la liste blanche. Les messages présents dans la liste blanche de numéros sont toujours remis à l'utilisateur.
- **Interdire les messages de numéros non présents dans la liste blanche et ceux sans numéro d'expéditeur** - le critère indique quels messages ne sont pas délivrés à l'utilisateur.

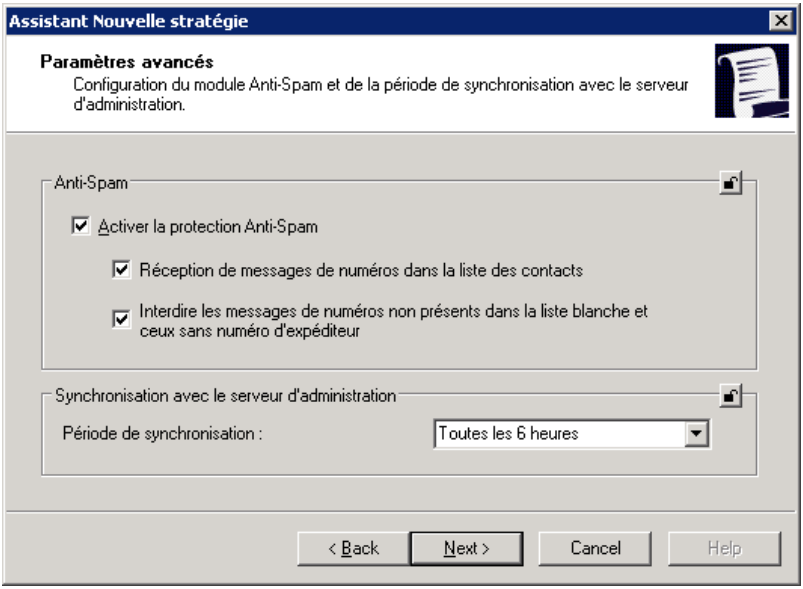

Figure 26. Paramètres d'application avancés

Spécifiez la fréquence de synchronisation dans la liste déroulante **Période de synchronisation** de la section **Synchronisation avec le serveur d'administration**.

Etape 5. Fin de la création de la stratégie

Le dernier écran de l'Assistant informe sur la réussite du processus de création de la stratégie (voir Figure 27).

Après la fin de l'Assistant, les stratégies pour Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition seront ajoutées au dossier **Stratégies** du groupe correspondant et affichées dans le panneau de résultats.

Vous pouvez modifier les paramètres de la nouvelle stratégie et imposer des restrictions à leur modification à l'aide du bouton dans chaque groupe de paramètres. Comme décrit auparavant, l'utilisateur d'un périphérique mobile ne pourra pas modifier des paramètres verrouillés. La stratégie sera activée lors de la première synchronisation du périphérique mobile client avec le serveur.

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

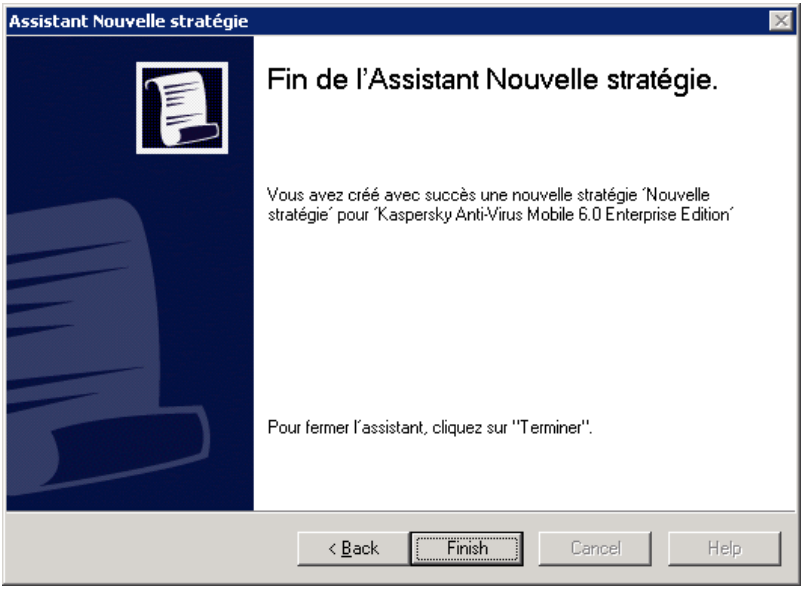

Figure 27. Fin de la création de la stratégie

3.1.2. 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 dans la stratégie d'application et de tâche des groupes imbriqués.

1. Dans l'explorateur de console, dans le dossier **Groupes**, sélectionnez le groupe d'ordinateurs dont vous souhaitez modifier les paramètres de stratégie.
2. Sélectionnez le dossier **Stratégie** faisant partie de ce groupe ; ceci affiche toutes les stratégies du groupe dans le panneau de résultats.
3. Sélectionnez la stratégie requise pour **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition** dans la liste (le nom de l'application est indiqué dans le champ **Application**).
4. Sélectionnez la commande **Propriétés** dans le menu contextuel de la stratégie sélectionnée.

Une boîte de dialogue de configuration des stratégies d'application apparaît, avec un certain nombre d'onglets.

Les onglets **Général**, **Contrôle** et **Événements** sont des onglets standard de Kaspersky Administration Kit (pour plus de détails, voir le Guide de l'administrateur de Kaspersky Administration Kit).

Le reste des onglets contient des contrôles pour paramétrer Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition. La présentation de chacun des onglets figure dans la suite.

Note

Quand vous modifiez les paramètres de stratégie, utilisez le bouton  pour verrouiller les données saisies. Comme décrit auparavant, l'utilisateur d'un périphérique mobile ne pourra pas modifier des paramètres verrouillés.

3.1.2.1. Informations sur l'application

L'information suivante sur la stratégie est affichée dans l'onglet **Général** (voir Figure 28) : nom de la stratégie, nom de l'application associée, version de l'application, date et heure de création de la stratégie et de sa dernière modification.

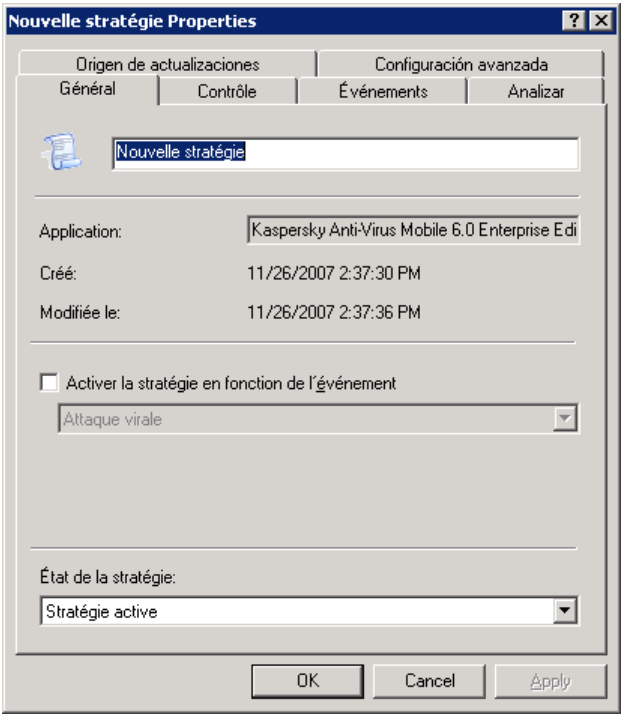

Figure 28. Onglet **Général**

Cette boîte de dialogue permet de modifier le nom de la stratégie, de l'activer ou de la désactiver, ou de configurer son activation lors d'un certain événement.

3.1.2.2. Affichage des résultats de l'application de la stratégie

L'onglet **Contrôle** (voir Figure 29) affiche des informations de référence sur l'application de la stratégie sur les périphériques mobiles présents dans le groupe et sur le nombre de dispositifs pour lesquels la stratégie :

- n'est pas définie ;
- est appliquée ;
- n'est pas encore appliqué ;
- la stratégie n'a pas pu être appliquée en raison d'une erreur.

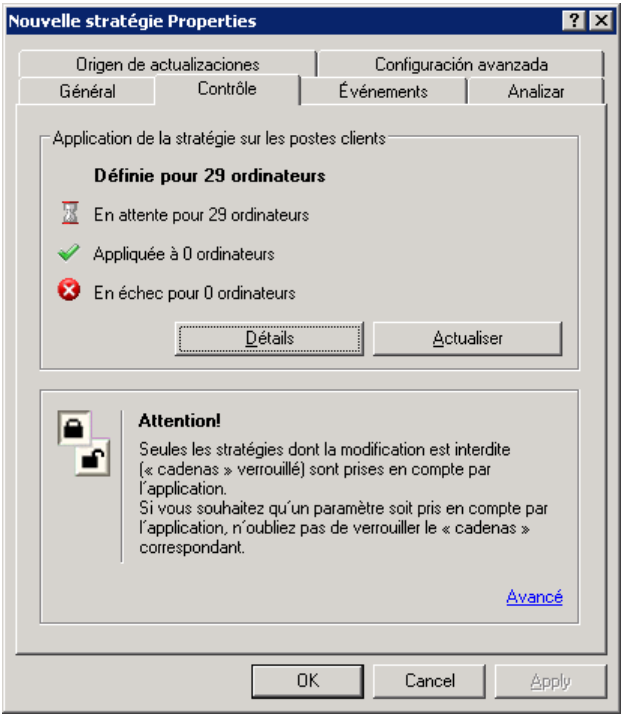

Figure 29. Onglet **Contrôle**

Des détails sur le résultat de l'application de la stratégie sur chaque ordinateur client du groupe sont affichés dans la boîte de dialogue ouverte avec **Détails** (pour plus d'informations voir le Guide de l'administrateur de Kaspersky Administration Kit 6.0).

3.1.2.3. Enregistrement de l'activité de l'application

Pendant son fonctionnement, Kaspersky Anti-Virus génère un certain nombre d'événements. Chaque événement possède une caractéristique qui reflète son niveau d'importance. Il existe quatre niveaux d'importance : événement critique, échec, avertissement et message d'information.

Des événements de même type peuvent avoir différents degrés d'importance, en fonction du moment où l'événement s'est produit.

L'onglet **Événements** (voir Figure 30) affiche les types d'événements générés par le fonctionnement de l'application et qui sont enregistrés dans le rapport, ainsi que l'emplacement disque du rapport et le mode de notification de l'administrateur ou des autres utilisateurs.

Pour afficher les types d'événements, sélectionnez le niveau d'importance requis dans la liste **Niveau d'importance**. Les événements correspondant au niveau d'importance choisi seront affichés dans la zone d'information inférieure.

Pour chaque événement, vous pouvez spécifier s'il doit être enregistré dans le rapport et si l'administrateur doit recevoir des notifications.

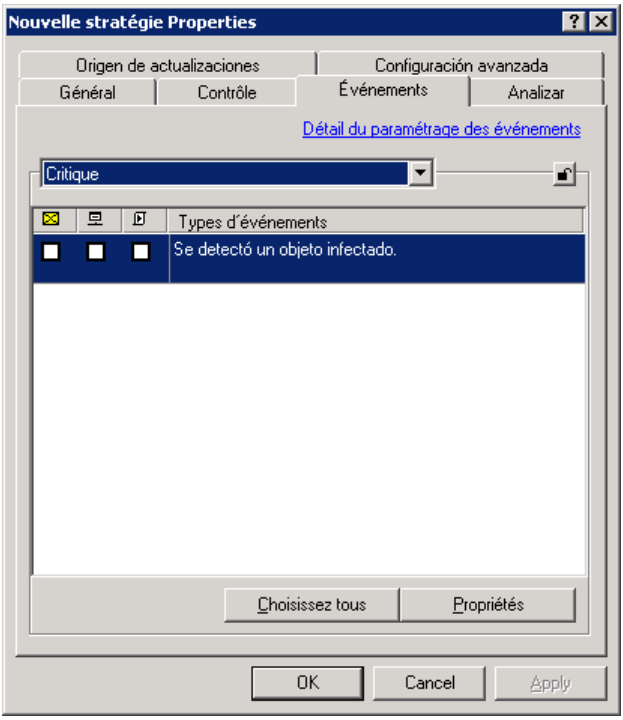

Figure 30. Onglet **Événements**

Pour plus de détails sur le reste des paramètres disponibles dans l'onglet **Événements**, voir le Guide de l'administrateur de Kaspersky Administration Kit 6.0.

3.1.2.4. Définition paramètres d'analyse antivirus

L'onglet **Analyse** (voir Figure 31) permet de définir les paramètres d'analyse à la demande : couverture de l'analyse, actions à réaliser sur les objets infectés et planification de son exécution. Cet onglet permet aussi de définir si le mode de protection en temps réel doit être activé.

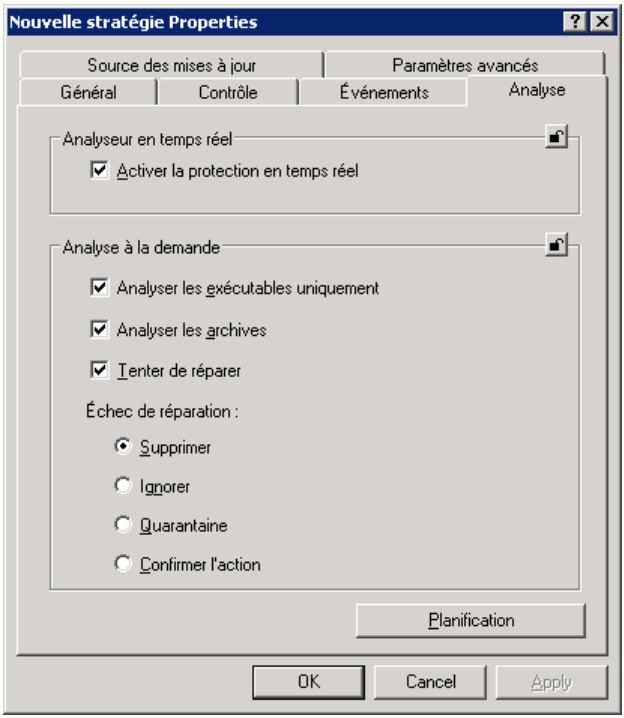

Figure 31. Onglet **Analyser**

Dans la section **Action antivirus** sélectionnez l'action exécutée en présence d'un objet infecté :

- **Supprimer**.
- **Ignorer** - laisse intacts les objets infectés détectés.
- **Quarantaine** – place en quarantaine les objets infectés détectés.
- **Confirmer l'action** – affiche à l'écran un message de détection d'un virus et laisse le choix de supprimer, de mettre en quarantaine ou d'ignorer l'objet infecté.

Les autres paramètres sont similaires a ceux déjà décrits dans la section 3.1.1 à la page 26.

3.1.2.5. Sélection de l'origine des mises à jour de Kaspersky Anti-Virus

L'onglet **Source des mises à jour** (voir Figure 32) permet de spécifier la source de téléchargement des mises à jour des bases antivirus. Cet onglet sert aussi pour planifier l'exécution des mises à jour.

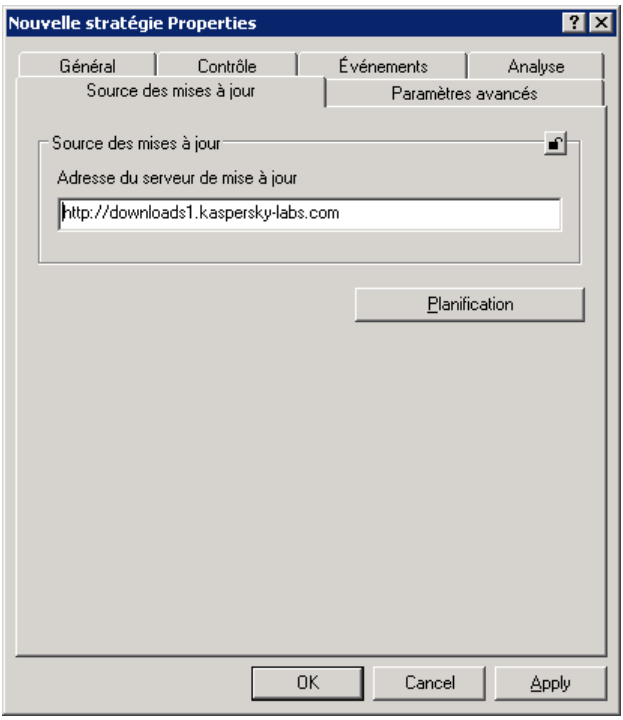

Figure 32. Onglet **Source des mises à jour**

3.1.2.6. Spécification de paramètres avancés

L'onglet **Paramètres avancés** (voir Figure 33) permet de configurer le composant Anti-Spam et de déterminer la fréquence des connexions avec le Serveur d'administration.

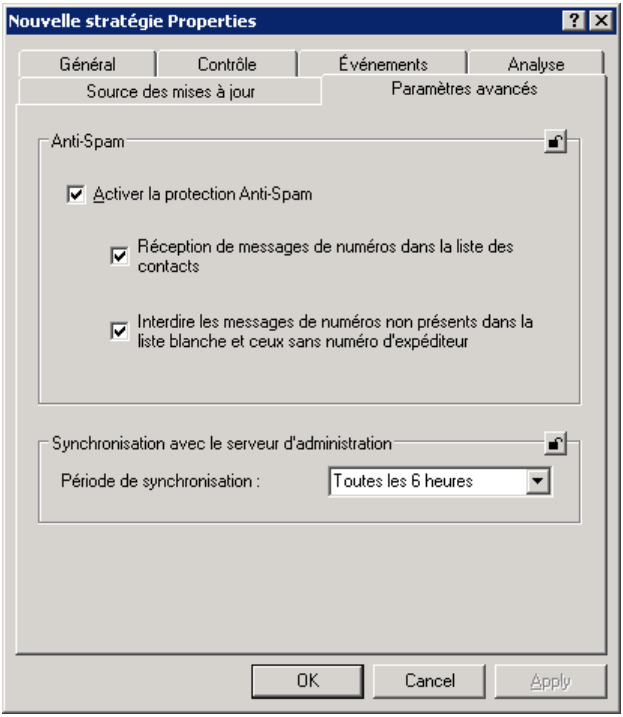

Figure 33. Onglet **Paramètres avancés**

3.2. Contrôle des paramètres d'application

Les paramètres d'application permettent de modifier l'application Kaspersky Anti-Virus installée sur un périphérique mobile, qu'il fasse partie d'un groupe ou qu'il soit local. Vous ne pouvez modifier que les paramètres qui ne sont pas verrouillés par une stratégie (pour plus de détails voir section 3.1 à la page 26).

Pour modifier les paramètres d'application :

1. Sélectionnez le nom du groupe contenant le périphérique mobile, dans le dossier **Groups**.
2. Dans le panneau de résultats sélectionnez le périphérique dont vous souhaitez modifier les paramètres d'application. Sélectionnez la

commande **Propriétés** dans le menu contextuel ou dans le menu **Actions**.

3. Ceci ouvrira la boîte de dialogue **Propriétés : Nom de l'ordinateur** s'affiche dans la fenêtre principale de l'application. Sélectionnez l'onglet **Applications** (voir Figure 34).

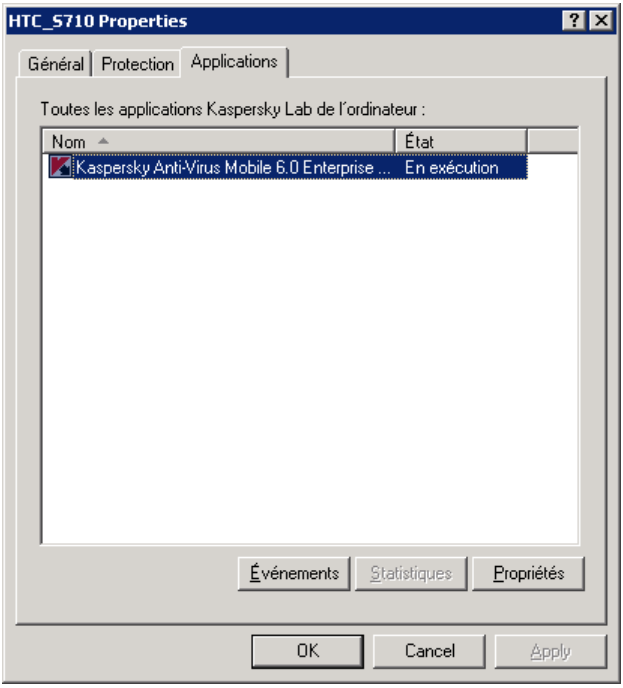

Figure 34. Fenêtre de propriétés du périphérique mobile. Onglet **Applications**

4. Sélectionnez l'application **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition**. Les boutons suivants se trouvent dans la partie inférieure de la fenêtre :

   - **Événements** – affiche la liste des événements apparus pendant le fonctionnement de l'application sur les périphériques mobiles et enregistrés par le Serveur d'administration.
   - **Statistiques** - affiche les statistiques sur le fonctionnement de l'application.

- **Propriétés** - configure l'application dans la fenêtre de paramètres de l'application de Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition

3.2.1.1. Informations sur l'application

L'onglet **Général** (voir Figure 35) permet d'afficher des informations sur Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

La partie supérieure de la fenêtre contient le nom de l'application installée, sa version, la date d'installation, son état (en exécution ou arrêtée sur le périphérique mobile) et l'état des bases de Kaspersky Anti-Virus.

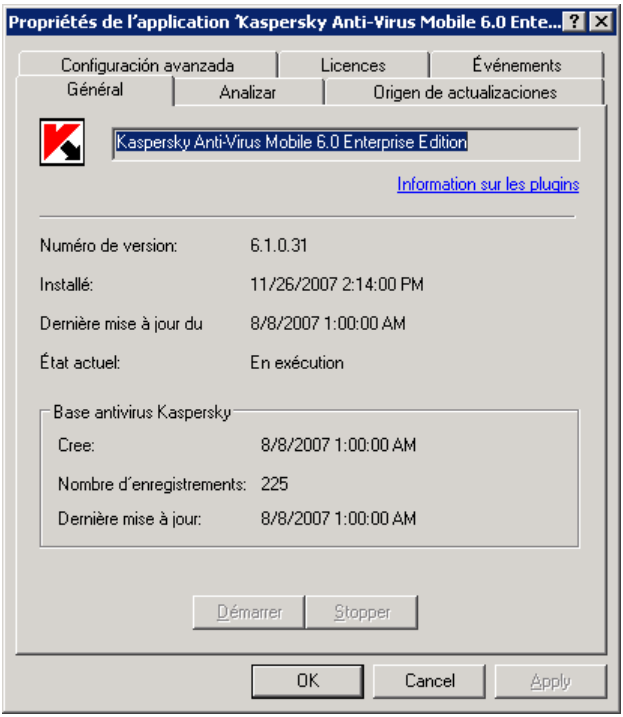

Figure 35. boîte de dialogue des Propriétés de l'application. L'onglet **Général**.

3.2.1.2. Informations sur les paramètres de l'application anti-virus

L'onglet **Analyse** (voir Figure 36) permet d'afficher des informations sur la tâche d'analyse à la demande : couverture de l'analyse, action à réaliser sur les objets et planification de son exécution. Cet onglet indique également si la protection en temps réel est activée sur le périphérique mobile.

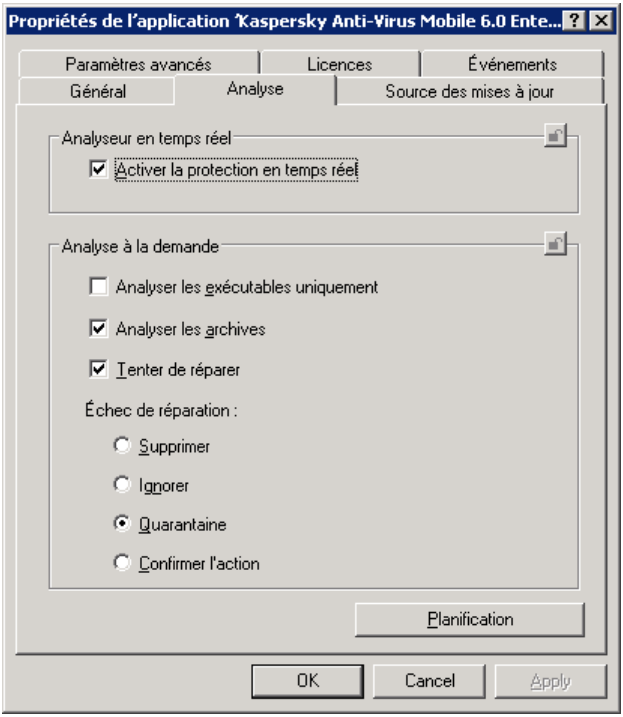

Figure 36. Onglet **Analyser**

3.2.1.3. Informations sur la source de mises à jour

L'onglet **Source des mises à jour** (voir Figure 37) contient des informations sur le serveur configuré en tant que source des mises à jour, ainsi que sur la planification des mises à jour, pour un périphérique mobile en particulier.

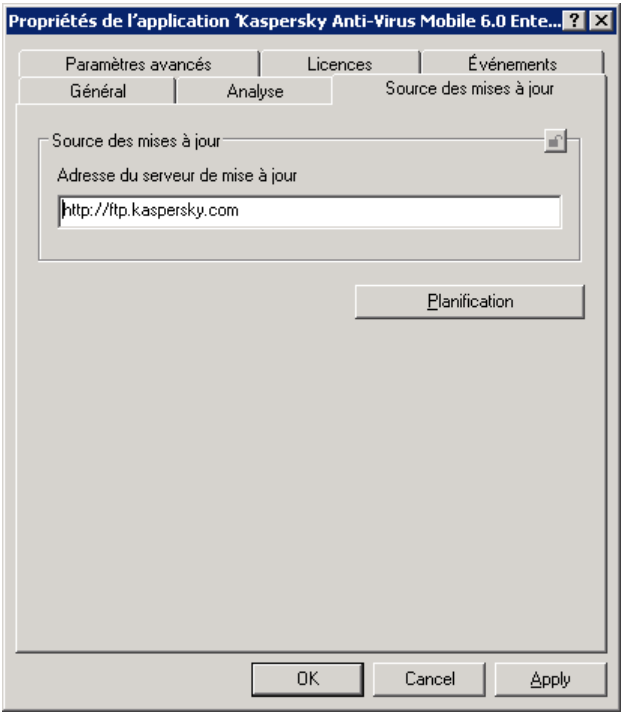

Figure 37. Onglet **Source des mises à jour**

3.2.1.4. Informations sur les paramètres avancés

L'onglet **Paramètres avancés** (voir Figure 38) permet d'obtenir des informations sur le composant Anti-Spam et la fréquence des communications avec le Serveur d'administration.

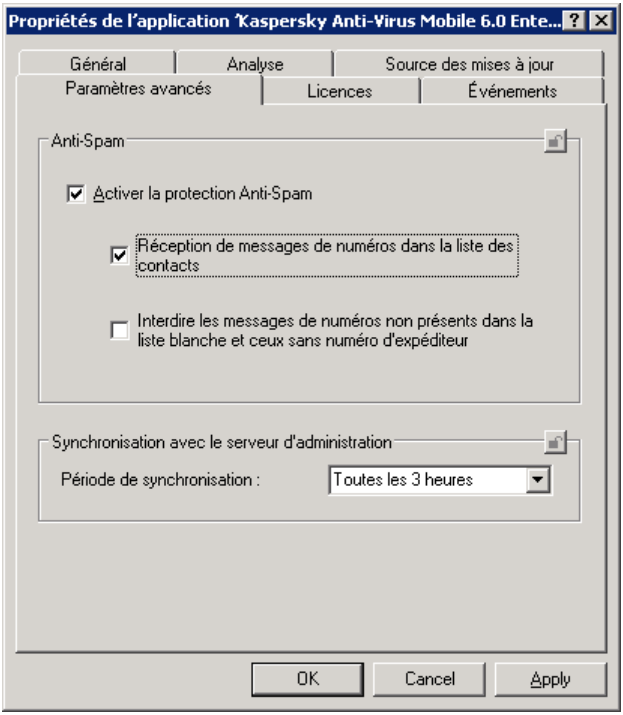

Figure 38. Onglet **Paramètres avancés**

3.2.1.5. Informations sur les clés de licence

L'onglet **Licence** (voir Figure 38) contient des informations sur la clé active ou de réserve installée sur un périphérique mobile en particulier. Il contient également des informations sur la clé courante, la durée et les restrictions de licence. Pour la clé courante, Il contient également des informations sur la clé courante, la date d'activation et celle d'expiration.

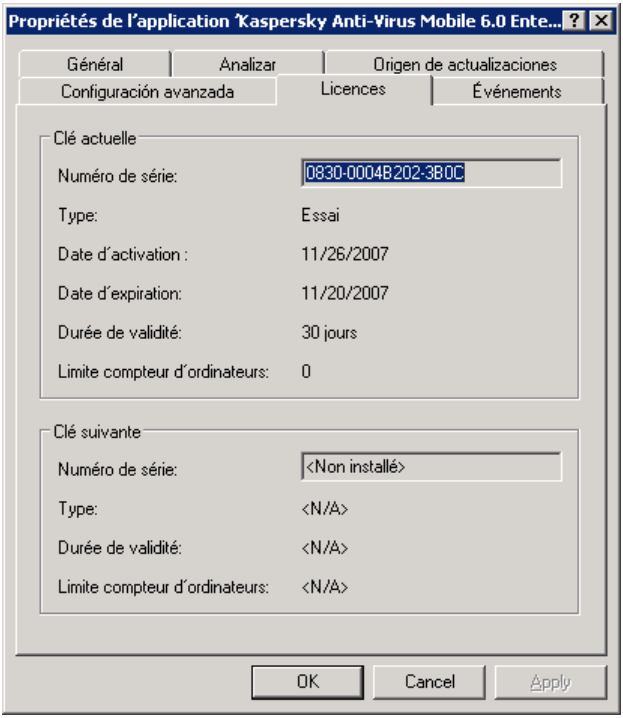

Figure 39. Onglet **Licences**

3.2.1.6. Informations sur les événements

Pendant son fonctionnement, Kaspersky Anti-Virus génère un certain nombre d'événements. Chaque événement possède une caractéristique qui reflète son niveau d'importance. Il existe quatre niveaux d'importance : événement critique, échec, avertissement et message d'information.

Des événements de même type peuvent avoir différents degrés d'importance, en fonction du moment où l'événement s'est produit.

L'onglet **Événements** (voir Figure 40) affiche les types d'événements générés par le fonctionnement de l'application et qui sont enregistrés dans le rapport, ainsi que l'emplacement disque du rapport et le mode de notification de l'administrateur ou des autres utilisateurs.

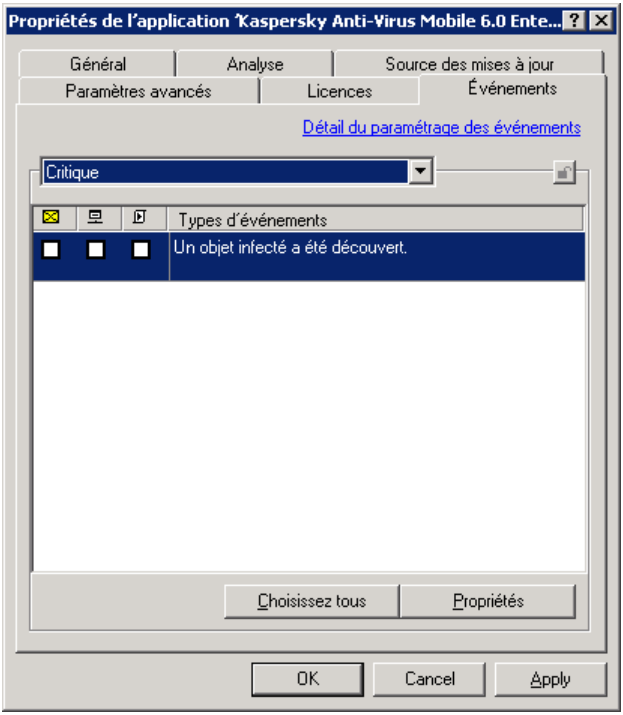

Figure 40. Onglet **Événements**

ANNEXE A. KASPERSKY LAB

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

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

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

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

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

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

A.1. Autres produits antivirus

Kaspersky Lab News Agent

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

News Agent permet également de:

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

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

Kaspersky® OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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

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

Kaspersky® Anti-Virus 7.0

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

Le programme assure une analyse antivirus sophistiquée, notamment :

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

La défense proactive permet de :

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

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

Kaspersky® Internet Security 7.0

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

Les fonctions antivirus proposées sont les suivantes :

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

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte

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

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

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

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

Kaspersky Anti-Virus for File servers

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

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

Avantages et fonctions :

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

Kaspersky Open Space Security

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

Cette application est composée de quatre logiciels :

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

Voici une description détaillée de chacun d'entre eux.

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

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable.* ;
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Blocage des fenêtres pop up et des bannières publicitaires* pendant la navigation sur Internet ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Outils de création d'un disque de démarrage* capable de restaurer le système après une attaque de virus ;
- *Système développé de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables* (technologie Intel® Centrino® Duo pour ordinateurs portables) ;

- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™).

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

Avantages et fonctions :

- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet* ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Répartition de la charge entre les processeurs du serveur* ;
- *Isolement des objets suspects* du poste de travail dans un répertoire spécial ;
- *Annulation des modifications malveillantes dans le système* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;
- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Protection lors de l'utilisation des réseaux sans fil* Wi-Fi ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Mise à jour automatique des bases*.

Kaspersky Enterprise Space Security

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

Avantages et fonctions :

- *Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers* ;
- *Protection des serveurs de messagerie Sendmail, Qmail, Posftix et Exim* ;
- *Analyse de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Prévention des épidémies de virus et des diffusions massives* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Utilisation sécurisée des réseaux sans fil* Wi-Fi ;
- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes dans le système* ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;

- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

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

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;
- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;
- *Utilisation de la technologie iSwift pour éviter les analyses répétées* dans le cadre du réseau ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;

- *Pare-Feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Travail en toute sécurité dans les réseaux de n'importe quel type*, y compris les réseaux Wi-Fi ;
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable* ;
- *Possibilité de réparation à distance* (technologie Intel® Active Management, composant Intel® vPro™);
- *Annulation des modifications malveillantes dans le système* ;
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants* ;
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits* ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

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

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel* ;
- *Filtrage des messages non sollicités* ;
- *Analyse des messages et des pièces jointes du courrier entrant et sortant* ;
- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange* y compris les dossiers partagés ;

- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino* ;
- *Filtrage des messages* en fonction du type de pièce jointe ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système convivial d'administration* du logiciel ;
- *Prévention des épidémies de virus* ;
- *Surveillance de l'état du système de protection* à l'aide de notifications ;
- *Système de rapports* sur l'activité de l'application ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases*.

Kaspersky Security for Internet Gateway

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

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

Voici quelques-unes de ses fonctions :

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

- *Mise à jour automatique des bases.*

Kaspersky® Anti-Spam

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

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

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

Kaspersky Anti-Virus® for MIMESweeper

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

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

A.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://kb.kaspersky.fr/faq.php
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://kb.kaspersky.fr/hq.php E-mail : info@fr.kaspersky.com

ANNEXE B. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD/DVD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD/DVD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la licence d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 *Utilisation*. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD/DVD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Il est interdit de transmettre le code d'activation et le fichier de clé de licence à un tiers. Le code d'activation et le fichier de clé de licence sont des informations strictement confidentielles.

1.1.7 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. *Assistance technique.*

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

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre

possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel kaspersky en version sur CD/DVD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce

Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. *Limites de Responsabilité.*

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.