KASPERSKY LAB

Kaspersky Mobile Security 7.0 Enterprise Edition

GUIDE DE L'UTILISATEUR

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Guide de l'utilisateur

Téléphone/Télécopie : +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
http://www.kaspersky.com/fr/

Date de révision : Août, 2009

Table des matières

CHAPITRE 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Kaspersky Mobile Security 7.0 Enterprise Edition est prévu pour assurer en la protection en temps réel de périphériques mobiles exploités sous Symbian OS et Microsoft Windows Mobile contre les logiciels malveillants, les messages indésirables et pour assurer les fonctions suivantes :

- **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 (infrarouge, Bluetooth), ainsi que les messages SMS, lors de la synchronisation avec un ordinateur personnel ou du téléchargement de fichiers avec un navigateur ;
  - fichiers ouverts sur le périphérique mobile ;
  - programmes installés dans l'interface du périphérique.
- **analyse des objets du système de fichiers** sur le périphérique mobile ou sur les cartes d'expansion connectées, à la demande de l'utilisateur, ou d'une manière planifiée ;
- **isolement sécurisé des objets infectés** dans la zone de quarantaine ;
- **mise à jour des bases de Kaspersky Mobile Security** utilisées pour l'analyse des logiciels malveillants et suppression des objets dangereux.
- **interdiction des messages SMS indésirables**.
- **verrouillage ou effacement des données utilisateur** en cas d'actions non autorisées avec le périphérique, comme par exemple, en cas de vol.
- **protection des connexions réseau du périphérique mobile**.

L'utilisateur dispose de possibilités de contrôle flexible des paramètres de Kaspersky Mobile Security, et peut afficher l'état courant et le journal des événements dans lequel les actions de l'application sont consignées.

L'application possède un menu système et une interface utilisateur conviviale.

Note

en cas de détection d'un logiciel malveillant, Kaspersky Mobile Security peut réparer les objets infectés (quand la réparation est possible), les supprimer ou les placer en quarantaine. Dans ce cas, aucune copie de l'objet supprimé ne sera conservée.

1.1. Spécifications matérielles et logicielles

Kaspersky Mobile Security peut être installé sur des périphériques mobiles exploitant l'un des systèmes suivants :

- Symbian OS 9.1, 9.2 Séries 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Kit de distribution

Vous pouvez acquérir Kaspersky Mobile Security par Internet (le kit de distribution et la documentation de l'application sont en format numérique). Vous pouvez également acquérir Kaspersky Mobile Security chez des revendeurs de services de communication pour mobiles. Pour plus détails, contactez votre opérateur mobile.

1.3. Installation de Kaspersky Mobile Security

Attention !

La version installée de Kaspersky Mobile Security ne prévoit pas la sauvegarde ou la restauration.

L'application est installée de manière centralisée par le biais de Kaspersky Administration Kit. L'administrateur réseau peut utiliser une des deux méthodes d'installation de l'application suivantes :

- installation avec l'ordinateur de l'utilisateur ;

- installation par le biais d'un message SMS.

Pour plus de détails sur l'installation à distance de l'application, consultez le Guide de l'administrateur de Kaspersky Mobile Security 7.0 Enterprise Edition.

1.3.1. Installation avec l'ordinateur de l'utilisateur

Après la connexion du périphérique mobile avec un ordinateur présent dans le réseau logique du Serveur d'administration, la fenêtre de l'utilitaire *kmlisten.exe* s'ouvre (Figure 1). Cet outil est prévu pour assurer l'installation of Kaspersky Mobile Security 7.0 Enterprise Edition sur un périphérique mobile.

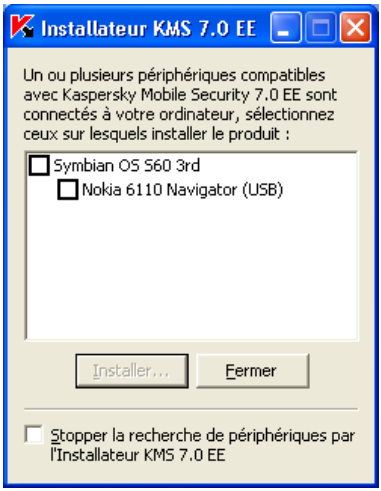

Figure 1. Utilitaire **Kmlisten**

Pour installer Kaspersky Mobile Security, procédez de la manière suivante :

dans fenêtre de l'utilitaire *kmlisten.exe*, cochez la case associée au nom du périphérique sur lequel installer l'application, puis cliquez sur **Installer**. Le kit de distribution pour l'installation de l'application est recopié dans votre périphérique mobile puis exécuté.

1.3.2. Installation par le biais d'un message SMS

Pour installer l'application, l'administrateur réseau peut utiliser le service d'installation para le biais d'un message SMS (pour plus de détails, consultez le Guide de l'administrateur de Kaspersky Mobile Security 7.0 Enterprise Edition). Un message SMS contenant le lien URL du serveur hébergeant le kit d'installation de l'application est envoyé au périphérique mobile.

Pour installer l'application par le biais d'un message SMS, procédez de la manière suivante :

1. Ouvrez un SMS contenant le lien URL du serveur d'où il est possible de télécharger le paquet d'installation de Kaspersky Mobile Security.
2. Utilisez le lien contenu dans le texte du message pour télécharger le kit d'installation de l'application sur le périphérique.
3. Enregistrez le kit d'installation de l'application.

Le processus d'installation de l'application démarre automatiquement.

1.4. Activation de l'application

Note

L'activation de l'application est obligatoire. Dans le cas contraire, les fonctions de l'application ne seront pas disponibles.

L'activation of Kaspersky Mobile Security 7.0 Enterprise Edition se produit lors de la synchronisation avec le Serveur d'administration. Pendant la synchronisation, le fichier clé utilisé est celui spécifié lors de la création de la stratégie de sécurité pour périphériques mobiles (pour plus d'informations sur les stratégies de Kaspersky Administration Kit pour périphériques mobiles, consultez le Guide de l'administrateur de Kaspersky Mobile Security 7.0 Enterprise Edition).

Le processus de synchronisation de l'application avec le serveur d'administration démarre automatiquement dans l'intervalle spécifié para la stratégie pour les périphériques mobiles. Vous pouvez également démarrer le processus de synchronisation manuellement (section 2.1.9 à la page 34 ou section 3.6 à la page 58).

Note

Lors de la création de la stratégie, toute possibilité de modification du fichier clé du périphérique doit être interdite. Dans le cas contraire, le périphérique ne sera pas activé lors de la synchronisation avec le Serveur d'administration.

CHAPITRE 2. KASPERSKY MOBILE SECURITY POUR SYMBIAN OS

Ce chapitre décrit le fonctionnement de Kaspersky Mobile Security 7.0 sur des modèles périphérique exploités sous Symbian version 9.1, 9.2 ou Séries 60 UI.

2.1. Utilisation de l'application

Cette section décrit la configuration de l'analyse anti-virus et de la protection en temps réel, le filtrage des messages SMS, l'analyse antivirus du périphérique, les mises à jour des bases de l'application, la configuration de l'application, la protection du périphérique sur le réseau, etc.

2.1.1. Lancement de l'application

Pour lancer Kaspersky Mobile Security, procédez de la manière suivante :

1. Ouvrez le menu principal du périphérique.
2. Sélectionnez **KMS 7.0 EE** puis lancez l'application avec la commande **Ouvrir** du menu **Options**.

Après le démarrage du périphérique, une fenêtre avec les principaux composants de Kaspersky Mobile Security (Figure 2) sera affichée sur l'écran du périphérique.

- **Protection** – utilisation du mode de protection en temps réel (section 2.1.4 à la page 13) ;
- **Dernière analyse** – date et heure de la dernière analyse anti-virus du périphérique.
- **Date de la base** – date de publication de la base utilisée par l'application.
- **Anti-Spam** – Mode de fonctionnement du module Anti-Spam (section 2.1.6 à la page 22).
- **Niveau du Pare-feu** – protection du périphérique sur le réseau (section 2.1.9 à la page 34).

Figure 2. Fenêtre d'état des composants de l'application

Pour revenir à l'interface de l'application, appuyez sur **OK**.

2.1.2. Interface graphique utilisateur

L'interface graphique contient six onglets :

- L'onglet **Analyse** permet d'effectuer une analyse antivirus du périphérique, de modifier les paramètres de l'analyse antivirus, de la protection en temps réel et de la quarantaine, ainsi que planifier des analyses automatiques.
- L'onglet **Mise à jour** permet de mettre à jour la base antivirus, de configurer et de planifier la mise à jour.
- L'onglet **Pare-feu** permet de surveiller l'activité réseau et de protéger le périphérique sur le réseau.
- L'onglet **Antivol** permet de verrouiller le périphérique et d'en effacer les informations en cas de vol ou de perte (module Antivol).
- L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS entrants (module Anti-Spam).
- L'onglet **Information** permet d'afficher les rapports d'activité des composants de l'application ;des informations générales sur l'application et la base antivirus utilisée, ainsi que de modifier les paramètres généraux de l'application.

Pour vous déplacer d'un onglet à l'autre, utilisez le joystick du périphérique ou sélectionnez **Ouvrir page** dans le menu **Options** (Figure 3).

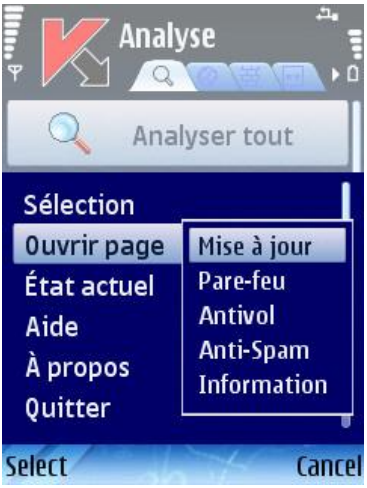

Figure 3. Le menu **Options**

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

2.1.3. Paramètres généraux

Les paramètres de l'onglet **Information** sous l'entrée **Paramètres** (Figure 4) permettent de configurer les fonctions suivantes de l'application :

- **Voir écran d'état** : détermine si l'état actuel de Kaspersky Mobile Security est affiché au lancement de l'application.
- **Taille rapport** : définit la taille maximum du rapport. Quand la limite maximum est atteinte, les enregistrements les plus anciens sont supprimés pour revenir à la limite inférieure spécifiée.
- **Rétro-éclairage** : indique si l'écran doit être éclairé pendant l'analyse antivirus. L'option de rétro-éclairage est désactivée par défaut.
- **Activer le son** : détermine l'utilisation d'alertes sonores avec certains événements (détection d'objets infectés, message concernant l'état de l'application, etc.). Par défaut, l'utilisation du son en cas de détection d'un virus dépend du profil du périphérique (valeur **Dépendant du profil**). Sélectionnez **En cours** pour utiliser le signal sonore, sans tenir compte du profil sélectionné sur le périphérique.

- **Volume du son** : détermine le volume du son en cas de détection d'un objet infecté.
- **Vibration** : indique si le périphérique doit vibrer quand l'infection d'un objet est détectée. Par défaut la vibration est activée.

Figure 4. Le menu **Paramètres**

Pour modifier les valeurs des paramètres, utilisez le joystick de votre périphérique ou sélectionnez **Modifier** dans le menu **Options**.

2.1.4. Analyse et protection antivirus

L'onglet **Analyse** permet d'effectuer l'analyse anti-virus complète du système de fichiers et de la mémoire du périphérique, ou seulement d'un dossier ou d'un fichier. Vous pouvez également modifier la configuration de l'analyse anti-virus et du mode de protection en temps réel, afficher un rapport avec les résultats de l'analyse, ou planifier l'exécution automatique de l'analyse.

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

Dans le mode de protection en temps réel, une partie résidente de Kaspersky Mobile Security reste chargée dans la mémoire RAM afin de surveiller toutes les données, y compris les données reçues par le périphérique.

Le mode de protection en temps réel démarre avec la mise sous tension du périphérique et reste en fonctionnement jusqu'à sa mise hors-tension (à moins que ce mode ne soit désactivé par configuration).

Kaspersky Mobile Security permet également de faire une analyse complète du système de fichiers du périphérique, y compris des objets situés sur les cartes d'expansion de la mémoire connectées.

Les résultats d'activité de la protection en temps réel et de l'analyse à la demande sont consignés dans un rapport. Pour afficher le rapport, sélectionnez l'entrée **Rapports** dans l'onglet **Analyse**.

Pour démarrer la protection en temps réel, procédez de la manière suivante :

1. Sélectionnez **Paramètres** dans l'onglet **Analyse**.
2. Sélectionnez l'entrée **Protection en temps réel** dans la section **Paramètres**.
3. Activez ou désactivez le mode de protection en temps réel en définissant la valeur correspondante du paramètre **Protection**.

Pour modifier les paramètres de protection en temps réel, procédez de la manière suivante :

1. Sélectionnez **Paramètres** dans l'onglet **Analyse**.
2. Sélectionnez l'entrée **Protection en temps réel** dans la section **Paramètres**.
3. Spécifiez la couverture de l'analyse dans la section **Masque** en sélectionnant les types de fichier à analyser :
   - **Tous les fichiers** – analyse tous les fichiers.
   - **Exécutables seuls** – analyse uniquement les fichiers d'application exécutables (par exemple : *.exe, *.sis, *.mdl, *.app).
4. Sélectionnez l'action qui sera exécutée lors de la découverte d'un objet infecté (paramètre **Action en cas de virus**).

   Par défaut, les objets malveillants découverts sont placés en quarantaine (valeur **Quarantaine** du paramètre).

   Pour s'assurer que les informations sur la détection d'un objet infecté sont consignées dans le rapport de l'application, choisissez la valeur **Consigner**.

   Pour que l'application supprime les objets malveillants découverts sans demander confirmation à l'utilisateur, sélectionnez **Suppression auto**.
5. Activez ou désactivez la fonction d'analyse des nouvelles cartes (paramètre **Analyser carte**).

Par défaut, chaque fois qu'une nouvelle carte mémoire est connectée, l'application informe l'utilisateur qu'elle doit être analysée.

Pour activer l'analyse des cartes flash connectées au périphérique, sélectionnez la valeur **Analyse auto**. Pour désactiver l'analyse automatique des cartes de mémoire flash, choisissez **Désactiver**.

6. Activez ou désactivez l'affichage de l'icône de protection (paramètre **Afficher l'icône dy KMS**).

   Sélectionnez **Toujours** dans le menu si vous souhaitez afficher en permanence l'icône de l'application sur l'écran du périphérique quand la protection en temps réel est activée. Si vous souhaitez afficher l'icône uniquement dans le menu du périphérique, sélectionnez **Menu uniquement**. Si vous ne souhaitez pas afficher cette icône, choisissez **Arrêté**.

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

1. Sélectionnez **Paramètres** dans l'onglet **Analyse**.
2. Sélectionnez l'entrée **Paramètres d'analyse** dans la section **Paramètres**.
3. Spécifiez la couverture de l'analyse dans la section **Masque** en sélectionnant les types de fichier à analyser :

   - **Tous les fichiers** – analyse tous les fichiers.
   - **Exécutables seuls** – analyse uniquement les fichiers d'application exécutables (par exemple : *.exe, *.sis, *.mdl, *.app).

4. Sélectionnez l'action qui sera exécutée lors de la découverte d'un objet infecté (paramètre **Action en cas de virus**).

   Par défaut, l'application tente de désinfecter les objets malveillants découverts (valeur **Tenter de réparer** du paramètre).

   Pour déplacer les objets malveillants en quarantaine, sélectionnez la valeur **Quarantaine**.

   Pour s'assurer que les informations sur la détection d'un objet infecté sont consignées dans le rapport de l'application, choisissez la valeur **Consigner**.

   Pour que l'application supprime les objets malveillants découverts sans demander confirmation à l'utilisateur, sélectionnez **Suppression auto**.

   Pour s'assurer qu'une confirmation de l'action est présentée à l'utilisateur en cas de découverte d'un objet infecté, sélectionnez **Demander**.

5. Spécifiez l'action exécutée si la réparation d'un objet infecté est impossible (paramètre **Echec de réparation**).

   Par défaut, les objets malveillants découverts sont placés en quarantaine (valeur **Quarantaine** du paramètre).

   Pour s'assurer que les informations sur la détection d'un objet infecté sont consignées dans le rapport de l'application, choisissez la valeur **Consigner**.

   Pour que l'application supprime les objets malveillants découverts sans demander confirmation à l'utilisateur, sélectionnez **Suppression auto**.

   Pour s'assurer qu'une confirmation de l'action est présentée à l'utilisateur en cas de découverte d'un objet infecté, sélectionnez **Demander**.

6. Activer / Désactiver l'analyse de la mémoire ROM du périphérique (paramètre **Analyser ROM**).

   Sous certaines circonstances, la mémoire ROM peut devenir vulnérable aux logiciels malveillants. Pour activer l'analyse de la ROM, choisissez **Oui**.

7. Activer / Désactiver la décompression des archives SIS et ZIP (paramètre **Décompresser archives**).

   Si vous souhaitez que l'application décomprime les archives SIS et ZIP, sélectionnez **Oui**. S'il n'est pas nécessaire de décomprimer les archives pendant l'analyse, choisissez **Non**.

Note

Pour modifier les valeurs des paramètres, utilisez le joystick de votre périphérique ou sélectionnez **Modifier** dans le menu **Options**.

Par défaut, l'application utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer la configuration recommandée, dans l'onglet **Analyse** sélectionnez **Par défaut** dans le menu **Options**.

Pour lancer une analyse antivirus, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).
2. Dans l'onglet **Analyse** (Figure 5) sélectionnez **Analyser tout** si vous souhaitez analyser le système de fichiers complet de votre périphérique, ou **Analyser dossier** pour analyser un dossier individuel.

Figure 5. Onglet **Analyser**

Quand l'option **Analyser dossier** est sélectionnée, une fenêtre présente alors le système de fichiers du périphérique. Utilisez les boutons du joystick pour vous déplacer dans le système de fichiers de votre périphérique. Pour analyser un dossier, positionnez le curseur sur le répertoire que vous souhaitez analyser et sélectionnez **Sélection** dans le menu **Options**.

Après le démarrage de l'analyse, une fenêtre affiche l'état courant de la tâche : nombre d'objets analysés, chemin de l'objet en cours d'analyse et une barre progression avec le pourcentage d'objets analysés (Figure 6).

Figure 6. Fenêtre **Progression de l'analyse**

Quand un objet infecté est découvert, l'action spécifiée par **Paramètres** → **Paramètres d'analyse** est exécuté.

Figure 7. Notification de détection de virus

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

Pour désactiver le rétro-éclairage pendant l'analyse,

ouvrez l'onglet **Information**, et dans le menu **Paramètres**, choisissez la valeur **Oui** du paramètre **Rétro-éclairage**.

Par défaut, le rétro-éclairage est automatiquement désactivé pour économiser les batteries.

2.1.4.2. Planification de l'analyse

Kaspersky Mobile Security permet de planifier des analyses automatiques du périphérique. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, l'action définie par les paramètres d'analyse sera exécutée sur cet objet (section 2.1.4.1 à la page 13).

Par défaut, la planification est désactivée.

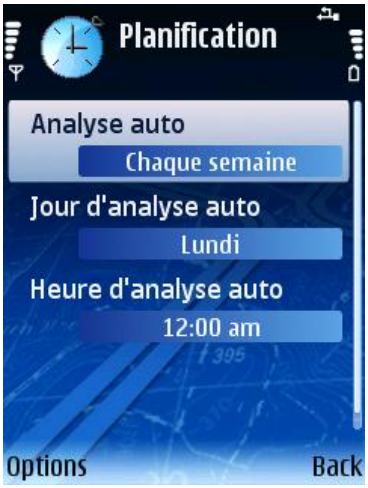

Figure 8. Le menu **Planification**

Pour planifier l'exécution de la tâche :

sélectionnez **Planification** dans l'onglet **Analyse** et configurez les paramètres **Analyse auto** (Figure 8) :

- **Chaque jour** – l'analyse s'exécutera tous les jours. Spécifiez l'**Heure d'analyse auto.** dans le champ de saisie.
- **Chaque semaine** – l'analyse s'exécutera une fois par semaine. Spécifiez le **Jour d'analyse auto** et l'**Heure d'analyse auto**.

2.1.5. Utilisation de la quarantaine

Les objets infectés placés en quarantaine ne supposent aucune menace pour le périphérique et peuvent être supprimés ou restaurés par la suite.

L'application peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

If vous souhaitez que l'application déplace les objets malveillants détectés vers la quarantaine sans demander confirmation, procédez de la manière suivante :

1. Ouvrez l'onglet **Analyse**.
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Paramètres d'analyse** ou **Paramètres en temps réel**.
4. Choisissez **Quarantaine** comme valeur du paramètre **Action en cas de virus**.

Si vous avez choisi **Demander** lors de la détection d'un objet infecté, Kaspersky Mobile Security vous proposera son effacement ou son déplacement en quarantaine.

Pour afficher la liste des objets en quarantaine,

ouvrez l'onglet **Analyse** et sélectionnez **Quarantaine** (Figure 9).

Figure 9. Nombre d'objets infectés en quarantaine

Le menu **Options** de la fenêtre Quarantaine permet de :

- Afficher le détail de n'importe quel objet conservé en quarantaine (**Afficher détails**).
- Supprimer l'objet sélectionné (**Supprimer fichier**).
- Effacer tous les objets de la quarantaine (**Supprimer tout**).
- Restaurer l'objet courant en quarantaine dans son dossier d'origine (**Restaurer fichier**).
- Afficher l'aide de la Quarantaine (**Aide**).

Pour configurer la quarantaine :

1. Ouvrez l'onglet **Analyse**.
2. Sélectionnez **Paramètres**.
3. Sélectionnez l'onglet **Quarantaine** (Figure 10).

Figure 10. Paramètres de quarantaine

Le paramètre **Taille de la quarantaine** définit le nombre maximum d'objets infectés pouvant être conservés en quarantaine. Les valeurs possibles sont **20**, **50** ou **100** fichiers.

Le paramètre **Limite de conservation** détermine la durée de conservation des objets infectés dans la quarantaine. Après cette période, les objets infectés sont automatiquement supprimés.

Note

Pour restaurer la configuration de quarantaine recommandée par les spécialistes de Kaspersky Lab, sélectionnez **Par défaut** dans le menu **Options**.

2.1.6. Utilisation du module Anti-Spam

Le module Anti-Spam est prévu pour protéger en temps réel votre périphérique contre les messages SMS indésirables.

Le filtrage fait appel aux listes dites « noire » et « blanche ». Ces listes contiennent des téléphones et des échantillons de frases caractéristiques des messages normaux ou indésirables. La séquence d'analyse du message est la suivante :

- vérifier si le numéro est présent dans la liste noire ;
- vérifier si le numéro de l'expéditeur est présent dans la liste blanche ;
- analyser la présence dans le texte du message de frases de la liste noire ;
- analyser la présence dans le texte du message de frases de la liste noire ;

si une correspondance est détectée, l'analyse est interrompue. Le message contenant un élément de la liste noire est interdit. Le message contenant un élément de la liste blanche est autorisé.

2.1.6.1. Modes de fonctionnement Anti-Spam

Le module Anti-Spam filtre les messages dans l'un des modes suivants :

- **Activé.** Dans ce mode, le module Anti-Spam filtre les messages entrants en fonction des listes noire et blanche uniquement. Quand un message est envoyé par un numéro qui ne figure dans aucune de ces listes, le module Anti-Spam affiche un message proposant d'interdire ou d'autoriser la réception du message et d'ajouter le numéro de téléphone à la liste blanche ou noire.
- **Liste noire.** Dans ce mode, le module Anti-Spam interdit les messages appartenant à la liste noire. Tous les autres messages sont remis.
- **Liste blanche.** Dans ce mode, le module Anti-Spam laisse passer les messages appartenant à la liste blanche. Tous les autres messages sont interdits.

- **Désactivé.** Le composant anti-spam est désactivé dans ce mode. Aucun filtrage des messages entrants n'est assuré.

Pour sélectionner le mode de fonctionnement du module Anti-Spam :

1. Ouvrez l'onglet **Anti-Spam**.
2. Sélectionnez **Paramètres**.
3. Définissez le mode de fonctionnement avec **Config. Anti-Spam**.

2.1.6.2. Modification des listes noire et blanche

Les enregistrements dans les **listes « noire »** et **« blanche »** contiennent des numéros de téléphone des SMS qui seront interdits ou autorisés par le module Anti-Spam. Des informations sur les messages interdits ou supprimés sont consignées dans le rapport.

Note

Les messages qui ne sont présents dans aucune des listes ne seront pas interdits.

Pour valider les modifications aux listes noire ou blanche,

ouvrez l'onglet **Anti-Spam** et choisissez l'entrée correspondante (Figure 11).

Pour modifier la liste utilisez le menu **Options** :

- **Ajouter/enregister** – ajoute un nouvel enregistrement à la liste.
- **Modif. enregistrement** – modifie l'enregistrement sélectionné.
- **Suppr. enregistrement** – supprime l'enregistrement de la liste.
- **Supprimer tout** – efface la liste en supprimant tous les enregistrements.
- **Aide** – affiche l'aide sur la gestion de la liste.

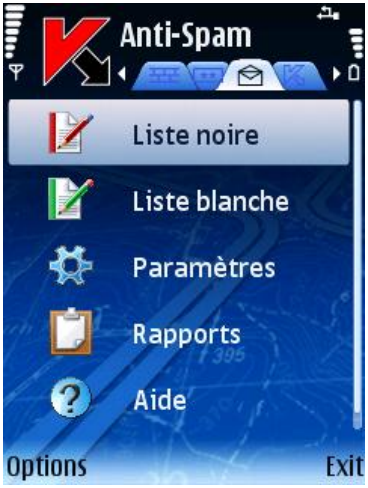

Figure 11. L'onglet **Anti-Spam**

- Si vous sélectionnez **Ajouter/enregistrer** ou **Modif. enregistrement**, vous devez spécifier les paramètres suivants de l'enregistrement (Figure 12)
- **Numéro de téléphone**. Spécifie le numéro de téléphone d'où proviennent les messages à interdire ou à autoriser. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ».
- **Texte**. Spécifiez le texte qui, lorsqu'il est détecté dans un message, permet d'interdire ou d'autoriser le message.

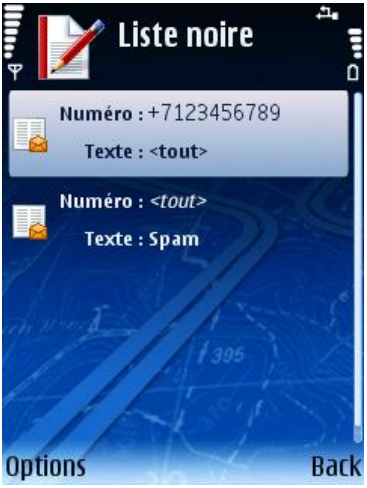

Figure 12. La liste noire

2.1.6.3. Paramètres de la fonction Anti-Spam

Pour modifier la configuration du module Anti-Spam :

ouvrez l'onglet **Anti-Spam** et choisissez l'entrée **Paramètres** (Figure 13).

Figure 13. Paramètres Anti-Spam

Les paramètres Anti-Spam suivants sont disponibles dans le menu **Paramètres** :

- **Config. Anti-Spam** – mode de fonctionnement du module Anti-Spam (section 2.1.6.1 à la page 22).
- **Autoriser contacts**. Si le paramètre est défini à **Oui**, le module Anti-Spam n'interdira pas la réception de messages provenant de numéros de téléphone inclus dans votre répertoire. Si cette option est désactivée (valeur **Non**), le module Anti-Spam filtre le numéro en fonction de sa présence dans la liste noire ou blanche.
- **Ajouter sortants**. Si le paramètre est défini à **Oui**, tous les numéros que vous utilisez pour envoyer des messages SMS seront automatiquement ajoutés à la liste blanche. Sélectionnez **Non** pour désactiver cette option.
- **Interdire non numériques.** Si le paramètre est défini à **Non**, le module Anti-Spam n'interdira pas les messages entrants provenant de numéros de téléphone sans numéro. Choisissez **Oui** pour activer l'option.

> **Note**
>
> Ce paramètre affectera les enregistrements créés par le module Anti-Spam dans l'un des cas suivants :
>
> - L'ajout de numéros sortants à la liste blanche (l'option **Ajouter sortants** est activée) ;
> - L'ajout de nouveaux numéros de téléphone d'où proviennent les messages, à l'une des listes (section 2.1.6.4 à la page 26).

Pour modifier les valeurs des paramètres, utilisez le joystick de votre périphérique ou sélectionnez **Modifier** dans le menu **Options**.

2.1.6.4. Actions appliquées aux messages

Quand vous recevez un message SMS ou MMS envoyé par un numéro qui ne figure dans votre liste noire ou blanche, le module Anti-Spam intercepte le message et affiche un avertissement sur l'écran du périphérique (Figure 14)

Dans le menu **Options**, choisissez l'une des actions suivantes à appliquer au 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** – interdit la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.

- **Ignorer** – autorise la réception du message. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Des informations sur les messages bloqués sont consignées dans le rapport de l'application. Pour afficher le rapport, Sélectionnez **Rapports** dans l'onglet **Anti-Spam**.

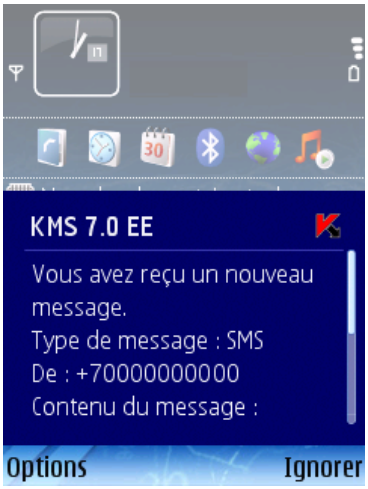

Figure 14. Avertissement du module Anti-Spam

2.1.7. Utilisation du module Antivol

Le module Antivol module est prévu pour garantir la protection des données conservées dans le périphérique mobile, contre un accès non autorisé en cas de perte ou de vol.

La première fois que vous accéder aux paramètres du module, vous devez définir un code. Par la suite, ce code donne accès aux paramètres du module afin de pouvoir les modifier. **Verrouillage** – permet de verrouiller le périphérique à la demande de l'utilisateur. Le périphérique ne pourra être déverrouillé qu'après avoir entré le code d'accès au module Antivol. Pour déverrouiller le périphérique avec la fonction Verrouillage, envoyez un message SMS avec le texte : "`block:code`" au périphérique. La fonction Verrouillage est désactivée. Pour activer la fonction, sélectionnez **Arrêté**.

La fonction **Suppression** permet d'effacer les données personnelles de l'utilisateur (contacts, messages, fichiers, données sur la carte mémoire, paramètres de connexion réseau). Pour activer la fonction Suppression, envoyez

un message SMS avec le texte "clean:code" au périphérique. La fonction Suppression est désactivée. Pour activer la fonction, sélectionnez **Arrêté**.

SIM-Surveillance – permet, quand la carte SIM est remplacée dans le périphérique, d'envoyer aux numéros spécifiés le nouveau numéro du téléphone et de verrouiller le périphérique volé. Pour activer la fonction, sélectionnez **Arrêté**.

Si un changement de code est nécessaire afin de travailler avec le module Antivol, sélectionnez **Modifier le mot de passe**. Entrez et confirmez le nouveau code puis cliquez sur **OK**.

Chaque fois que vous accédez à la configuration du module Antivol (Figure 14) vous devez saisir le code défini précédemment.

Figure 15. Onglet **Antivol**

Des informations sur l'activité du module seront consignées dans le rapport de l'application. Pour afficher le rapport, Sélectionnez **Rapports** dans l'onglet **Antivol**.

2.1.7.1. Section Suppression

Pour configurer la fonction Suppression :

1. Ouvrez l'onglet **Antivol** et saisissez le code (section 2.1.7 à la page 27).
2. Sélectionnez **Paramètres**.
3. Sélectionnez **Suppression**.

La section **Suppression** présente la liste des données qui pourront être supprimées en cas de perte ou de vol du périphérique (Figure 16).

Figure 16. Onglet **Suppression**

Si vous souhaitez supprimer votre carnet de téléphones aussitôt après la perte ou le vol de votre périphérique mobile, sélectionnez **Supprimer les contacts** et définissez sa valeur à **Oui**.

Note

Les contacts effacés sont uniquement ceux du périphérique. Le carnet de la carte SIM n'est pas effacé.

Pour supprimer les messages de courrier et les messages SMS (dossiers Boîte de réception et de messagerie) sélectionnez **Nett. la boîte de récept.** et définissez sa valeur à **Oui**.

L'option **Supprimer les fichiers** se charge de la suppression des données personnelles (données du dossier C:\Data\). Par défaut, la suppression des fichiers personnels n'est pas activée. Si vous souhaitez supprimer votre carnet de téléphones en cas de perte ou de vol de votre périphérique, sélectionnez cette entrée et définissez sa valeur à **Oui**.

Sélectionnez **Suppr. les fich. sur carte** pour effacer la carte mémoire du périphérique perdu. Cette fonction est désactivée par défaut. Pour activer l'effacement des données de la carte mémoire, sélectionnez **Suppr. les fich. sur carte** et sélectionnez la valeur **Oui**.

Pour activer la suppression des paramètres de connexion réseau, sélectionnez **Supp. les param.réseau** et choisissez la valeur **Oui**.

Cliquez sur **OK** pour enregistrer les modifications.

2.1.7.2. Paramètres SIM-Surveillance

Pour configurer la fonction SIM-Surveillance, ouvrez l'onglet **Antivol**. Entrez le code (section 0 à la page 27) puis sélectionnez **SIM-Surveillance** dans la fenêtre ouverte.

La fonction **SIM-Surveillance** permet de contrôler le remplacement de la carte SIM dans le périphérique (Figure 17).

Figure 17. Onglet **SIM-Surveillance**

Utilisez les champs **Numéro de téléphone 1** et **Numéro de téléphone 2** pour indiquer les numéros destinataires du nouveau numéro de téléphone en cas de remplacement de la carte SIM de votre périphérique. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.

Vous pouvez également verrouiller le périphérique si la carte SIM est remplacée. Pour ce faire, sélectionnez **Bloquer le périphérique** et définissez sa valeur à **Oui**. Le périphérique ne pourra être déverrouillé qu'après avoir entré le code d'accès au module Antivol. Par défaut, le verrouillage du périphérique n'est pas activé.

Cliquez sur **OK** pour enregistrer vos modifications.

2.1.8. Mise à jour des bases de l'application

La détection de logiciels malveillants fait appel aux enregistrements des bases de l'application, contenant les descriptions de tous les logiciels malveillants connus jusqu'à cette date. Il est extrêmement important d'assurer la mise à jour des bases.

Leur mise à jour peut se faire manuellement ou de manière planifiée. Les mises à jour sont téléchargées depuis les serveurs de Kaspersky Lab.

Vous pouvez lancer l'analyse antivirus automatique de votre périphérique après chaque mise à jour des bases de Kaspersky Mobile Security. Pour ce faire, sélectionnez **Paramètres** dans l'onglet **Mise à jour** et **Arrêté** le paramètre **Analyser après la MAJ**.

La valeur du paramètre **Analyser Quar. après MAJ** détermine si les objets en quarantaine seront de nouveau analysés après chaque mise à jour des bases de l'application. Par défaut, l'analyse est exécutée. Si vous ne souhaitez pas effectuer l'analyse, choisissez **Marche**.

Si nécessaire, pour changer de point d'accès actif, utilisez le paramètre **Point d'accès**. Puis sélectionnez la valeur requise dans la liste. Par défaut, le point d'accès est le point d'accès prédéfini dans le périphérique.

Le paramètre **Serveur de mise à jour** définit la source de mise à jour des bases de l'application : serveurs de mise à jour de Kaspersky Lab (valeur **Par défaut**) ou serveur spécifié par l'utilisateur (valeur **Personnalisé**). Si vous avez choisi l'option **Personnalisé** indiquez le lien URL dans la fenêtre ouverte. Si nécessaire, vous pouvez spécifier un serveur de mise à jour alternatif.

Vous pouvez visualiser des informations détaillées sur les bases utilisées dans la zone **Infos des bases** de l'onglet **Information**.

Des informations sur la mise à jour des bases seront consignées dans le rapport. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Mise à jour**.

2.1.8.1. Paramètres de mise à jour

Pour configurer de mises à jour des bases d'application, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).
2. Ouvrez l'onglet **Paramètres** dans l'onglet **Mise à jour** (Figure 18).

Figure 18. Onglet **Mise à jour**

3. Sélectionnez le point d'accès (paramètre **Point d'accès**) (Figure 19).

> **Note**
>
> La configuration du point d'accès utilise les informations de votre fournisseur de services mobiles.

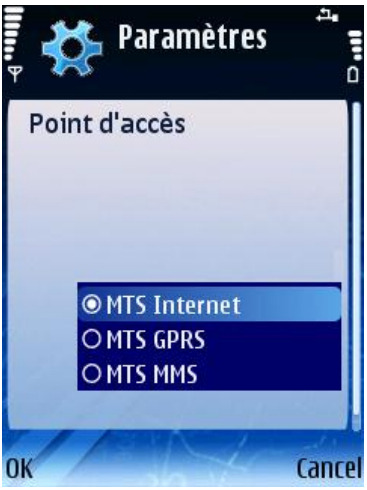

Figure 19. Sélection du point d'accès

4. Entrez l'adresse du serveur de mise à jour (si nécessaire). Pour ce faire, sélectionnez **Serveur de mise à jour** puis choisissez la valeur **Personnalisé**. Entrez le lien URL de la source de mise à jour dans la fenêtre ouverte (Figure 20).

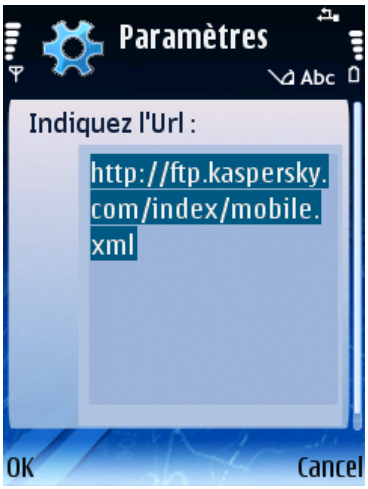

Figure 20. Adresse du serveur de mise à jour

Par défaut, les mises à jour sont téléchargées depuis le serveur de Kaspersky Lab : http://ftp.kaspersky.com/index/mobile.xml.

Remarque :

La mise à jour sera suivie par la déconnexion, même si la connexion était déjà établie.

2.1.8.2. Mise à jour manuelle

Pour lancer une mise à jour manuelle des bases antivirus :

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).
2. Sélectionnez **Mettre à jour** dans l'onglet **Mise à jour** (Figure 18)

2.1.8.3. Mise à jour planifiée

Pour une mise à jour automatique des bases d'application.

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).

2. Sélectionnez **Planification** dans l'onglet **Mise à jour** et configurez les paramètres **Mise à jour auto** :

   - **Arrêté** – ne pas exécuter de mises à jour planifiées.
   - **Chaque jour** – la mise à jour s'exécutera tous les jours. Spécifiez l'heure de mise à jour dans le champ correspondant.
   - **Chaque semaine** – la mise à jour s'effectuera une fois par semaine. Spécifiez la date et l'heure de mise à jour dans les champs correspondants.

2.1.9. Mise à jour des paramètres de l'application

Note

Pour plus de détails sur le fonctionnement conjoint de Kaspersky Mobile Security et de Kaspersky Administration Kit, consultez le Guide de l'administrateur de Kaspersky Mobile Security.

Quand Kaspersky Mobile Security est utilisé avec Kaspersky Administration Kit, les paramètres de l'application sont définis par la stratégie du groupe de périphériques mobiles. L'activation de l'application et le verrouillage des paramètres de la stratégie (pour éviter leur modification) se produit quand un périphérique est ajouté au groupe d'administration.

La postérieure synchronisation de l'application avec le serveur d'administration se réalise automatiquement dans l'intervalle défini dans les paramètres de la stratégie.

Pour exécuter une synchronisation manuelle de l'application avec le Serveur d'administration :

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).
2. Ouvrez l'onglet **Mise à jour**.
3. Choisissez **Synchronisation**.

Au cours de la synchronisation, les paramètres d'application sont téléchargés et des rapports d'activité de l'application sont transmis par votre périphérique au serveur d'administration. Si les paramètres d'application n'ont pas changé depuis la dernière synchronisation, les paramètres de la stratégie ne sont pas appliqués.

2.1.10. Utilisation du module Pare-feu

Le module Pare-feu permet de surveiller l'activité réseau et protéger votre périphérique mobile sur le réseau (Figure 21).

Vous pouvez sélectionner le niveau de protection (paramètre **Pare-feu**) afin de contrôler le trafic entrant et sortant avec les options offertes :

- **Haut** – toute l'activité réseau est interdite sauf la mise à jour des bases de l'application et la connexion avec Kaspersky Administration Kit.
- **Moyen** – toutes les connexions entrantes sont interdites, les connexions sortantes ne sont autorisées qu'à travers les ports SSH, HTTP, HTTPS, IMAP, SMTP.
- **Bas** – seules les connexions entrantes sont interdites.
- **Arrêt** – toute l'activité réseau est autorisée.

Le paramètre **Notifications** permet d'activer ou de désactiver les notifications à l'utilisateur sur les tentatives de connexion par rapport au niveau de protection sélectionné du Pare-feu. Pour désactiver la réception de notifications, sélectionnez **Arrêté**.

Figure 21. Onglet **Pare-feu**

Des informations sur l'activité du module Pare-feu seront consignées dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Pare-feu**.

2.1.11. Affichage du rapport d'activité de l'application

Vous pouvez visualiser le journal chronologique des événements liés au fonctionnement de Kaspersky Mobile Security dans l'onglet **Information**. Pour ce faire, ouvrez l'onglet et sélectionnez **Rapports** (Figure 22).

Figure 22. Rapport d'activité de l'application

2.2. Désinstallation de l'application

Pour désinstaller Kaspersky Mobile Security, procédez de la manière suivante :

1. Fermez Kaspersky Mobile Security. Pour ce faire :
   a) Maintenez appuyé le bouton **Menu**.
   b) Sélectionnez **KMS 7.0 EE** dans la liste des applications en exécution puis cliquez sur **Options**.
   c) Choisissez **Quitter** dans le menu (Figure 23).

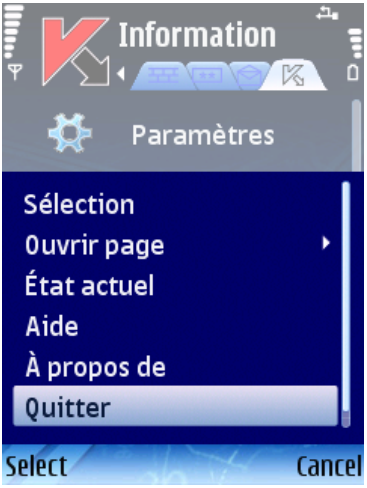

Figure 23. Fermeture de l'application

2. Désinstallation de Kaspersky Mobile Security

   a) Appuyez sur **Menu** puis sélectionnez **Gestionnaire d'applications** (Figure 24).

Figure 24. Démarrage du **Gestionnaire d'applications**

   b) Sélectionnez **KMS7.0 EE** dans la liste des applications puis cliquez sur **Options** (Figure 25).

Figure 25. Sélection de l'application

c) Sélectionnez la commande **Supprimer** (Figure 26).

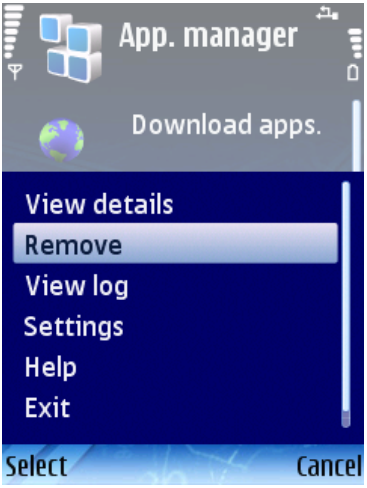

Figure 26. Désinstallation de l'application

d) Cliquez sur **Oui** dans la fenêtre de confirmation de suppression de l'application.

CHAPITRE 3. KASPERSKY MOBILE SECURITY POUR MICROSOFT WINDOWS MOBILE

Ce chapitre décrit le fonctionnement de Kaspersky Mobile Security sur des périphériques mobiles exploités sous l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

3.1. Premiers pas

Cette section explique comment démarrer l'application. Elle explique également le fonctionnement général de l'interface utilisateur.

3.1.1. Lancement de l'application

Pour lancer Kaspersky Mobile Security, procédez de la manière suivante :

1. Ouvrez le menu **Applications** sur votre périphérique mobile.
2. Sélectionnez **KMS 7.0 EE** pour lancer l'application.

Après le démarrage de l'application, une fenêtre avec les principaux composants de Kaspersky Mobile Security (Figure 27) sera affichée sur l'écran du périphérique mobile.

- **Prot. en temps réel** – état de la protection en temps réel.
- **Dernière analyse** – date et heure de la dernière analyse anti-virus du périphérique mobile.
- **Dernière mise à jour** – date de publication des bases de Kaspersky Mobile Security utilisées par l'application.

Remarque :

Si l'analyse antivirus d'un périphérique mobile n'a pas été réalisée ou qu'elle date de plus de deux semaines, l'icône correspondante se présente comme ceci : ⚠. Cette icône apparaît également si le mode de protection en temps réel ou le module Anti-Spam sont désactivés.

- **Pare-feu** – protection du périphérique sur le réseau.
- **Anti-Spam** – état du module Anti-Spam utilisé pour filtrer les messages SMS.

Remarque :

Le module Anti-Spam n'est pas disponible pour les modèle PDA !

Figure 27. Fenêtre d'état des composants de l'application

3.1.2. Interface graphique utilisateur

L'interface utilisateur compte six onglets disponibles dans le **Menu** (Figure 28) :

- L'onglet **Analyse** permet d'effectuer une analyse antivirus du périphérique mobile, de modifier les paramètres de l'analyse antivirus, de la protection en temps réel et de la quarantaine, et planifier des analyses automatiques (section 3.2 à la page 42).
- L'onglet **Pare-feu** permet de surveiller l'activité réseau et de protéger le périphérique sur le réseau (section 3.7 à la page 58).
- L'onglet **Mise à jour** permet de mettre à jour la base antivirus, de configurer et de planifier la mise à jour (section 3.5 à la page 56).

- L'onglet **Anti-Spam** permet de configurer les filtres de messages SMS entrants (module Anti-Spam) (section 3.4.1 à la page 48).
- L'onglet **Antivol** permet de verrouiller le périphérique et d'en effacer les informations en cas de vol ou de perte (module Antivol) (section 3.4.2 à la page 52).
- L'onglet **Information** permet d'afficher les rapports d'activité des composants de l'application ; des informations générales sur l'application et la base antivirus utilisée (section 3.8 à la page 60).

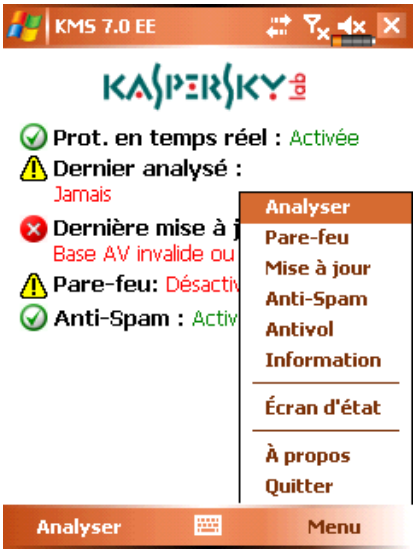

Figure 28. Menu de l'application

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

Pour afficher des informations générales sur l'application, sélectionnez **À propos**.

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

3.2. Analyse antivirus et protection en temps réel

L'onglet **Analyse** permet d'effectuer l'analyse anti-virus complète du système de fichiers et de la mémoire du périphérique mobile, ou seulement d'un dossier ou d'un fichier. Vous pouvez également modifier la configuration de l'analyse anti-virus et du mode de protection en temps réel, afficher un rapport avec les résultats de l'analyse, ou planifier l'exécution automatique de l'analyse.

3.2.1. Analyse à la demande

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

1. Sélectionnez **Paramètres d'analyse** dans la section **Analyse**.
2. Spécifiez la couverture de l'analyse dans la section **Options d'analyse** en sélectionnant les types de fichier à analyser :
   - **Analyser les archives** – analyse les fichiers comprimés dans des archives.
   - **Exécutables seuls** – 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. Si la désinfection n'est pas nécessaire, sélectionnez une action possible en spécifiant l'une des valeurs suivantes du paramètre **Action principale** :
   - **Quarantaine** – place en quarantaine les objets infectés détectés.
   - **Demander confirmation** – affiche à l'écran un message de détection de virus 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.

   Pour faire en sorte que l'application tente de réparer l'objet infecté, cochez la case **Tenter de réparer**. Choisissez l'action appliquée si la désinfection est impossible dans la section **Si la réparation est impossible**.

Pour lancer une analyse antivirus, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.1.1 à la page 39).

2. Dans la section **Analyse** (Figure 29) sélectionnez **Analyser téléphone** si vous souhaitez analyser le système de fichiers complet du périphérique mobile ou **Analyser dossier** pour analyser un dossier individuel.

Figure 29. Section **Analyser**

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

Après le démarrage de l'analyse, une fenêtre affiche l'état courant de la tâche : nombre d'objets analysés et chemin de l'objet en cours d'analyse (Figure 30).

Figure 30. Fenêtre **Progression de l'analyse**

Figure 31. Notification de détection de virus

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

3.2.2. Protection en temps réel des fichiers

Dans le mode de protection en temps réel, une partie résidente de Kaspersky Mobile Security reste chargée dans la mémoire RAM du périphérique afin d'analyser les programmes exécutables et les fichiers ouverts par l'utilisateur.

Le mode de protection en temps réel démarre avec la mise sous tension du périphérique et reste en fonctionnement jusqu'à sa mise hors-tension (à moins que ce mode ne soit désactivé par configuration).

En outre, Kaspersky Mobile Security 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 consignés dans un rapport. Pour afficher le rapport, sélectionnez **Rapport d'analyse**. Le rapport est également disponible dans la section **Information** (section 3.8 à la page 60) ;

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

1. Sélectionnez **Paramètres de surveillance** dans la section **Analyse**.
2. Cochez la case **Prot. en temps réel**.

Pour modifier les paramètres de protection en temps réel, procédez de la manière suivante :

1. Sélectionnez **Paramètres de surveillance** dans la section **Analyse**.
2. Cochez la case **Exécutables seuls** dans la section **Paramètres d'analyse** if vous souhaitez que la protection en temps réel analyse uniquement les fichiers exécutables. Décochez la case pour que la protection en temps réel analyse tous les programmes exécutables et les fichiers ouverts par l'utilisateur.
3. Dans la section **Action antivirus**, spécifiez l'action que l'application doit réaliser quand elle détecte un objet infecté. Vous avez le choix parmi les options suivantes :
   - **Quarantaine** – place en quarantaine les objets infectés détectés.
   - **Supprimer** – supprime les objets infectés détectés.
   - **Ignorer** — ne réalise aucune action sur les objets infectés.

3.2.3. Planification de l'analyse

Kaspersky Mobile Security permet de planifier des analyses automatiques du périphérique mobile. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, l'action définie par les paramètres d'analyse sera exécutée sur cet objet (entrée **Paramètres d'analyse**).

Par défaut, la planification est désactivée.

Pour planifier l'analyse du système de fichiers du périphérique, procédez de la manière suivante :

sélectionnez **Planification** dans la section **Analyser** et programmez l'exécution de l'analyse (Figure 32) :

- **Chaque jour** – l'analyse s'exécutera tous les jours. L'heure d'analyse est déterminée par le paramètre **Heure**.
- **Chaque semaine** – l'analyse s'exécutera une fois par semaine. La date et l'heure d'analyse sont spécifiées par les paramètres **Jour de la semaine** et **Heure**.
- **Manuel** – l'action est lancée manuellement par l'utilisateur.

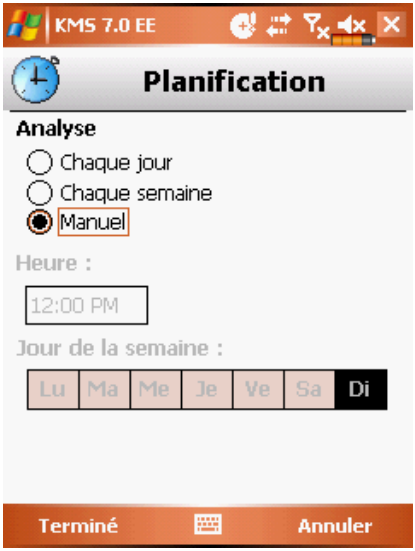

Figure 32. Le menu **Planification**

3.3. Utilisation de la quarantaine

Les objets infectés placés en quarantaine ne supposent aucune menace pour le périphérique et peuvent être supprimés ou restaurés par la suite.

L'application peut déplacer les objets infectés détectés vers la quarantaine automatiquement ou après confirmation de votre part.

Pour déplacer automatiquement les objets infectés vers la quarantaine :

1. Ouvrez la section **Analyse**.
2. Sélectionnez **Paramètres d'analyse**.
3. Dans la section **Action antivirus**, spécifiez **Quarantaine** pour l'action à quand l'application détecte un objet infecté.

   Si vous choisissez l'action **Demander confirmation**, quand un objet infecté est découvert, une fenêtre est présentée à l'utilisateur offrant le choix de supprimer l'objet ou de le placer en quarantaine.

Pour afficher le contenu de la quarantaine,

ouvrez l'onglet **Analyse** et sélectionnez **Quarantaine** (Figure 33).

Figure 33. **Quarantaine**

Le menu **Menu** de la fenêtre Quarantaine permet de :

- Afficher le détail d'un objet sélectionné en quarantaine (**Info détaillée**).
- Supprimer l'objet sélectionné (**Supprimer fichier**).
- Restaurer l'objet courant en quarantaine vers son dossier d'origine (**Restaurer**).
- Effacer tous les objets de la quarantaine (**Vider la quarantaine**).

3.4. Utilisation des modules Anti-Spam et Antivol

Le module Anti-Spam est prévu pour protéger en temps réel votre périphérique contre les messages SMS indésirables.

Le filtrage fait appel aux listes dites « noire » et « blanche ». Ces listes contiennent des téléphones et des échantillons de frases caractéristiques des messages normaux ou indésirables. La séquence d'analyse du message est la suivante :

- vérifier si le numéro est présent dans la liste noire ;
- vérifier si le numéro de l'expéditeur est présent dans la liste blanche ;
- analyser la présence dans le texte du message de frases de la liste noire ;
- analyser la présence dans le texte du message de frases de la liste blanche ;

si une correspondance est détectée, l'analyse est interrompue. Le message contenant un élément de la liste noire est interdit. Le message contenant un élément de la liste blanche est autorisé.

3.4.1. Module anti-spam

Le module Anti-Spam est prévu pour protéger en temps réel votre mobile contre les messages SMS et MMS indésirables.

Remarque :

Le module Anti-Spam n'est pas disponible pour les modèle PDA !

Le filtrage fait appel aux listes dites « noire » et « blanche ». Ces listes contiennent des téléphones et des échantillons de frases caractéristiques des

messages normaux ou indésirables. La séquence d'analyse du message est la suivante :

- vérifier si le numéro est présent dans la liste noire ;
- vérifier si le numéro de l'expéditeur est présent dans la liste blanche ;
- analyser la présence dans le texte du message de frases de la liste noire ;
- analyser la présence dans le texte du message de frases de la liste blanche ;

si une correspondance est détectée, l'analyse est interrompue. Le message contenant un élément de la liste noire est interdit. Le message contenant un élément de la liste blanche est autorisé.

Pour modifier la configuration du module Anti-Spam :

1. Sélectionnez **Paramètres** dans la section **Anti-Spam**.
2. Sélectionnez le mode de fonctionnement **Anti-Spam** avec le paramètre **Anti-Spam** :
   - **Normal.** Dans ce mode, le module Anti-Spam filtre les messages entrants en fonction des listes noire et blanche uniquement. Quand un message est envoyé par un numéro qui ne figure dans aucune de ces listes, le module Anti-Spam affiche un message proposant d'interdire ou d'autoriser la réception du message et d'ajouter le numéro de téléphone à la liste blanche ou noire.
   - **Liste noire uniquement.** Dans ce mode, le module Anti-Spam interdit les messages appartenant à la liste noire. Tous les autres messages sont remis.
   - **Liste blanche uniquement.** Dans ce mode, le module Anti-Spam laisse passer les messages appartenant à la liste blanche. Tous les autres messages sont interdits.
   - **Désactivé.** Le composant anti-spam est désactivé dans ce mode. Aucun filtrage des messages entrants n'est assuré.
3. Cochez la case **Ajout contacts liste blanche** pour éviter que le module Anti-Spam ne bloque la réception de messages appartenant à la liste des contacts.
4. Cochez la case **Interdire non numériques** pour que le module Anti-Spam bloque les messages provenant d'expéditeurs non numériques.

3.4.1.1. Modification des listes noire et blanche

La Liste noire conserve des données utilisées par le module Anti-Spam pour interdire les messages avec le même contenu.

La Liste noire conserve des données utilisées par le module Anti-Spam pour interdire les messages avec le même contenu.

Pour modifier la liste noire ou blanche,

ouvrez la section **Anti-Spam** (Figure 34) et sélectionnez l'entrée correspondante.

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

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

Sélectionnez **Insérer numéro** et spécifiez le numéro de téléphone (champ **Indiquer un téléphone**) que vous souhaitez inclure dans la liste. Le numéro peut commencer par un chiffre ou par le signe « + ». En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ».

Vous pouvez également spécifier le texte (champ **Entrez le texte**) dont la détection déclenche les actions suivantes de l'application :

- le message contenant ce texte présent dans la liste blanche sera autorisé ;
- le message contenant ce texte présent dans la liste blanche sera interdit ;

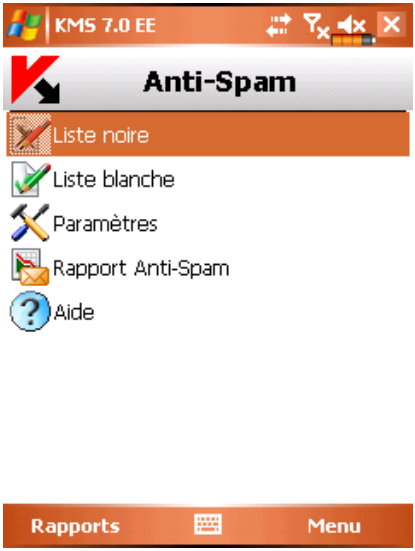

Figure 34. Section **Anti-Spam**

Après avoir modifié la liste, appuyez sur **Terminé** pour revenir à la section **Anti-Spam**.

3.4.1.2. 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 (section 3.4.1 à la page 48), un avertissement apparaît sur l'écran du périphérique mobile (Figure 35).

Figure 35. Avertissement du module Anti-Spam

Dans le **Menu**, choisissez l'une des actions suivantes à appliquer au 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** – interdit 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 consignées dans le rapport de l'application.

Pour afficher le rapport, sélectionnez **Rapport Anti-Spam** dans la section **Anti-Spam**. Le rapport est également disponible dans la section **Information** (section 3.8 à la page 59) ;

3.4.2. Onglet Antivol

Le module Antivol (section **Antivol** (Figure 36) est prévu pour garantir la protection contre un accès non autorisé aux données conservées dans le périphérique mobile, en cas de perte ou de vol.

La première fois que vous accéder aux paramètres du module, vous devez définir un code. Ce code donne accès aux paramètres du module et permet d'activer ses fonctions. Le code est nécessaire pour empêcher un accès non autorisé aux paramètres du module et pour permettre à l'utilisateur de verrouiller et d'effacer les informations enregistrées dans le périphérique en cas de perte ou de vol.

Verrouillage – permet de verrouiller le périphérique à la demande de l'utilisateur. Le périphérique ne pourra être déverrouillé qu'après avoir entré le code d'accès au module Antivol. Le déclenchement de cette caractéristique se produit après que l'utilisateur envoie un message SMS « block:code » au périphérique perdu.

Suppression – permet d'effacer les données personnelles de l'utilisateur (contacts, messages entrants, fichiers personnels, paramètres de connexion réseau). Le déclenchement de cette caractéristique se produit après que l'utilisateur envoie un message SMS « clean:code » au périphérique perdu.

La fonction **SIM-Surveillance** permet, quand la carte SIM est remplacée dans le périphérique, d'envoyer aux numéros spécifiés le nouveau numéro du téléphone et de verrouiller le périphérique volé. Le périphérique ne pourra être déverrouillé qu'après avoir entré le code d'accès au module Antivol.

Si un changement de code est nécessaire afin de travailler avec le module Antivol, sélectionnez **Changer le code**. Entrez et confirmez le nouveau code puis cliquez sur **Terminé**.

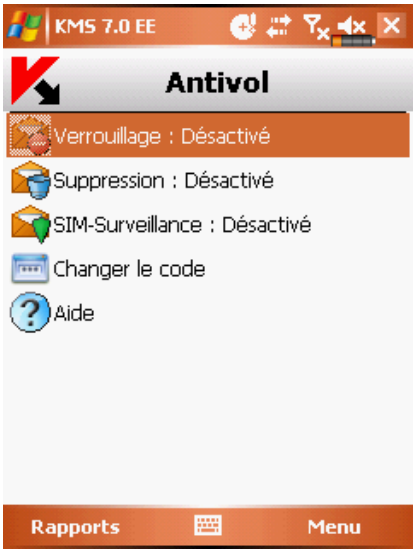

Figure 36. Section **Antivol**

Des informations sur l'activité du module Antivol seront consignées dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapport** dans la section **Antivol**. Le rapport est également disponible dans la section **Information** (section 3.8 à la page 60) ;

3.4.2.1. Paramètres de la fonction Suppression

La fonction **Suppression** permet d'effacer les données du périphérique en cas de perte (Figure 37).

Pour modifier la configuration de la fonction Suppression, procédez de la manière suivante :

1. Ouvrez la section **Antivol**
2. Entrez le code puis choisissez **Suppression** dans la fenêtre ouverte.
3. Cochez la case **contacts** box si vous souhaitez supprimer votre carnet de téléphones aussitôt après la perte ou le vol de votre périphérique mobile.
4. Cochez la case **boîte de réception** pour supprimer les messages et les SMS.
5. Cochez la case **documents** if vous souhaitez supprimer les fichiers personnels.
6. Cochez la case **paramètres réseau** if vous souhaitez effacer les paramètres de connexion réseau.
7. Cochez la case **fichiers sur la carte** si vous souhaitez supprimer les fichiers de la carte mémoire du périphérique.
8. Appuyez sur **Terminé** pour enregistrer les modifications.

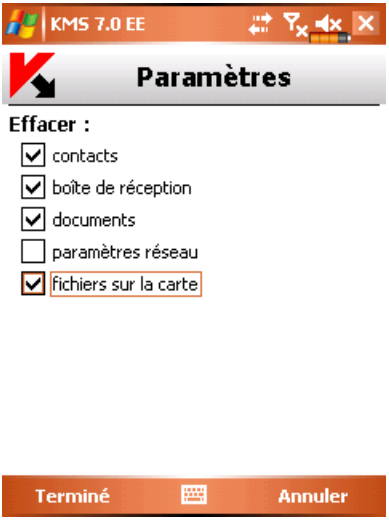

Figure 37. Paramètres Suppression

3.4.2.2. Paramètres de la fonction SIM-Surveillance

La fonction **SIM-Surveillance** permet de contrôler le remplacement de la carte SIM dans le périphérique (Figure 38).

Pour modifier la configuration de la fonction SMS-Watch, procédez de la manière suivante :

1. Ouvrez la section **Antivol**
2. Entrez le code puis choisissez **SIM-Surveillance** dans la fenêtre ouverte.
3. Utilisez les champs **1)** et **2)** pour indiquer les numéros destinataires du nouveau numéro de téléphone en cas de remplacement de la carte SIM de votre périphérique. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.
4. Cochez la case **Bloquer** pour verrouiller le périphérique si la carte SIM est remplacée.
5. Appuyez sur **Terminé** pour enregistrer les modifications.

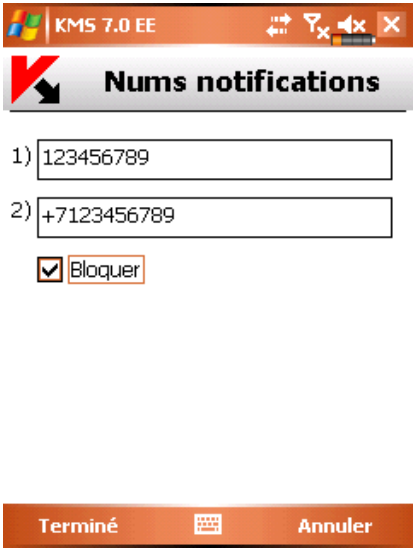

Figure 38. Paramètres de la fonction SIM-Surveillance

3.5. Mise à jour des bases de l'application

La détection de logiciels malveillants fait appel aux enregistrements des bases de Kaspersky Mobile Security, contenant les descriptions de tous les logiciels malveillants connus jusqu'à cette date. Il est extrêmement important d'assurer la mise à jour des bases.

Leur mise à jour peut se faire manuellement ou de manière planifiée. Pour configurer et lancer la mise à jour, utilisez l'onglet **Mise à jour** (Figure 39). Les mises à jour sont téléchargées depuis les serveurs de Kaspersky Lab.

Des informations sur la mise à jour des bases seront consignées dans le rapport. Pour afficher le rapport, sélectionnez **Rapport de Mise à jour** dans la section **Mise à jour**. Le rapport est également disponible dans la section **Information** (section 3.8 à la page 60) ;

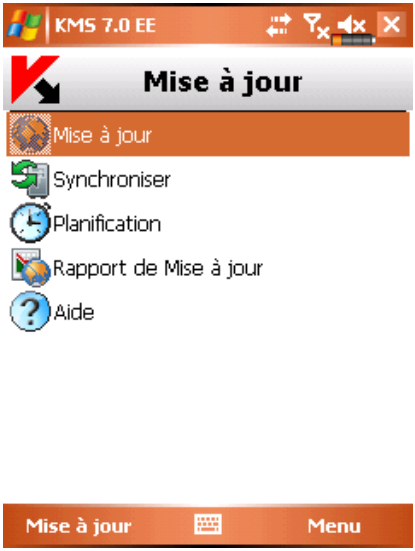

Figure 39. L'onglet **Mise à jour**

Pour lancer manuellement la mise à jour des bases d'application, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.1.1 à la page 39) et ouvrez la section **Mise à jour**.
2. Sélectionnez **Mise à jour** pour lancer le téléchargement des mises à jour.

Pour planifier la mise à jour des bases d'application, procédez de la manière suivante.

1. Lancez Kaspersky Mobile Security (section 3.1.1 à la page 39) et ouvrez la section **Mise à jour**.
2. Sélectionnez **Planification**.
3. Spécifiez la fréquence des mises à jour dans la section **Mise à jour automatique** :
   - **Chaque jour** – la mise à jour s'exécute tous les jours. Le cas échéant, spécifiez l'**Heure** de la mise à jour.
   - **Chaque semaine** – la mise à jour s'effectuera une fois par semaine. Le cas échéant, spécifiez le **Jour de la semaine** et l'**Heure** de mise à jour.

- **Manuel** – l'action est lancée manuellement par l'utilisateur.

Vous pouvez vérifier la date et le nombre de signatures antivirus de la base d'application dans la section **Information**. Pour ce faire, sélectionnez **À propos des bases** sur le même onglet.

3.6. Mise à jour des paramètres de l'application

Note

Pour plus de détails sur le fonctionnement conjoint de Kaspersky Mobile Security et de Kaspersky Administration Kit, consultez le Guide de l'administrateur de Kaspersky Mobile Security.

Quand Kaspersky Mobile Security est utilisé avec Kaspersky Administration Kit, les paramètres de l'application sont définis par la stratégie du groupe de périphériques mobiles. L'activation de l'application et le verrouillage des paramètres de la stratégie (pour éviter leur modification) se produit quand un périphérique est ajouté au groupe d'administration.

La postérieure synchronisation de l'application avec le serveur d'administration se réalise automatiquement dans l'intervalle défini dans les paramètres de la stratégie.

Pour exécuter une synchronisation manuelle de l'application avec le Serveur d'administration :

1. Lancez Kaspersky Mobile Security (section 2.1.1 à la page 10).
2. Ouvrez la section **Mise à jour**.
3. Sélectionnez **Synchroniser**.

Au cours de la synchronisation, les paramètres d'application sont téléchargés et des rapports d'activité de l'application sont transmis par votre périphérique au serveur d'administration. Si les paramètres d'application n'ont pas changé depuis la dernière synchronisation, les paramètres de la stratégie ne sont pas appliqués.

3.7. Pare-feu

Le module **Pare-feu** permet de surveiller l'activité réseau et protéger votre périphérique mobile sur le réseau (Figure 40).

Pour modifier la configuration du Pare-feu, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.1.1 à la page 39) et ouvrez la section **Pare-feu**.
2. Sélectionnez **Paramètres du Pare-feu**. Dans la fenêtre ouverte, définissez le niveau de protection pour indiquer le degré de surveillance du trafic entrant et sortant. Les options suivantes sont disponibles :
   - **Bloquer tout** – toute l'activité réseau est interdite sauf la mise à jour des bases de l'application et la connexion avec Kaspersky Administration Kit.
   - **Moyen** – toutes les connexions entrantes sont interdites, les connexions sortantes ne sont autorisées qu'à travers les ports SSH, HTTP, HTTPS, IMAP, SMTP.
   - **Bas** – seules les connexions entrantes sont interdites.
   - **Désactivé** – toute l'activité réseau est autorisée.

Des informations sur le fonctionnement du Pare-feu seront consignées dans le rapport. Pour afficher le rapport, sélectionnez **Rapport du Pare-feu** dans la section **Pare-feu**.

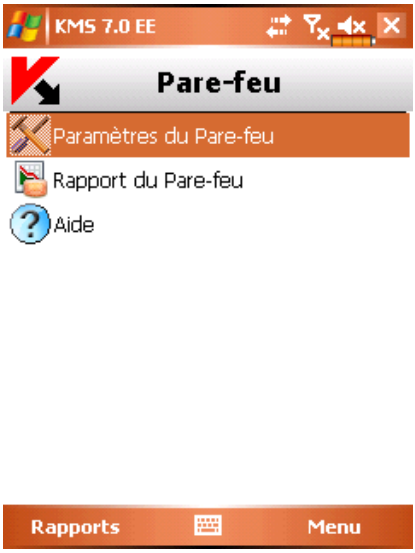

Figure 40. Section **Pare-feu**

3.8. Affichage de rapports d'activité de l'application

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

- analyse antivirus ;
- mise à jour des bases de l'application ;
- fonction pare-feu ;
- module anti-spam
- Le module Antivol.

Pour afficher le rapport d'activité d'un composant de l'application, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.1.1 à la page 39).
2. Sélectionnez **Rapports** dans l'onglet **Information** (Figure 41).
3. Sélectionnez le rapport du composant souhaité dans la fenêtre ouverte.

Figure 41. Section **Rapports**

3.9. Désinstallation de l'application

Pour désinstaller Kaspersky Mobile Security, procédez de la manière suivante :

1. Mode de protection de l'objet (pour plus de détails voir section 3.2 à la page 42) ;

Figure 42. Désactivation de la protection en temps réel

2. Fermez Kaspersky Mobile Security. Pour ce faire, choisissez **Quitter** dans le menu (Figure 43).

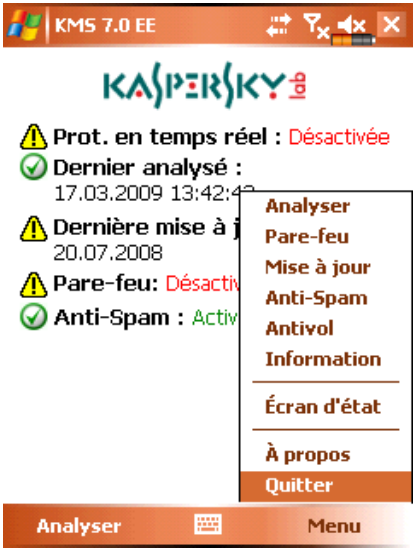

Figure 43. Fermeture de l'application

3. Désinstallez l'application. Pour ce faire :

   a) Cliquez sur **Démarrer**, dans le menu **Paramètres**, ouvrez l'onglet **Système** puis **Suppression d'applications** (Figure 44) :

Figure 44. Lancement de la désinstallation de l'application

b) Sélectionnez **Kaspersky Mobile Security** dans la liste des applications installées puis cliquez sur **Supprimer** (Figure 45).

Figure 45. Sélection de l'application

c) Cliquez sur **Oui** dans la fenêtre de confirmation de suppression de l'application (section Figure 46). Ensuite, une fenêtre d'information sur la suppression du fichier des paramètres d'application apparaît. Choisissez **Non** pour désinstaller complètement l'application. Si vous choisissez **Oui**, le fichier avec les paramètres de l'application sera conservé sur le périphérique.

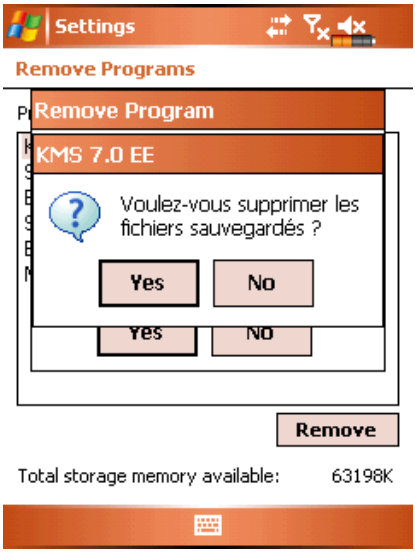

Figure 46. Confirmation avant d'enregistrer les paramètres de l'application

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, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux États-Unis (Californie). 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 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 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. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Kaspersky® Anti-virus, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : 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. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus® : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site officiel de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie de virus :	http://www.viruslist.com/fr/
Laboratoire Anti-Virus :	newvirus@kaspersky.com (uniquement pour l'envoi des objets suspects archivés) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les demandes auprès des experts de virus)

ANNEXE B. CRYPTOEX S.A.R.L.

La composition et l'analyse de la signature numérique électronique dans Kaspersky Administration Kit repose sur la bibliothèque logicielle de protection de l'information (PBZI) "Crypto-Si" développée par CryptoEx S.A.R.L. CryptoEx S.A.R.L. possède la licence FAPSI (FSB) et le certificat PBZI "Crypto-Si".

Le site de CryptoEx : http://www.cryptoex.ru

ANNEXE C. CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

LE LOGICIEL PEUT ETRE ACCOMPAGNE D'UN CONTRAT SUPPLEMENTAIRE, OU D'UN DOCUMENT SUPPLEMENTAIRE (LE « CONTRAT ADDITIONNEL »), QUI PEUT DETERMINER LE NOMBRE D'ORDINATEURS SUR LESQUELS PEUT ETRE UTILISE LE LOGICIEL, LA PERIODE D'UTILISATION DU LOGICIEL, LES TYPES D'OBJETS AUXQUELS IL EST DESTINE ET DIVERSES AUTRES CONDITIONS D'ACHAT, D'ACQUISITION ET D'UTILISATION SUPPLEMENTAIRES. CE CONTRAT ADDITIONNEL EST PARTIE INTEGRANTE DU CONTRAT DE LICENCE.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les « téléphones intelligents », les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *« Vous »* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *« entité »,* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limité, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patch, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

1.8. **Acquisition du logiciel** signifie son achat ou acquisition à des conditions définies dans un contrat additionnel, y compris une acquisition gratuite.

2. Concession de la Licence

2.1. Le Titulaire des droits convient par la présente de Vous accorder une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (« l'utilisation ») du Logiciel sur un nombre spécifié d'Ordinateurs pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions

générales de ce Contrat (la « Licence ») et vous acceptez cette Licence :

Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs spécifiés dans les licences que vous avez obtenues auprès du Titulaire des droits, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence achetée vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acheté sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel ou comme spécifié dans le Contrat additionnel.

2.3. Si le Logiciel a été acheté sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'achat de la Licence du Logiciel ou comme spécifié dans le Contrat additionnel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques ou morales dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que

vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acheté le Logiciel auprès du Titulaire des droits.

2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acheté sur un support physique) ou stipulée pendant l'achat (si le Logiciel a été acheté sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acheté sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat ou comme spécifié dans le Contrat additionnel.

3.3. Si le Logiciel a été acheté sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'achat ou comme spécifié dans le Contrat additionnel.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acheté le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com

5. Recueil d'informations

5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.

5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.

5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.

5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

6. Limitations

6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.

6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.

6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

7. Garantie limitée et avis de non-responsabilité

7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.

7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.

7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la

période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

7.6. LE LOGICIEL EST FOURNI « TEL QUEL » ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LE « COMMON LAW », LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

8. Exclusion et Limitation de responsabilité

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À

L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

9. Licence GNU et autres licences de tierces parties

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (« Logiciel libre »). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre

de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

10. Droits de propriété intellectuelle

10.1 Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des Etats-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les « Marques de commerce »). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

10.2 Vous convenez que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du

Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.

10.3 Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

11. Droit applicable ; arbitrage

Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 11 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

12. Délai de recours.

Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

13. Intégralité de l'accord ; divisibilité ; absence de renoncement.

Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste

du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en equity de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

14. Service clientèle du titulaire des droits

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com