

KASPERSKY LAB

Kaspersky Mobile Security 7.0

GUIDE DE
L'UTILISATEUR

KASPERSKY MOBILE SECURITY 7.0

Guide de l'utilisateur

© Kaspersky Lab

Tel., Télécopie : +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000

<http://www.kaspersky.com/fr>

Date de révision : Décembre, 2007

Table des matières

CHAPITRE 1. KASPERSKY MOBILE SECURITY 7.0.....	5
1.1. Spécifications matérielles et logicielles.....	6
1.2. Contenu de la distribution.....	6
CHAPITRE 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS.....	7
2.1. Installation de Kaspersky Mobile Security	7
2.2. Utilisation de l'application	8
2.2.1. Activation de l'application	8
2.2.2. Lancement de l'application.....	9
2.2.3. Interface graphique utilisateur	10
2.2.4. Paramètres généraux.....	11
2.2.5. Analyse et protection antivirus	12
2.2.6. Utilisation de la quarantaine	16
2.2.7. Utilisation des modules Anti-Spam et Antivol.....	18
2.2.8. Mise à jour des bases de l'application	26
2.2.9. Utilisation du module Firewall.....	29
2.2.10. Affichage du rapport d'activité de l'application.....	30
2.3. Suppression de l'application.....	30
CHAPITRE 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE	33
3.1. Installation de Kaspersky Mobile Security	33
3.2. Premiers pas.....	34
3.2.1. Activation de l'application	34
3.2.2. Lancement de l'application.....	35
3.2.3. Interface graphique utilisateur	37
3.3. Analyse et protection antivirus	38
3.3.1. Protection en temps réel et analyse à la demande des fichiers	38
3.3.2. Planification de l'analyse	42
3.4. Utilisation de la quarantaine.....	43
3.5. Utilisation des modules Anti-Spam et Antivol.....	44
3.5.1. Module anti-spam	44

3.5.2. Modification des listes noire et blanche	45
3.5.3. Actions appliquées aux messages	46
3.5.4. Le module Antivol	47
3.6. Mise à jour des bases de l'application	51
3.7. Firewall	53
3.8. Affichage de rapports d'activité de l'application	54
3.9. Suppression de l'application.....	55
 ANNEXE A. KASPERSKY LAB	 59
A.1. Autres produits Kaspersky Lab	60
A.2. Comment nous contacter	71
 ANNEXE B. CONTRAT DE LICENCE	 73

CHAPITRE 1. KASPERSKY

MOBILE SECURITY 7.0

Kaspersky Mobile Security 7.0 est conçu pour assurer en la protection en temps réel de périphériques Smartphone et Communicator 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), les messages EMS et MMS, lors de la synchronisation avec un ordinateur personnel ou du téléchargement de fichiers par 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 et MMS entrants 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 les rapports d'activité de la protection antivirus consignés par l'application.

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 appareils Smartphone et Communicator 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.

Le logiciel s'exécute uniquement sur des modèles Smartphones et Communicator prenant en charge la réception et l'envoi de messages SMS.

1.2. Contenu de la 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.

CHAPITRE 2. KASPERSKY

MOBILE SECURITY FOR

SYMBIAN OS

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

2.1. Installation de Kaspersky Mobile Security

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

1. Copiez le paquet de distribution de l'application dans votre Smartphone.
2. Exécutez l'installation (ouvrez le fichier CAB de la distribution dans le Smartphone).
3. Pour confirmer l'installation, choisissez **Oui** (voir Figure 1).



Figure 1. Confirmation de l'installation

4. Si la langue du système d'exploitation et de la version de Kaspersky Mobile Security ne correspond pas, un message apparaîtra sur l'écran. Pour continuer l'installation en français, cliquez sur **OK**.
5. Lisez le texte du contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir Figure 2).

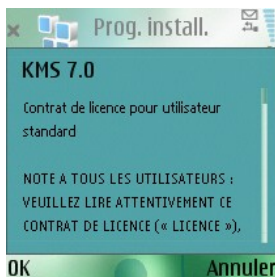


Figure 2. Contrat de licence

Attention !

Ce logiciel ne prévoit pas sa propre sauvegarde ou restauration.

2.2. 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 et MMS, l'analyse anti-virus du Smartphone, les mises à jour de l'application sur le réseau, etc.

2.2.1. Activation de l'application

Quand l'application est exécutée pour la première fois, la fenêtre d'activation de Kaspersky Mobile Security (voir Figure 3) sera affichée sur l'écran du Smartphone.



Figure 3. La fenêtre d'activation de l'application

L'activation est nécessaire pour rendre disponibles toutes les fonctions de Kaspersky Mobile Security. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab..

Attention !

Pour activer Kaspersky Mobile Security 7.0, une connexion GPRS ou WLAN du Smartphone est nécessaire.

Le code d'activation est composé de lettres en alphabet latin et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus.

Après avoir saisi le code d'activation, sélectionnez **Lancer l'activation** dans le menu **Options**. L'application envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe la clé.

Si le code d'activation saisi est invalide, un message vous l'indique sur l'écran du Smartphone.

2.2.2. Lancement de l'application

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

1. Ouvrez le menu principal du téléphone.
2. Sélectionnez **KMS 7.0** puis lancez l'application à avec **Ouvrir** dans le menu **Options**.

Note

Quand l'application démarre pour la première fois, elle vous propose d'activer la fonction de démarrage automatique (section 2.2.4 à la page 11). Si vous êtes d'accord, appuyez sur **OK**.

Ensuite, le Smartphone présente dans une fenêtre les principaux composants de Kaspersky Mobile Security (voir Figure 4) sera affichée sur l'écran du Smartphone.

- **Prot. en temps réel** – utilisation du mode de protection en temps réel (section 2.2.5 à la page 12) ;
- **Dernière Analyse**– date et heure de la dernière analyse anti-virus du Smartphone.
- **Date de la base** – date de publication de la base utilisée par l'application.
- **Config. Anti-Spam** – mode de fonctionnement du composant Anti-Spam (section 2.2.7 à la page 18).
- **Niveau du Firewall** – niveau de protection du Smartphone (section 2.2.9 à la page 29).



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

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

2.2.3. Interface graphique utilisateur

L'interface graphique contient six onglets :

- L'onglet **Analyseur** permet d'effectuer une analyse anti-virus du Smartphone, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique.
- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects.
- L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de configurer et de planifier la mise à jour.
- L'onglet **Firewall** permet de surveiller l'activité réseau et de protéger le Smartphone sur le réseau.
- L'onglet **Divers** permet de filtrer les messages SMS et MMS entrants (module Anti-Spam), de verrouiller le Smartphone ou d'en effacer les informations en cas de vol ou de perte (module Antivol).
- L'onglet **Information** permet d'afficher les rapports d'activité des composants de l'application ; des informations générales sur l'application et la base anti-virus utilisée, ainsi que de modifier les paramètres généraux de l'application.

Pour vous déplacer d'un onglet à l'autre, utilisez le joystick du Smartphone ou sélectionnez **Ouvrir page** dans le menu **Options** (voir Figure 5).

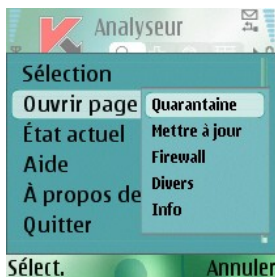


Figure 5. Le menu **Options**

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

2.2.4. Paramètres généraux

Les paramètres de l'onglet **Information** sous l'entrée **Paramètres** (voir Figure 6) permettent de configurer les fonctions suivantes de l'application :

- **Lancement automat.** – mode de démarrage automatique. Dans le mode de lancement automatique, les fonctions principales de l'application seront lancées à la mise sous tension du Smartphone. En désactivant le lancement automatique, ces fonctions principales seront arrêtées. Si vous souhaitez maintenir en permanence la protection des fonctions principales, sélectionnez **Oui**.
- **Voir écran d'état** détermine si l'état actuel de la protection est affiché au lancement de l'application.
- **Taille rapport** : définit la taille maximum du rapport. Quand cette limite est atteinte, les anciens messages sont supprimés afin de respecter la valeur maximale 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.). Sélectionnez **Oui** si vous souhaitez utiliser des alertes sonores.
- **Vibration** : indique si le Smartphone doit vibrer quand l'infection d'un objet est détectée. Par défaut la vibration est activée.



Figure 6. Le menu **Paramètres**

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

2.2.5. Analyse et protection antivirus

L'onglet **Analyseur** permet d'effectuer l'analyse anti-virus complète du système de fichiers et de la mémoire du Smartphone, 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.

2.2.5.1. 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 Smartphone.

Le mode de protection en temps réel démarre avec la mise sous tension du Smartphone 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 Smartphone, 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 **Analyseur**.

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

1. Sélectionnez **Paramètres** dans l'onglet **Analyseur**.
2. Activez ou désactivez le mode de protection en temps réel en définissant la valeur correspondante du paramètre **Prot. en temps réel**.

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

1. Sélectionnez **Paramètres** dans l'onglet **Analyseur**.
2. 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.
 - **Fichiers exécutables** – analyse uniquement les fichiers d'application exécutables (par exemple : *.exe, *.sis, *.mdl, *.app).
3. Sélectionnez l'action qui sera exécutée lors de la découverte d'un objet infecté (paramètre **Action en cas de virus**).

Si vous souhaitez afficher un message de confirmation de l'action à prendre en présence d'un objet infecté, sélectionnez la valeur **Confirmer l'action**.

Pour supprimer sans afficher de demande de confirmation, sélectionnez **Suppression auto**.

Si vous souhaitez que les objets détectés soient automatiquement déplacés en quarantaine, sélectionnez **Quarantaine**. La mise en quarantaine des objets infectés est l'action par défaut.

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

Sous certaines circonstance, la mémoire ROM peut devenir vulnérable aux logiciels malveillants. Pour autoriser l'analyse de la mémoire ROM par Kaspersky Mobile Security, choisissez **Oui**.

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

Si vous souhaitez que Kaspersky Mobile Security décomprime les archives SIS et ZIP au cours de l'analyse, sélectionnez **Oui**. S'il n'est pas nécessaire de décompresser les archives pendant l'analyse, désactivez cette fonction avec **Non**.

6. Activez ou désactivez la fonction d'analyse des nouvelles cartes (paramètre **Analyser carte**).

Pour que Kaspersky Mobile Security analyse en arrière-plan les cartes insérées, choisissez **Analyse auto**. Pour désactiver l'analyse automatique des cartes de mémoire flash, choisissez **Désactiver**. Si vous souhaitez que Kaspersky Mobile Security affiche un message de confirmation avant d'analyser une nouvelle carte lors de son insertion, choisissez **Avec confirmation**.

7. Activez ou désactivez l'affichage de l'icône de protection (paramètre **Afficher l'icône PTR**).

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

Note

Pour modifier les valeurs des paramètres, utilisez le joystick de votre Smartphone 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 par défaut, dans l'onglet **Analyser**, sélectionnez **Par défaut** dans le menu **Options**.

Pour planifier les analyses, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 2.2.2 à la page 9).
2. Dans l'onglet **Analyseur** (voir Figure 7) sélectionnez **Tout analyser** si vous souhaitez analyser le système de fichiers complet de votre Smartphone, ou **Dossier** pour analyser un dossier individuel.



Figure 7. L'onglet **Analyseur**

Si vous avez choisi l'option **Dossier**, une fenêtre présente alors le système de fichiers du Smartphone. Utilisez les boutons du joystick pour vous déplacer dans le système de fichiers de votre Smartphone.

Pour analyser un dossier, positionnez le curseur sur le répertoire que vous souhaitez analyser et sélectionnez **Lancer l'analyse** dans le menu **Options**.

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



Figure 8. Fenêtre **Progression de l'analyse**

Quand un objet infecté est détecté, l'application propose de supprimer le fichier concerné (action **Supprimer**), de le déplacer vers la quarantaine (action **Quarantaine**) ou de laisser intact (action **Ignorer**).

Attention !

Le logiciel ne demandera l'action à réaliser sur l'objet que si le paramètre **Action en cas de virus** est défini à **Confirmer l'action** (pour plus détails, voir section 2.2.5.1 à la page 12).



Figure 9. Notification de détection de virus

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

Si vous souhaitez un rétro-éclairage permanent pendant l'analyse, ouvrez l'onglet **Information**, ouvrez le menu **Paramètres** puis choisissez la valeur **Oui**

pour le **Rétro-éclairage**. Par défaut, si aucune touche du Smartphone n'est utilisée, le rétro-éclairage sera automatiquement désactivé pour économiser les batteries.

2.2.5.2. Planification de l'analyse

Kaspersky Mobile Security permet de planifier des analyses automatiques du Smartphone. L'analyse est exécutée en arrière plan. Quand un objet infecté est détecté, l'action définie par les paramètres d'analyse sera exécutée sur cet objet (section 2.2.5.1 à la page 12).

Par défaut, la planification est désactivée.

Pour planifier l'analyse :

Dans l'onglet **Analyseur**, sélectionnez **Planification** et configurez les paramètres **Analyse auto** (voir Figure 10):

- **Chaque jour** – l'analyse s'exécutera tous les jours. Spécifiez **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 **Heure d'analyse auto**.



Figure 10. Le menu **Planification**

2.2.6. Utilisation de la quarantaine

Les objets infectés placés en quarantaine ne supposent aucune menace pour le Smartphone 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 configurer la quarantaine automatique des objets infectés, ouvrez l'onglet **Analyseur**, sélectionnez **Paramètres** puis choisissez la valeur **Quarantaine** pour le paramètre **Action en cas de virus**.

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

L'accès aux fonctions principales de la quarantaine est disponible dans l'onglet **Quarantaine** (voir Figure 11).



Figure 11. Le menu **Quarantaine**

Sélectionnez **Quarantaine** pour afficher la liste de tous les objets en quarantaine (voir Figure 12).

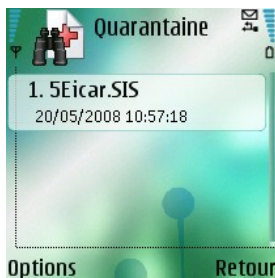


Figure 12. Nombre d'objets infectés en quarantaine

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

- Afficher le détail de n'importe quel objet conservé en quarantaine (**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**).
- Voir l'aide de la quarantaine (**Aide**).

Pour configurer les paramètres de quarantaine, utilisez le menu **Paramètres** de l'onglet **Quarantaine** (voir Figure 13).



Figure 13. 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**.

2.2.7. Utilisation des modules Anti-Spam et Antivol

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

Le filtrage fait appel aux listes dites « noire » et « blanche ». Les messages entrants provenant de téléphones ajoutés à la liste noire sont bloqués par le composant Anti-Spam. Les messages provenant de numéros ajoutés à la liste « blanche » ne sont pas bloqués.

Le module Antivol assure le verrouillage du Smartphone et la suppression des informations conservées en mémoire en cas de vol.

2.2.7.1. Modes de fonctionnement Anti-Spam

Pour configurer le mode de fonctionnement Anti-Spam, ouvrez l'onglet **Divers**, sélectionnez **Anti-Spam**, puis sélectionnez **Paramètres**. Sélectionnez l'un des modes suivants du paramètre **Config. Anti-Spam** :

- **Activer.** Dans ce mode, le composant 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 composant 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.
- **Listes B/N uniquement.** Dans ce mode, le composant Anti-Spam filtre les messages entrants en fonction des listes noire et blanche uniquement. La réception de messages de numéros qui ne sont présents dans aucune des listes sera autorisée sans demander confirmation à l'utilisateur.
- **Désactiver.** Le composant anti-spam est désactivé dans ce mode. Aucun filtrage des messages entrant n'est assuré.

2.2.7.2. Modification des listes noire et blanche

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

Note

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

Pour modifier la liste noire ou blanche, ouvrez l'onglet **Anti-Spam** (voir Figure 14) et sélectionnez la liste souhaitée.

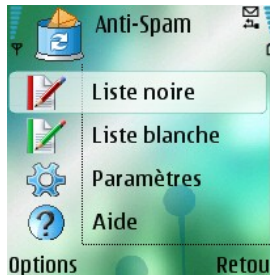


Figure 14. Le menu **Anti-Spam**

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

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

Si vous sélectionnez **Ajouter enregistr.** ou **Modifier enregistr.**, vous devez spécifier les paramètres suivants de l'enregistrement :

- **Type de message** : spécifie le type des messages entrants qui seront bloqués ou autorisés (pour la liste noire ou blanche, respectivement). Valeurs autorisées: **SMS seuls**, **MMS seuls** et **Tous messages**.
- **Numéro de téléphone**. Spécifie le numéro de téléphone d'où proviennent les messages à interdire ou à autoriser. Pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » and « * ».
- Dans le champ **Texte**, spécifiez le texte du message entrant, 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 ;

La séquence d'analyse du message est la suivante :

- vérifier si le numéro est présent dans la liste noire ;
- vérifier si le numéro est présent dans la liste blanche ;

- vérifier si le texte du message est présent dans la liste noire ;
- vérifier si le texte du message est présent dans la liste blanche ;

Si le message vérifie n'importe laquelle des conditions, l'analyse ne continue pas et le message est autorisé ou bloqué, selon qu'il correspond à la liste noire ou blanche.

Après avoir spécifié ces paramètres, appuyez sur **Retour** pour enregistrer les modifications et revenir à la fenêtre contenant la liste (voir Figure 15).

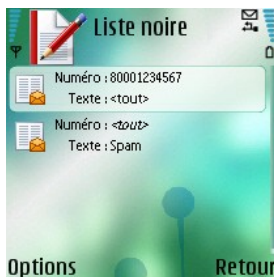


Figure 15. La liste noire

2.2.7.3. Paramètres Anti-Spam

Pour configurer le composant Anti-Spam, ouvrez l'onglet **Anti-Spam** et sélectionnez **Paramètres** (voir Figure 16).



Figure 16. Paramètres Anti-Spam

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

- **Autoriser contacts.** Si le paramètre est défini à **Oui**, le composant 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 composant 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**, le composant Anti-Spam ajoutera automatiquement à la liste blanche tous les numéros de téléphone utilisés pour envoyer des messages SMS ou MMS. Sélectionnez **Non** pour désactiver cette option.
- **Non numérique seulmt.** Si le paramètre est défini à **Non**, le composant Anti-Spam n'interdira pas les messages entrants provenant de numéros de téléphone sans numéro. Choisissez **Oui** pour activer l'option.
- **Différencier les types :** Si le paramètre est défini à **Non**, la valeur **Tous messages** sera utilisé pour le type de message des enregistrements créés dans la liste blanche ou noire (pour plus de détails sur les paramètres des enregistrements de ces listes, voir 2.2.7.2 à la page 19 autrement, les nouveaux enregistrements seront créés selon le type de message spécifique (SMS ou MMS).

Note

Ce paramètre affectera les enregistrements créés par le composant 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 2.2.7.4 à la page 22).

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

2.2.7.4. 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 composant Anti-Spam intercepte le message et affiche un avertissement sur l'écran du Smartphone (voir Figure 17).

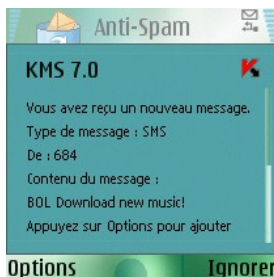


Figure 17. Avertissement du composant Anti-Spam

Dans le menu **Options**, choisissez l'une des actions suivantes à appliquer au message :

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

Si le paramètre **Différencier les types** est défini à **Non** dans la configuration du composant Anti-Spam, alors les actions **Ajouter à la liste blanche** ou **Ajouter à la liste noire** créeront respectivement une entrée pour tous les types messages dans la liste correspondante (**Type de message – Tous messages**), autrement le type correspondra au type du message reçu (pour plus de détails sur les paramètres des enregistrements de ces listes, voir section 2.2.7.2 à la page 19).

Des informations sur les messages bloqués sont consignées dans le rapport de l'application. Pour afficher le rapport, sélectionnez l'entrée **Rapports** dans l'onglet Divers.

2.2.7.5. Module Antivol

Ce module est conçu 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 accédez aux paramètres du module, vous devez définir un mot de passe. Ce mot de passe vous donne accès aux paramètres du module afin de pouvoir les modifier. Le mot de passe est nécessaire pour empêcher un accès non autorisé aux paramètres et pour permettre à l'utilisateur de verrouiller et d'effacer les informations enregistrées dans le Smartphone en cas de perte ou de vol.

SMS-Block – permet de verrouiller le périphérique à la demande de l'utilisateur. Le périphérique ne pourra être déverrouillé qu'après avoir entré le mot de passe d'accès au module Antivol. L'activation du paramètre se produit après que l'utilisateur du Smartphone volé envoie un SMS : « *block:code* ». Pour utiliser cette fonction, choisissez **Marche**.

SMS-Clean permet d'effacer les données personnelles de l'utilisateur (contacts, messages entrants, fichiers personnels). Le déclenchement de cette caractéristique se produit après que l'utilisateur du périphérique volé envoie un SMS : « *clean:code* ». Pour utiliser la fonction **SMS-Clean**, choisissez **Marche**.

SIM-Watch permet, quand la carte SIM est remplacée dans le Smartphone, d'envoyer au numéro spécifié le nouveau numéro et de verrouiller le dispositif volé. Pour utiliser cette fonction, choisissez **Marche**.

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

Chaque fois que vous accédez à la configuration du module Antivol (voir Figure 18) vous devez saisir le mot de passe défini précédemment.



Figure 18. 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 **Divers**.

2.2.7.6. Paramètres du module SMS-Clean

Pour configurer la fonction SMS-Clean, ouvrez l'onglet **Divers** puis sélectionnez **Antivol**. Entrez le mot de passe (section 2.2.7.5 à la page 23) puis sélectionnez **SMS-Clean** dans la fenêtre ouverte.

La section **SMS-Clean** présente la liste des données qui pourront être supprimées en cas de perte ou de vol (voir Figure 19).

Figure 19. Onglet **SMS-Clean**

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

Pour supprimer les messages de courrier, les SMS ou les MMS (dossiers Boîte de réception et de messagerie) sélectionnez **Nettoyer B. Réception/Supp. Fichiers perso** et définissez sa valeur à **Oui**.

L'option **Supp. Fichiers perso** se charge de la suppression des données personnelles (données du dossier !:\Data\). Par défaut, la suppression des fichiers personnels n'est pas activée. Si vous souhaitez supprimer votre répertoire téléphonique en cas de perte ou de vol de votre Smartphone, sélectionnez cette entrée et définissez sa valeur à **Oui**.

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

2.2.7.7. Paramètres SIM-Watch

Pour configurer la fonction **SIM-Watch**, ouvrez l'onglet **Divers** puis sélectionnez **Antivol**. Entrez le mot de passe (section 2.2.7.5 à la page 23) puis sélectionnez **SIM-Watch** dans la fenêtre ouverte.

La section **SIM-Watch** permet de surveiller la substitution de la carte SIM dans le périphérique (voir Figure 20).



Figure 20. Onglet **SIM-Watch**

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 Smartphone. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.

Vous pouvez également configurer le verrouillage de votre Smartphone en cas de remplacement de la carte SIM. Pour ce faire, sélectionnez **Verr. périphérique** et définissez sa valeur à Oui. Le périphérique ne pourra être déverrouillé qu'après avoir entré le mot de passe d'accès au module Antivol. Par défaut, le verrouillage du périphérique n'est pas activé.

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

2.2.8. 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 Smartphone après chaque mise à jour des bases de Kaspersky Mobile Security. Pour ce faire, sélectionnez **Paramètres** sur l'onglet **Mise à jour** et définissez la valeur **Marche** à l'entrée **Analyser après 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 **Arrêt**.

Si vous ne souhaitez pas avoir à sélectionner le point d'accès Internet à chaque mise à jour, choisissez **Non** pour le paramètre **Demander le point** : l'application mémorisera le point d'accès utilisé par la dernière mise à jour réussie, et l'utilisera à l'avenir pour établir une connexion réseau. Vous pouvez également configurer un nouveau point d'accès.

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 un autre serveur défini par l'utilisateur (valeur **Personnalisé**). Si vous avez choisi l'option **Spécifier**, 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**.

2.2.8.1. Paramètres des mises à jour

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

1. Lancez Kaspersky Mobile Security (section 2.2.2 à la page 9).
2. Ouvrez l'onglet **Paramètres** dans l'onglet **Mise à jour** (voir Figure 21).

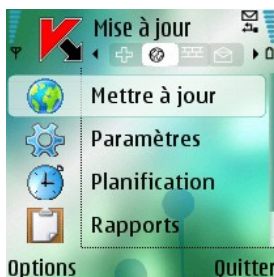


Figure 21. Onglet **Mise à jour**

3. Active / désactive la demande du point d'accès (paramètre **Demander le point**).

Note

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

Si vous avez choisi **Non**, la connexion sera établie avec le point d'accès utilisée lors de la mise à jour précédente.

Si la demande est activée, l'application vous propose de choisir dans une liste de points d'accès disponibles (voir Figure 22).



Figure 22. 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 (voir Figure 23).



Figure 23. 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>.

Attention !

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

2.2.8.2. Mise à jour manuelle

Pour lancer une mise à jour manuelle,

1. Lancez Kaspersky Mobile Security (section 2.2.2 à la page 9).
2. Sélectionnez **Mettre à jour** dans l'onglet **Mise à jour** (voir Figure 21).

2.2.8.3. Mise à jour planifiée

Pour planifier la mise à jour des bases :

1. Lancez Kaspersky Mobile Security (section 2.2.2 à la page 9).
2. Sélectionnez **Planification** dans l'onglet **Mise à jour** et configurez les Paramètres de **Mise à jour auto** :
 - **Arrêt** – 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 champs 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.

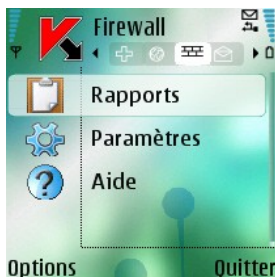
2.2.9. Utilisation du module Firewall

Le module Firewall (pare-feu) est conçu pour surveiller l'activité réseau de votre Smartphone (voir Figure 24).

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

- **Haut** – toute l'activité réseau est interdite.
- **Moyen** – toutes les connexions entrantes sont interdites, seul le trafic sortant des applications normales est autorisé.
- **Bas** – seules les connexions entrantes sont interdites.
- **Désactivé** – toute l'activité réseau est autorisée.

Le paramètre **Notifications** permet de configurer la réception de notifications si l'utilisateur exécute des actions non prévues par le niveau de protection sélectionné. Pour désactiver la réception de notifications, sélectionnez **Arrêt**.

Figure 24. Onglet **Firewall**

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

2.2.10. 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** (voir Figure 25).



Figure 25. Rapport d'activité de l'application

2.3. Suppression de l'application

Pour supprimer Kaspersky Mobile Security de votre Smartphone, procédez de la manière suivante :

1. Fermez Kaspersky Mobile Security. Pour ce faire :
 - Maintenez appuyé le bouton **Menu**.

- Sélectionnez **KMS 7.0** dans la liste des applications en exécution puis cliquez sur **Options**.
- Sélectionnez la commande **Quitter** (voir Figure 26).



Figure 26. Fermeture de l'application

2. Supprimez Kaspersky Mobile Security

- Appuyez sur **Menu** puis sélectionnez **Gestionnaire d'applications** (voir Figure 27).



Figure 27. Lancement du Gestionnaire d'applications

- Sélectionnez **KMS 7.0** dans la liste des applications puis cliquez sur **Options** (voir Figure 28).

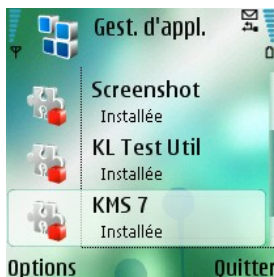


Figure 28. Sélection de l'application

- Sélectionnez la commande **Supprimer** (voir Figure 29).



Figure 29. Suppression de l'application

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

CHAPITRE 3. KASPERSKY

MOBILE SECURITY FOR

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. Installation de Kaspersky

Mobile Security

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

1. Copiez le fichier CAB contenant la distribution de l'application dans votre périphérique mobile.
2. Exécutez l'installation (ouvrez le fichier CAB de la distribution dans le périphérique mobile). L'application sera installée dans la mémoire principale du périphérique mobile.
3. Lisez le texte du contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Pour abandonner l'installation, appuyez sur **Annuler** (voir Figure 30).

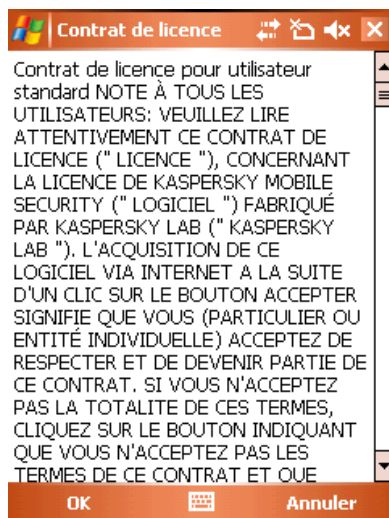


Figure 30. Contrat de licence

3.2. Premiers pas

Cette section décrit comment activer puis lancer l'application après son installation dans le périphérique mobile. Elle explique également le fonctionnement général de l'interface utilisateur.

3.2.1. Activation de l'application

Quand l'application est exécutée pour la première fois, the fenêtre d'activation de Kaspersky Mobile Security (voir Figure 31) sera affichée sur l'écran du périphérique mobile.



Figure 31. La fenêtre d'activation de l'application

L'activation est nécessaire pour rendre disponibles toutes les fonctions de Kaspersky Mobile Security. Vous pouvez obtenir le code d'activation sur le site Internet de Kaspersky Lab..

Attention !

Pour activer Kaspersky Mobile Security, une connexion GPRS du périphérique mobile est nécessaire.

Le code d'activation est composé de lettres en alphabet latin et de chiffres, et n'est pas sensible à la casse. Saisissez le code dans les 4 champs contigus.

Après avoir saisi le code d'activation, appuyez sur **Activation**. L'application envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe la clé de licence.

Si le code d'activation saisi est invalide, un message vous l'indique sur l'écran du Smartphone.

3.2.2. 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** afin de lancer l'application.

Après le démarrage de l'application startup, une fenêtre avec les principaux composants de Kaspersky Mobile Security (voir Figure 32) sera affichée sur l'écran du périphérique mobile.

- **Prot. en temps réel** – état de la protection en temps réel.
- **Dernière analyse** – date 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.

Attention !

Si l'analyse antivirus d'un périphérique mobile n'a pas été réalisée ou qu'elle date de plus de deux semaine, 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.

- **Firewall** – niveau de protection du Smartphone.
- **Anti-spam** – état du module Anti-Spam utilisé pour filtrer les messages SMS.

Attention !

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



Figure 32. Fenêtre d'état des composants de l'application

3.2.3. Interface graphique utilisateur

L'interface utilisateur compte six onglets disponibles dans le **Menu** (voir Figure 33):

- L'onglet **Analyser** permet d'effectuer une analyse anti-virus du périphérique mobile, de modifier les paramètres de l'analyse anti-virus et de la protection en temps réel et de configurer la planification de l'analyse automatique (section 3.3 à la page 38).
- L'onglet **Firewall** permet de surveiller l'activité réseau et de protéger le Smartphone sur le réseau (section 3.7 à la page 53).
- L'onglet **Mise à jour** permet de mettre à jour la base anti-virus, de configurer et de planifier la mise à jour.3.6 à la page 51).
- L'onglet **Quarantaine** permet de gérer la quarantaine – une zone spéciale destinée aux objets infectés et suspects (section 3.4 à la page 43).
- L'onglet **Divers** permet de filtrer les messages SMS et MMS entrants (module Anti-Spam), de verrouiller le périphérique ou d'en effacer les informations en cas de vol ou de perte (module Antivol) (section 3.5 à la page 44).
- L'onglet **Information** permet d'afficher les rapports d'activité des composants de l'application ; des informations générales sur l'application et la base anti-virus utilisée, ainsi que de modifier les paramètres généraux de l'application (section 3.8 à la page 54).



Figure 33. Menu de l'application

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

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

3.3. Analyse et protection antivirus

L'onglet **Analyser** 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.

3.3.1. 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.

La 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 aussi disponible sur l'onglet **Information** (section 3.8 à la page 54).

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

1. Sélectionnez **Paramètres d'analyse** dans le menu **Analyser** tab.
2. Activez ou désactivez la protection en temps réel en cochant ou décochant la case **État de la prot. en temps réel**.

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

1. Sélectionnez **Paramètres d'analyse** dans le menu **Analyser** tab.
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. Pour faire en sorte que Kaspersky Mobile Security tente de réparer l'objet infecté, cochez la case **Tenter de réparer**. Si la désinfection n'est pas nécessaire, sélectionnez une action possible en spécifiant l'une des valeurs suivantes du paramètre **Primary action** :
 - **Quarantaine** – place en quarantaine les objets infectés détectés.
 - **Confirmer l'action** – affiche un message de détection de virus à l'écran avec le choix de supprimer l'objet infecté, de le placer en quarantaine ou de l'ignorer.
 - **Supprimer** – supprime les objets infectés détectés.
 - **Ignorer** – ne réalise aucune action sur les objets infectés.

Vous pouvez aussi spécifier l'une des actions suivantes au cas où la réparation de l'objet infecté échouerait. Pour ce faire, cochez la

case **Tenter de réparer** et sélectionnez l'action requise dans la liste **Échec de réparation**.

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

1. Lancez Kaspersky Mobile Security (section 3.2.1 à la page 34).
2. Ouvrez l'onglet **Paramètres d'analyse**.
 - Spécifiez la couverture de l'analyse dans la section **Options d'analyse** en sélectionnant les types de fichier à analyser (voir plus haut).
 - Déterminez l'action que l'application doit réaliser quand elle détecte un objet infecté (voir plus haut).
3. Dans l'onglet **Analyser** (voir Figure 34) sélectionnez **Analyser le mobile** si vous souhaitez analyser le système de fichiers complet du périphérique mobile ou **Analyser un dossier** pour analyser un dossier individuel.

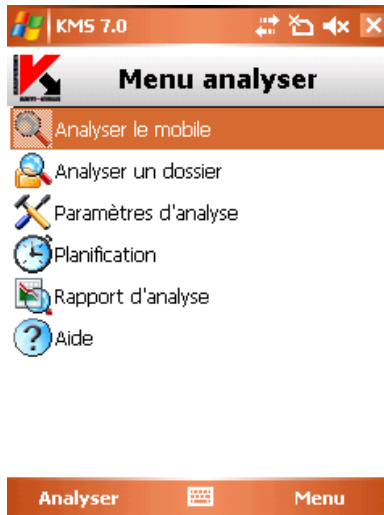


Figure 34. Onglet **Analyser**

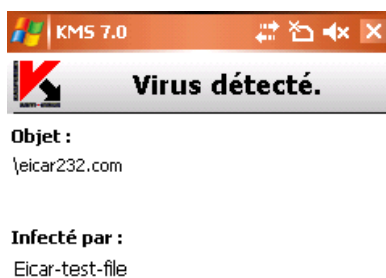
Si vous avez choisi l'option **Analyser un dossier**, une fenêtre présente alors le système de fichiers du périphérique. Pour lancer l'analyse sur un dossier, déplacez le curseur vers le dossier concerné et cliquez sur **Analyser**.

Après le démarrage de l'analyse, une fenêtre affiche l'état courant, le nombre d'objets analysés et le chemin de l'objet en cours d'analyse (voir Figure 35).



Arrêter

Figure 35. Progression de l'analyse



Ignorer

Action

Figure 36. Notification de détection de virus

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

3.3.2. Planification de l'analyse

Kaspersky Mobile Security permet de planifier des analyses automatiques du périphérique mobile. L'analyse est exécutée 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 :

Dans l'onglet **Analyser**, sélectionnez **Planification** et configurez les paramètres d'analyse (voir Figure 37):

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

KMS 7.0

Planification

Analyser

☐ Chaque jour

☒ Chaque semaine

☐ Manuellement

Heure :

12:00 PM

Jour de la semaine :

Lu Ma Me Je Ve Sa Di

Terminé Annuler

Figure 37. Le menu **Planification**

3.4. Utilisation de la quarantaine

Les objets infectés placés en quarantaine ne supposent aucune menace pour le périphérique mobile 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.

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

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

Pour afficher le contenu de la quarantaine, ouvrez vers les onglets **Quarantaine** (voir Figure 38).



Figure 38. 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**).

3.5. Utilisation des modules Anti-Spam et Antivol

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

Le filtrage fait appel aux listes dites « noire » et « blanche ». Les messages entrants provenant de téléphones ajoutés à la liste noire sont bloqués par le composant Anti-Spam. Les messages provenant de numéros ajoutés à la liste « blanche » ne sont pas bloqués.

Le module Antivol assure le verrouillage du Smartphone et la suppression des informations conservées en mémoire en cas de vol.

3.5.1. Module anti-spam

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

Le filtrage fait appel aux listes dites « noire » et « blanche ». Les messages entrants provenant de téléphones ajoutés à la liste noire sont bloqués par le composant Anti-Spam. Les messages provenant de numéros ajoutés à la liste « blanche » ne sont pas bloqués.

Pour modifier la configuration du composant Anti-Spam, procédez de la manière suivante :

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

3.5.2. Modification des listes noire et blanche

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

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

Pour modifier la liste noire ou blanche, ouvrez l'onglet **Anti-Spam** (voir Figure 39) et sélectionnez la liste souhaitée.

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

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

Sélectionnez **Insérer numéro** et spécifiez le numéro de téléphone (champs **Saisir un numéro**) 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 « ? » and « * ».

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 39. Le menu **Anti-Spam**

La séquence d'analyse du message est la suivante :

- vérifier si le numéro est présent dans la liste noire ;
- vérifier si le numéro est présent dans la liste blanche ;
- vérifier si le texte du message est présent dans la liste noire ;
- vérifier si le texte du message est présent dans la liste blanche ;

Si le message vérifie n'importe laquelle des conditions, l'analyse ne continue pas et le message est autorisé ou bloqué, selon qu'il correspond à la liste noire ou blanche.

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

3.5.3. 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 3.5.1 à la page 44), un avertissement apparaît sur l'écran du périphérique mobile (voir Figure 40).

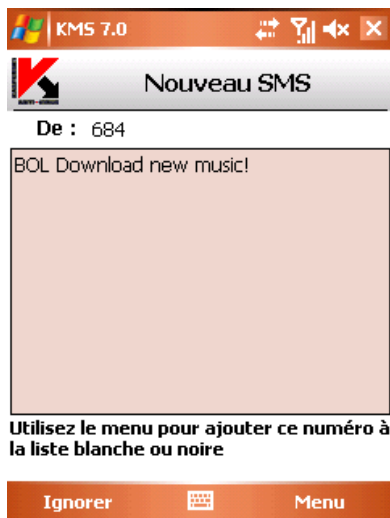


Figure 40. Avertissement du composant Anti-Spam

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, appuyez sur **Rapport** sur l'onglet **Anti-Spam** ou sélectionnez **Rapport Anti-Spam** sur le même onglet. Le rapport est aussi disponible sur l'onglet **Information** (section 3.8 à la page 54).

3.5.4. Le module Antivol

Ce module Antivol (onglet **Divers**, commande **Antivol**) (voir Figure 41) est conçu 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 accédez aux paramètres du module, vous devez définir un mot de passe. Ce mot de passe vous donne accès aux paramètres du module afin de pouvoir les modifier. Le mot de passe est nécessaire pour empêcher un accès non autorisé aux paramètres et pour permettre à l'utilisateur

de verrouiller et d'effacer les informations enregistrées dans le Smartphone en cas de perte ou de vol.

SMS-Block permet de verrouiller le périphérique à la demande de l'utilisateur. Le périphérique ne pourra être déverrouillé qu'après avoir entré le mot de passe d'accès au module Antivol. L'activation du paramètre se produit après que l'utilisateur du Smartphone volé envoie un SMS : « *block:code* ». La fonction **SMS-Block** est activée si sélectionnée: lisez le message d'information puis appuyez sur **Terminé** si vous souhaitez utiliser cette fonction.

SMS-Clean permet d'effacer les données personnelles de l'utilisateur (contacts, messages entrants, fichiers personnels). Le déclenchement de cette caractéristique se produit après que l'utilisateur du périphérique volé envoie un SMS : « *clean:code* ». La fonction **SMS-Clean** est activée si sélectionnée: spécifiez les valeurs requises de configuration (section 3.5.4.1 à la page 49), lisez le message d'information puis appuyez sur **Terminé** si vous souhaitez utiliser cette fonction.

SIM-Watch permet, quand la carte SIM est remplacée dans le Smartphone, d'envoyer au numéro spécifié le nouveau numéro et de verrouiller le dispositif volé. Le périphérique ne pourra être déverrouillé qu'après avoir entré le mot de passe d'accès au module Antivol. La fonction **SIM-Watch** est activée si sélectionnée: spécifiez les valeurs requises de configuration (section 3.5.4.2 à la page 50), lisez le message d'information puis appuyez sur **Terminé** si vous souhaitez utiliser cette fonction.

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

Figure 41. Onglet **Antivol**

Des informations sur l'activité du module Antivol seront consignées dans le rapport de l'application. Pour afficher le rapport, sélectionnez **Rapport Antivol** dans l'onglet **Divers**. Le rapport est aussi disponible sur l'onglet **Information** (section 3.8 à la page 54).

3.5.4.1. Paramètres du module SMS-Clean

La section **SMS-Clean** présente la liste des données qui pourront être supprimées en cas de perte ou de vol (voir Figure 42).

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

1. Sélectionnez **Antivol** sur l'onglet **Divers**.
2. Entrez le mot de passe puis choisissez **SMS-Clean** dans la fenêtre ouverte.
3. Cochez la case **contacts** si vous souhaitez supprimer votre répertoire téléphonique aussitôt après la perte ou le vol de votre périphérique mobile.
4. Cochez la case **Boîte de réception** pour supprimer les courriers, les SMS et les MMS entrants indésirables.

5. Cochez la case **documents** si vous souhaitez supprimer les données personnelles de l'utilisateur.
6. Cochez la case **Paramètres réseau** si vous souhaitez to supprimer les paramètres réseau.
7. Cliquez sur **Terminé** pour enregistrer les modifications.



Figure 42. Onglet **SMS-Clean**

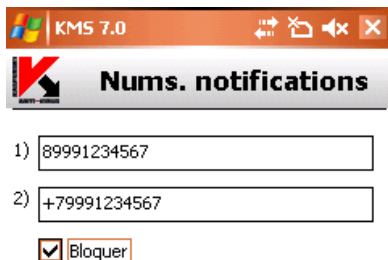
3.5.4.2. Paramètres SIM-Watch

La section **SIM Watch** permet de surveiller la substitution de la carte SIM dans le périphérique (voir Figure 43).

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

1. Sélectionnez **Antivol** sur l'onglet **Divers**.
2. Entrez le mot de passe puis choisissez **SIM-Watch** 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 Smartphone. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.

4. Configurez le verrouillage du périphérique mobile en cas de remplacement de la carte SIM. Pour ce faire, cochez la case **Bloquer**.
5. Appuyez sur **Terminé** pour enregistrer les modifications.



KMS 7.0

Nums. notifications

1) 89991234567

2) +79991234567

☒ Bloquer



Terminé Annuler

Figure 43. Onglet **SIM-Watch**

3.6. 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** (voir Figure 44). Les mises à jour sont téléchargées depuis les serveurs de Kaspersky Lab. En cas d'erreur, assurez-vous que le périphérique mobile dispose d'accès à Internet.

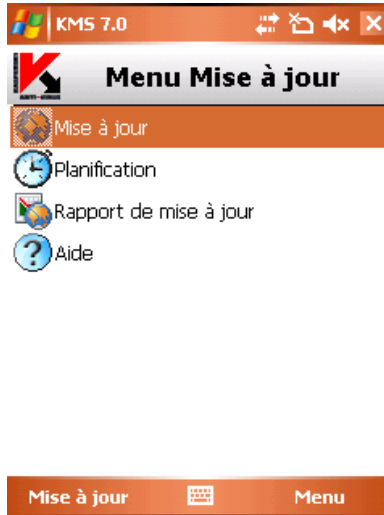


Figure 44. Onglet **Mise à jour**

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 l'onglet **Mise à jour**. Le rapport est aussi disponible sur l'onglet **Information** (section 3.8 à la page 54).

Pour lancer manuellement la mise à jour des bases d'application depuis les serveurs de mise à jour de Kaspersky Lab, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.2.1 à la page 34) et ouvrez l'onglet **Mise à jour**.
2. Sélectionnez **Mise à jour** pour lancer le téléchargement des mises à jour.

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

1. Lancez Kaspersky Mobile Security (section 3.2.1 à la page 34) et ouvrez l'onglet **Mise à jour**.
2. Pour modifier la planification de la mise à jour automatique, sélectionnez **Planification**.
3. Spécifiez la fréquence des mises à jour :
 - **Chaque jour** – la mise à jour s'exécutera 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.
- **Manuellement** – l'action est lancée manuellement par l'utilisateur.

L'onglet **Information** vous informe de la date de publication des bases antivirus actuellement installées sur le périphérique mobile et du nombre de signatures de virus. Pour ce faire, sélectionnez **A propos des bases** sur cet onglet.

3.7. Firewall

Le module **Firewall** permet de surveiller l'activité réseau et protéger votre périphérique mobile sur le réseau (voir Figure 45).

Pour modifier la configuration du Firewall, procédez de la manière suivante :

1. Lancez Kaspersky Mobile Security (section 3.2.1 à la page 34) et ouvrez l'onglet **Firewall**.
2. Sélectionnez **Paramètres du Firewall**. 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.
 - **Moyen** – tout le trafic entrant est interdit, seul le trafic sortant des applications normales est autorisé.
 - **Bas** – seul le trafic entrant est interdit.
 - **Désactivé** – toute l'activité réseau est autorisée.

Des informations sur le fonctionnement du Firewall seront consignées dans le rapport. Pour afficher le rapport, sélectionnez **Rapport du Firewall** dans l'onglet **Firewall**. Le rapport est aussi disponible sur l'onglet **Information** (section 3.8 à la page 54).



Figure 45. Onglet Firewall

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 firewall (pare-feu) ;
- module anti-spam
- Le module Antivol.

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

1. Lancez Kaspersky Mobile Security (section 3.2.1 à la page 34).
2. Pour afficher le rapport, sélectionnez **Rapports** dans l'onglet **Information** (voir Figure 46).

3. Sélectionnez un rapport sur la protection en temps réel dans la fenêtre ouverte.



Figure 46. Onglet **Rapports**

3.9. Suppression de l'application

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

1. Désactivez la protection en temps réel (pour plus de détails, voir section 3.3 à la page 38) ;

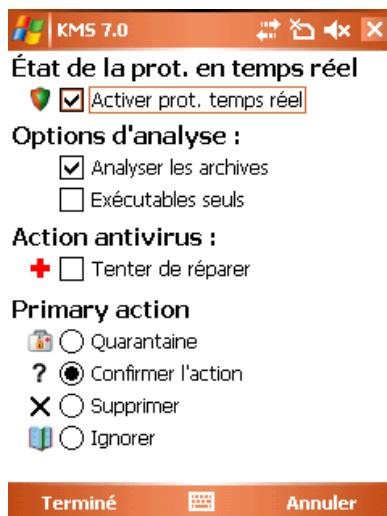


Figure 47. Arrêt de la protection en temps réel

2. Fermez Kaspersky Mobile Security. Pour ce faire, sélectionnez Quitter dans le menu de l'application (voir Figure 48).



Figure 48. Fermeture de l'application

3. Supprimer l'application. Pour ce faire :

- appuyez sur **Quitter**, choisissez Paramètres puis **Suppression d'applications** (voir Figure 49):

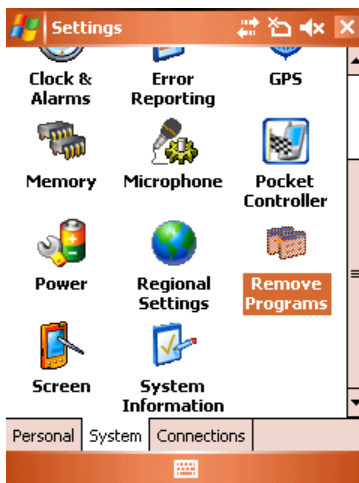


Figure 49. Lancement de la suppression de l'application

- Sélectionnez **KMS 7.0** dans la liste des applications installées puis cliquez sur **Supprimer** (voir Figure 50).

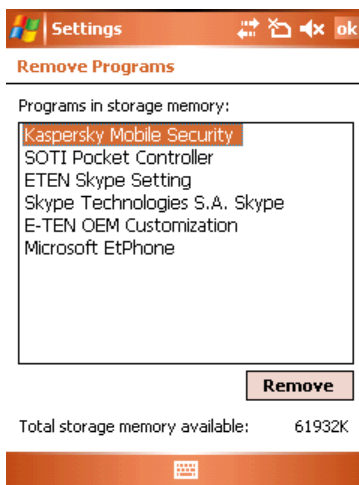


Figure 50. Sélection de l'application

- Cliquez sur **Oui** dans la fenêtre de confirmation de suppression de l'application (voir Figure 51).

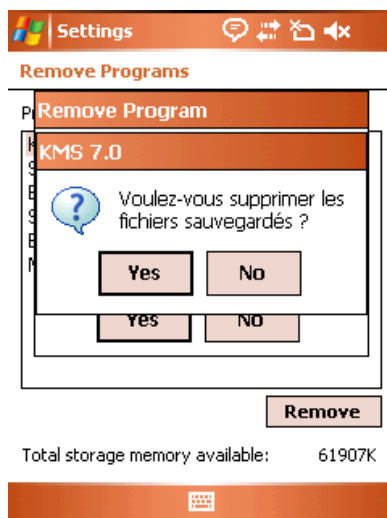


Figure 51. Confirmation de suppression de l'application

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, aux États-Unis (Canada), dans les pays du Benelux, en Chine, en Pologne et en Roumanie. 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 450 experts, tous spécialistes des technologies anti-virus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat, et deux experts senior sont des membres permanents de la CARO (Organisation pour la recherche anti-virus en informatique).

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 informatiques. Une analyse complète du comportement des virus informatiques permet à la société de fournir une protection complète contre les menaces présentes et futures. La résistance à de futures attaques est la stratégie de base mise en oeuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections anti-virus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-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. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automatisation avancée, en vue d'une protection anti-virus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau de Kaspersky Anti-Virus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde) et BorderWare (Canada).

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

A.1. Autres produits Kaspersky Lab

Kaspersky Lab News Agent

Le composant News Agent est conçu pour distribuer périodiquement les bulletins d'annonce de Kaspersky Lab, avec des notifications sur l'état courant d'activité virale et des nouvelles de dernière heure. L'application parcourt une liste et lit le contenu des bulletins d'informations du serveur de news de Kaspersky Lab avec une fréquence définie.

Le composant News Agent permet aux utilisateurs de :

- Visualiser les annonces de virus actuels dans la zone de notifications de la barre des tâches
- S'abonner ou se désabonner aux canaux d'informations
- Récupérer les informations des canaux sélectionnés à l'intervalle spécifié, et recevoir des notifications de dernière heure
- Lire les informations des canaux sélectionnés
- Examiner la liste et l'état des canaux
- Ouvrir le texte complet de l'article dans le navigateur

Le produit News Agent est une application Microsoft Windows indépendante, qui peut être utilisée seule ou intégrée avec différentes solutions fournies par Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Le programme est un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab. Le service offre en ligne une analyse anti-virus efficace de votre ordinateur. Kaspersky OnLine Scanner s'exécute directement dans votre navigateur. Les utilisateurs reçoivent ainsi des réponses rapides à leurs questions sur une infection potentielle de leurs ordinateurs. Avec ce service, les visiteurs peuvent :

- Exclure de l'analyse les fichiers compressés et les bases de messagerie ;

- Choisir des bases antivirus standard ou étendues pour réaliser l'analyse ;
- Enregistrer un rapport avec les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Le programme est un service par abonnement offert aux visiteurs du site Internet de la société Kaspersky Lab. Le service offre en ligne une analyse anti-virus efficace de votre ordinateur et la neutralisation des fichiers dangereux. Kaspersky OnLine Scanner Pro s'exécute directement dans votre navigateur. Avec ce service, les visiteurs peuvent :

- Exclure de l'analyse les fichiers compressés et les bases de messagerie ;
- Choisir des bases antivirus standard ou étendues pour réaliser l'analyse ;
- Enregistrer un rapport avec les résultats de l'analyse au format txt ou html.

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 est conçu pour protéger les ordinateurs personnels contre les logiciels malveillants et offre une combinaison excellente de méthodes anti-virus conventionnelles et de technologies proactives récentes.

Le programme offre une vérification anti-virus complexe qui comprend :

- Analyse anti-virus du trafic de messagerie au niveau des protocoles de transmission de données (POP3, IMAP et NNTP pour le courrier entrant, et SMTP pour le courrier sortant), indépendamment du client utilisé, ainsi que la désinfection des bases de messagerie.
- Analyse anti-virus en temps réel du trafic Internet échangé via HTTP.
- Analyse anti-virus de fichiers individuels, de répertoires ou d'unités de disque. En outre, une tâche prédéfinie permet de centrer l'analyse anti-virus exclusivement sur les zones critiques du système d'exploitation et sur les objets de démarrage de Microsoft Windows.

La protection proactive offre les caractéristiques suivantes :

- *Contrôle des modifications dans le système de fichiers.* Le programme permet aux utilisateurs de créer une liste d'applications qui seront contrôlées en fonction de leurs composants. Ceci permet de protéger l'intégrité des applications contre les actions de logiciels nocifs.
- *Surveillance des processus en mémoire vive.* Kaspersky Anti-Virus 7.0 informe régulièrement les utilisateurs chaque fois qu'il détecte des

processus suspects ou cachés ou quand des modifications non autorisées se produisent dans des processus actifs.

- *Surveillance des changements dans le Registre du système* grâce à un contrôle interne du Registre système.
- *Surveillance des processus cachés* qui protège contre le code malveillant dissimulé dans le système d'exploitation par des technologies de type « rootkit ».
- *Analysateur heuristique*. Au cours de l'analyse d'un logiciel, l'analysateur simule son exécution et enregistre toutes les activités suspectes, par exemple l'ouverture ou l'écriture dans un fichier, l'interception des vecteurs d'interruption, etc. En fonction de cette procédure, une décision est prise sur la possible infection du logiciel par un virus. L'émulateur travaille dans un environnement virtuel isolé qui protège contre tout risque d'infection de l'ordinateur.

Restauration du système après l'attaque d'un logiciel malveillant, grâce à l'enregistrement de toutes les modifications introduites dans le Registre et les fichiers système, puis leur annulation à la demande de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky® Internet Security 7.0 est une solution intégrale de protection des ordinateurs personnels contre les principales menaces aux données, à savoir, les virus, les pirates, le courrier indésirable et les logiciels espions. Une interface unique permet aux utilisateurs de configurer et de gérer tous les composants du logiciel.

Les caractéristiques de protection anti-virus comprennent :

- **Analyse anti-virus du trafic de messagerie** au niveau des protocoles de transmission de données (POP3, IMAP et NNTP pour le courrier entrant, et SMTP pour le courrier sortant), indépendamment du client utilisé. Le programme inclut des plug-ins pour les clients les plus répandus (Microsoft Office Outlook, Microsoft Outlook Express / Windows Mail et The Bat!) et assure la désinfection de leurs bases de messagerie.
- **Analyse anti-virus en temps réel du trafic Internet** échangé via HTTP.
- **Protection du système de fichiers**: analyse anti-virus de fichiers individuels, de répertoires ou d'unités de disque. En outre, l'application peut réaliser l'analyse anti-virus centrée exclusivement sur les zones critiques du système d'exploitation et sur les objets de démarrage de Microsoft Windows.

- **Protection proactive:** le programme surveille en continu l'activité des applications et des processus exécutés en mémoire vive, pour éviter toute modification dangereuse du système de fichiers ou du Registre, et il restaure le système après toute action malveillante.

La protection contre les fraudes Internet est assurée grâce à sa capacité pour identifier les tentatives de fraude (phishing), pour éviter les fuites de données confidentielles (à commencer par les mots de passe, les numéros de comptes bancaires et de carte de crédit) et pour bloquer l'exécution de scripts dangereux sur les pages Internet, dans les fenêtres indépendantes et les bandeaux publicitaires. La fonction de blocage des numéroteurs permet d'identifier et d'empêcher l'activité des logiciels qui tentent d'utiliser votre modem pour se connecter à votre insu à des services téléphoniques payants.

Kaspersky Internet Security 7.0 enregistre les tentatives d'exploration des ports de votre ordinateur, qui précèdent fréquemment des attaques réseau, et vous défend avec succès contre les typiques attaques de pirates. Le programme fait appel à des définitions de règles pour surveiller toutes les transactions réseau et contrôler tous les paquets de données entrants ou sortants. Le mode invisible (dépendant de la technologie SmartStealth™) évite la détection de votre ordinateur depuis l'extérieur. Quand vous activez ce mode, le système bloque toutes les activités réseau, à l'exception des quelques transactions autorisées par les règles personnalisées.

L'application emploie une approche complexe pour filtrer le courrier indésirable dans les messages entrants :

- Vérification sur des listes blanche et noire de destinataires (y compris les adresses de sites de fraude)
- Examen des phrases dans le corps du message
- Analyse du texte du message à l'aide d'un algorithme d'auto-apprentissage.
- Reconnaissance d'images indésirables.

Kaspersky Anti-Virus for File Servers

Ce paquet logiciel offre une protection fiable des systèmes de fichiers sur des serveurs sous Microsoft Windows, Novell NetWare, Linux et Samba, contre tous les types de logiciels malveillants. La suite comprend les applications Kaspersky Lab suivantes :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus pour postes de travail et Linux File Server.

- Kaspersky Anti-Virus pour postes de travail et serveurs de fichiers Novell Netware.
- Kaspersky Anti-Virus pour Samba Server.

Fonctions et caractéristiques :

- *Protection en temps réel des systèmes de fichiers du serveur*: tous les fichiers serveur sont analysés lors de leur accès ou enregistrement sur le serveur
- *Prévention contre les offensives virales* ;
- *Analyses à la demande* du système de fichiers complet ou de dossiers ou fichiers individuels ;
- *Utilisation de technologies d'optimisation* lors de l'analyse d'objets dans le système de fichiers du serveur ;
- *Restauration du système après une attaque virale* ;
- *Évolutivité du paquet logiciel* en tenant compte des ressources système disponibles ;
- *Surveillance de la répartition de charge du serveur* ;
- *Création d'une liste de processus de confiance* dont l'activité serveur n'est pas contrôlée par le paquet logiciel ;
- *Administration distante* du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- *Enregistrement de copies de sauvegarde des objets infectés ou supprimés* en prévision d'une possible restauration ;
- *Mise en quarantaine d'objets suspects* ;
- *Envoi à l'administrateur de notifications sur des événements* pendant l'activité du logiciel ;
- *Enregistrement de rapports détaillés* ;
- *Mise à jour automatique* des bases du programme.

Kaspersky Open Space Security

Kaspersky Open Space Security est un paquet logiciel qui offre une nouvelle approche de la sécurité aux réseaux d'entreprise de toutes tailles, avec des systèmes de gestion centralisés et la prise en charge de poste distants et d'utilisateurs mobiles.

La suite contient quatre applications :

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

Les particularités de chaque programme figurent ci-après.

Kaspersky WorkSpace Security est un programme de protection centralisé des postes de travail situés à l'intérieur et à l'extérieur de réseaux d'entreprise contre toutes les menaces contemporaines de l'Internet (virus, logiciels espions, piratages et courrier indésirable).

Fonctions et caractéristiques :

- Protection complète contre les virus, les logiciels espions, les tentatives de piratage et le courrier indésirable ;
- Défense proactive contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- Restauration des modifications malveillantes dans le système ;
- Protection contre les tentatives de fraude et le publipostage indésirable ;
- Répartition dynamique des ressources pendant les analyses complètes du système ;
- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- Compatibilité Cisco® NAC (Network Admission Control) ;
- Analyse des messages et du trafic Internet en temps réel ;
- Interdiction des fenêtres indépendantes et des bandeaux publicitaires pendant la navigation sur Internet ;
- Fonctionnement sécurisé sur tous types de réseaux, y compris les réseaux Wi-Fi ;
- Outils de création d'un disque de secours permettant de restaurer le système après une offensive virale ;
- Système complet de rapports sur l'état de la protection ;
- Mises à jour automatique des bases ;

- Prise en charge complète des systèmes d'exploitation 64 bits ;
- Optimisation des performances du programme sur les portables (technologie Intel® Centrino® Duo) ;
- Fonctions de désinfection à distance (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security offre une protection optimale des ressources d'information de votre société contre les menaces contemporaines de l'Internet. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichier contre tous les types de virus, de chevaux de Troie et de vers, il protège contre les offensives virales et il sécurise vos données, tout en offrant aux utilisateurs un accès instantané aux ressources d'information du réseau.

Fonctions et caractéristiques :

- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- Compatibilité Cisco® NAC (Network Admission Control) ;
- Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet ;
- La technologie iSwift évite les analyses répétées de fichiers dans le réseau ;
- Répartition de charge entre les processeurs du serveur ;
- Mise en quarantaine d'objets suspects depuis les postes de travail ;
- Restauration des modifications malveillantes dans le système ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- Analyse des messages et du trafic Internet en temps réel ;
- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- Protection des utilisateurs de réseaux Wi-Fi ;
- Autodéfense contre les logiciels malveillants ;
- Mise en quarantaine d'objets suspects ;

- Mises à jour automatique des bases.

Kaspersky Enterprise Space Security

Ce logiciel dispose de composants de protection pour les postes de travail et les serveurs liés, contre toutes les menaces contemporaines de l'Internet. Il supprime les virus des messages et préserve vos données tout en fournissant un accès sécurisé aux ressources réseau des utilisateurs.

Fonctions et caractéristiques :

- Protection des postes de travail et des serveurs de fichiers contre les virus, les chevaux de Troie et les vers ;
- Protection des serveurs de messagerie Sendmail, Qmail, Postfix et Exim ;
- Analyse de tous les messages sur Microsoft Exchange Server, y compris les dossiers partagés ;
- Traitement des messages, des bases de données et des autres objets sur serveurs Lotus Domino ;
- Protection contre les tentatives de fraude et le publipostage indésirable ;
- Prévention des publipostages et des épidémies virales ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- Compatibilité Cisco ® NAC (Network Admission Control) ;
- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- Fonctionnement sécurisé sur les réseaux Wi-Fi ;
- Analyse du trafic Internet en temps réel ;
- Restauration des modifications malveillantes dans le système ;
- Répartition dynamique des ressources pendant les analyses complètes du système ;
- Mise en quarantaine d'objets suspects ;

- Système complet de rapports sur l'état de la protection ;
- Mises à jour automatique des bases.

Kaspersky Total Space Security

Cette solution surveille tous les flux de données en entrée et sortie (messages, Internet et toutes les interactions réseau). Cette solution contient des composants de protection des postes de travail fixes ou de périphériques mobiles, qui protège les données tout en offrant aux utilisateurs un accès sécurisé aux ressources d'information de la société et à Internet, et des communications par messagerie sécurisées.

Fonctions et caractéristiques :

- Protection complète contre les virus, les logiciels espions, les tentatives de piratage et le courrier indésirable à tous les niveaux du réseau d'entreprise, depuis les postes de travail jusqu'aux passerelles Internet ;
- Défense proactive des postes de travail contre les nouveaux programmes malveillants dont la signature n'a pas encore été ajoutée à la base de données ;
- Protection de serveurs de messagerie et de serveurs liés ;
- Analyse du trafic Internet (HTTP/FTP) qui circule sur le réseau local en temps réel ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- Interdiction de connexions des postes de travail infectés ;
- Prévention contre les offensives virales ;
- Génération centralisée de rapports sur la protection ;
- Administration distante du paquet logiciel, y compris l'installation, la configuration et la gestion à distance ;
- Compatibilité Cisco® NAC (Network Admission Control) ;
- Prise en charge de boîtiers à serveur proxy intégré ;
- Filtrage du trafic Internet moyennant une liste de serveurs de confiance, de types d'objets et de groupes d'utilisateurs ;
- La technologie iSwift évite les analyses répétées de fichiers dans le réseau ;
- Répartition dynamique des ressources pendant les analyses complètes du système ;

- Pare-feu personnel doté d'un système de détection des intrusions et d'alertes en cas de piratage réseau ;
- Fonctionnement sécurisé sur tous types de réseaux, y compris les réseaux Wi-Fi ;
- Protection contre les tentatives de fraude et le publipostage indésirable ;
- Fonctions de désinfection à distance (Intel® Active Management, Intel® vPro™) ;
- Restauration des modifications malveillantes dans le système ;
- Autodéfense contre les logiciels malveillants ;
- Prise en charge complète des systèmes d'exploitation 64 bits ;
- Mises à jour automatique des bases.

Kaspersky Security for Mail Servers

Ce logiciel permet de protéger des serveurs de messagerie et des serveurs liés contre les logiciels malveillants et le courrier indésirable. Le logiciel contient une application pour la protection de tous les serveurs de messagerie standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim) et permet également de configurer une passerelle de messagerie dédiée. La solution comprend :

- [Kaspersky Administration Kit.](#)
- [Kaspersky Mail Gateway.](#)
- [Kaspersky Anti-Virus pour Lotus Notes/Domino.](#)
- [Kaspersky Anti-Virus pour postes de travail et serveurs de fichiers Microsoft Exchange.](#)
- [Kaspersky Anti-Virus pour Linux Mail Server.](#)

Les caractéristiques comprennent :

- Protection fiable contre les logiciels malveillants ou potentiellement dangereux ;
- Filtrage des pollupostages indésirables ;
- Analyse des pièces jointes dans les messages entrants et sortants ;
- Analyse antivirus de tous les messages sur Microsoft Exchange Server y compris les dossiers partagés ;

- Traitement des messages, des bases de données et des autres objets sur serveurs Lotus Notes/Domino ;
- Filtrage des messages par type de pièce de jointe ;
- Mise en quarantaine des objets suspects ;
- Système convivial d'administration du logiciel ;
- Prévention contre les offensives virales ;
- Surveillance de l'état du système de protection à l'aide de notifications ;
- Système de rapports sur le fonctionnement du programme ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;
- Mises à jour automatique des bases.

Kaspersky Security for Internet Gateways

Ce logiciel offre un accès Internet sécurisé à tous les employés d'une entreprise, en supprimant automatiquement les logiciels malveillants ou à risque dans les données HTTP/FTP entrantes. La solution comprend :

- [Kaspersky Administration Kit.](#)
- [Kaspersky Anti-Virus for Proxy Server.](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server.](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1.](#)

Les caractéristiques comprennent :

- Protection fiable contre les logiciels malveillants ou potentiellement dangereux ;
- Analyse du trafic Internet (HTTP/FTP) en temps réel ;
- Filtrage du trafic Internet moyennant une liste de serveurs de confiance, de types d'objets et de groupes d'utilisateurs ;
- Mise en quarantaine des objets suspects ;
- Système convivial d'administration ;
- Système de rapports sur le fonctionnement du programme ;
- Prise en charge de boîtiers à serveur proxy intégré ;
- Évolutivité du paquet logiciel en tenant compte des ressources système disponibles ;

- Mises à jour automatique des bases.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle de pointe, conçue pour permettre aux organisations équipées de réseaux de petite ou moyenne taille, de lutter contre le fléau des messages indésirables (« spam », pourriel). Le produit combine les technologies révolutionnaires d'analyse linguistique avec toutes les méthodes modernes de filtrage des messages électroniques, y compris les listes noires de DNS et la reconnaissance de structures formelles. Sa combinaison unique de services permet aux utilisateurs d'identifier et d'éliminer près de 95% du trafic indésirable.

Kaspersky® Anti-Spam se comporte comme un barrage contre le courrier indésirable, installé à l'entrée du réseau, qui analyse les flux de courrier entrant à la recherche de spam. Le logiciel prend en charge tous les systèmes de messagerie, et peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées pour le filtrage, à partir des échantillons fournis par les spécialistes du laboratoire linguistique de notre Société. Les bases de données sont mises à jour toutes les 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper for SMTP assure une analyse anti-virus à haute vitesse du trafic SMTP sur des serveurs exploités sous les versions Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

L'application se présente comme un complément logiciel (plug-in) et réalise l'analyse anti-virus et le traitement préventif de tous les messages entrants et sortants en temps réel.

A.2. Comment nous contacter

Si vous avez des questions, des commentaires ou des suggestions, adressez-vous à nos revendeurs ou directement à Kaspersky Lab. Nous serons heureux de vous renseigner sur notre produit par téléphone ou par courrier électronique. Toutes vos recommandations et suggestions sont soigneusement étudiées et prises en compte.

Support technique	Pour le service d'assistance technique, visitez : http://www.kaspersky.com/supportinter.html Helpdesk : www.kaspersky.com/helpdesk.html
-------------------	---

Informations générales	WWW :http://www.kaspersky.com/fr http://www.viruslist.com/fr E-mail : info@kaspersky.com
---------------------------	--

ANNEXE B. CONTRAT DE LICENCE

Contrat de licence pour utilisateur standard

NOTE À TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT CE CONTRAT DE LICENCE (« LICENCE »), CONCERNANT LA LICENCE DE KASPERSKY MOBILE SECURITY (« LOGICIEL ») FABRIQUÉ PAR KASPERSKY LAB (« KASPERSKY LAB »).

SI VOUS AVEZ ACHETÉ CE LOGICIEL VIA INTERNET, EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITÉ DE CES TERMES, CLIQUEZ SUR LE BOUTON INDICANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETÉ CE LOGICIEL SOUS FORME PHYSIQUE, EN OUVRANT LE SCELLÉ DU CD/DVD, VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE VOUS ENGAGER SUR CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITÉ DES TERMES DE CE CONTRAT, N'OUVREZ PAS LE BOÎTIER DU CD/DVD, NE TÉLÉCHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

Conformément à la législation, dans le cas d'un LOGICIEL KASPERSKY destiné à des consommateurs particuliers et acheté en ligne sur le site Internet de KASPERSKY LAB OU DE SES PARTENAIRES, le consommateur dispose de QUATORZE (14) jours ouvrables à partir de la date de réception du produit pour le renvoyer au revendeur et réclamer son échange ou le remboursement, sous réserve que le logiciel ne soit PAS ouvert.

Dans le cas d'un Logiciel Kaspersky destiné à des consommateurs particuliers et qui n'a pas été acheté en ligne sur Internet, ce logiciel ne pourra être ni retourné ni échangé, sauf clauses contraires prévues par les revendeurs partenaires. Dans ce cas, Kaspersky LAB ne sera pas lié par les clauses de ses revendeurs partenaires.

LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'À L'ACHETEUR INITIAL.

Toutes les références au « Logiciel » apparaissant dans le présent contrat de licence incluent la clé d'activation (Fichier Clé d'Identification) qui sera fournie par Kaspersky Lab comme faisant partie Kaspersky Anti-Virus 7.0.

1. Licence de droits. Sous réserve du paiement du prix d'achat du logiciel et d'acceptation des termes de la présente Licence d'utilisation, Kaspersky Lab

vous autorise à utiliser une copie unique et non transférable de la version spécifiée de ce logiciel et de la documentation (la « Documentation ») selon les termes de ce Contrat uniquement pour un usage interne à l'entreprise. Vous pouvez installer une copie du Logiciel sur un seul ordinateur.

1.1 Utilisation. Le Logiciel est distribué sous licence individuelle, il ne peut pas être utilisé sur plus d'un ordinateur ou par plus d'un utilisateur à la fois, sauf stipulation contraire dans cette Section.

1.1.1 Le logiciel est « utilisé » sur un ordinateur lorsqu'il est chargé dans la mémoire temporaire (RAM, mémoire vive ou d'accès aléatoire) ou installé dans la mémoire permanente (disque dur, CD/DVD-ROM ou autre périphérique de stockage) de l'ordinateur. La présente licence vous autorise à réaliser une copie unique du logiciel dans son intégralité à des fins de sauvegarde, à condition que les copies contiennent toutes les notices de propriété du Logiciel. Vous devrez garder une trace de toute copie du logiciel et de sa documentation et prendre toutes les précautions raisonnables contre des copies ou des utilisations non autorisées.

1.1.2 Le logiciel protège le dispositif contre les virus et les attaques réseau dont les signatures sont présentes dans les bases antivirus disponibles sur les serveurs de Kaspersky Lab.

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

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

1.1.5 Il vous est interdit ainsi qu'à des tiers (sauf présente autorisation expresse), de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, ou d'en produire des applications dérivées.

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

1.1.7 Il est interdit de fournir le code d'activation ou le fichier clé de licence à des tiers, ou de donner accès à des tiers au code d'activation ou à la clé de licence. Le code d'activation et la clé de licence sont des données confidentielles.

1.1.8 Kaspersky Lab peut demander à l'Utilisateur d'installer la dernière version du Logiciel (dernière version ou dernier pack de maintenance).

1.1.9 Vous ne pourrez pas utiliser ce Logiciel avec des outils automatiques, semi-automatiques ou manuels conçus pour créer des signatures de virus, des routines de détection de virus ou tout autre programme de détection de code malveillant ou de données malveillantes.

2. Assistance technique.

(i) Kaspersky Lab fournira une assistance technique (« Services de support ») comme décrit ci-dessous pour une durée spécifiée par le Fichier clé de licence, tel qu'indiqué dans la fenêtre « Service », à compter de la date d'achat, sous réserve que :

- (a) les frais de l'assistance technique en cours aient été payés, et :
- (b) vous remplissiez le Formulaire d'inscription au Services de support fourni avec le produit ou disponible sur le site Web de Kaspersky Lab, et qui nécessitera la saisie du code d'activation fourni par Kaspersky Lab avec le présent Contrat de Licence. Il restera à l'entière discrétion de Kaspersky Lab de juger si vous remplissez les conditions d'accès prévues aux services de support technique.

Les services de support seront disponibles après l'activation du Logiciel. Le service d'Assistance technique de Kaspersky Lab est également autorisé à demander à l'Utilisateur final un complément d'identification avant de fournir ses prestations.

Avant toute activation du Logiciel et/ou obtention de l'Identificateur d'Utilisateur final (ID Client) le service Support n'assure que l'assistance nécessaire à l'activation du Logiciel et à l'inscription de l'Utilisateur final.

(ii) En remplissant le Formulaire d'Inscription au Support technique, vous acceptez les termes de la Politique de confidentialité de Kaspersky Lab disponible sur www.kaspersky.com/privacy, et vous consentez explicitement au transfert de données vers d'autres pays que le vôtre en accord avec les termes de la Politique de confidentialité.

(iii) Le support technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iv) Les « Services de support technique » signifient :

- (a) Mises à jour quotidiennes de la base anti-virus ;
- (b) Mises à jour logicielles gratuites, y compris les mises à niveau de la version ;
- (c) Support technique par Internet et par téléphone auprès de votre distributeur ou revendeur ;

- (d) Mises à jour des outils de détection et d'éradication antivirus par intervalles de 24 heures
- (v) Les services de Support ne sont assurés que si la dernière version du Logiciel (y compris les packs de maintenance) disponible sur le site officiel de Kaspersky Lab (<http://www.kaspersky.com/fr>) est installée dans votre ordinateur.

3. Droits de propriété. Le logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les droits de propriété, brevets, marques déposées et autres droits de propriété intellectuelle applicables. Le fait que vous en possédiez une copie et que vous l'ayez installée ne vous donne aucun droit de propriété intellectuelle sur le logiciel.

4. Confidentialité. Vous acceptez que le Logiciel et la Documentation, y compris la conception et structure des logiciels individuels constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez pas et ne fournirez en aucun cas ces informations confidentielles sous quelque forme que ce soit à un tiers sans l'autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables afin de protéger cette information confidentielle, ainsi que pour conserver la sécurité du code d'activation.

5. Limite de garantie.

- (i) Kaspersky Lab garantit, pour une durée de six (6) mois suivant le téléchargement ou l'installation du logiciel acheté sur un support physique, le fonctionnement du Logiciel comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.
- (ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et sa Documentation répondront à vos besoins et que leur utilisation sera exempte d'interruptions ou d'erreurs.
- (iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaitra tous les virus connus ou qu'il n'affichera pas de message de détection erroné à propos d'un virus.
- (iv) La responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement au paragraphe (i), et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un représentant au cours de la période de garantie. Vous devrez fournir toutes les informations nécessaires au fournisseur pour remédier à tout problème éventuel.

- (v) La garantie décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.
- (vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (v) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par disposition légale, usage ou toute autre raison, qui sont toutes exclues ici (y compris, sans limitation, les conditions, garanties ou autres termes qualitatifs relatifs à la satisfaction, adéquation à l'utilisation ou à des compétences normales).

6. Limite de responsabilités.

- (i) Rien dans le présent Contrat ne saurait exclure ou limiter la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction, (b) de décès ou de dommages physiques résultant d'infractions aux lois en vigueur ou du non-respect des termes du présent Contrat ou © de toute infraction aux obligations impliquées par la loi.
- (ii) Selon les termes du paragraphe (i) ci-dessus, Kaspersky Lab ne pourra être tenu pour responsable (suite au contrat, à un acte dommageable, à une restitution ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres) :
 - (a) Perte de revenus ;
 - (b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats) ;
 - (c) Perte de moyens de paiement ;
 - (d) Perte d'économies prévues ;
 - (e) Perte de marché ;
 - (f) Perte d'opportunités commerciales ;
 - (g) Perte d'image ;
 - (h) Perte de réputation ;
 - (i) Perte, dommage ou corruption des données ; ou :
 - (j) Tout dommage ou toute perte qu'ils soient directs ou indirects ou causés de quelque façon que ce soit (y compris, pour éviter le doute, les dommages ou pertes prévus aux paragraphes (ii), (a) jusqu'à (ii), (i).
- (iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (suite au contrat, à un acte dommageable, à une restitution ou autre)

survenant lors de la fourniture du Logiciel n'excédera en aucun cas un montant égal au prix d'achat du Logiciel.

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

Quand vous utilisez un logiciel de démonstration, vous ne bénéficiez pas du Support technique spécifié à l'article 2 de ce CLUF, et vous n'avez pas le droit de vendre la copie en votre possession à d'autres parties.

Vous êtes autorisé à utiliser le logiciel à des fins de démonstration pendant la durée spécifiée dans le fichier clé de licence à compter de son activation (cette durée est indiquée dans la fenêtre Service de l'interface du logiciel).