

KASPERSKY LAB

---

Kaspersky Mobile Security 7.0  
Enterprise Edition

GUIDE DE  
L'ADMINISTRATEUR

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE  
EDITION

---

# Guide de l'administrateur

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

Date de révision : Octobre, 2009

---

# Table des matières

CHAPITRE 1. GESTION AVEC KASPERSKY ADMINISTRATION KIT .....	5
CHAPITRE 2. DEPLOIEMENT D'APPLICATIONS .....	8
2.1. Création d'un paquet d'installation .....	8
2.2. Installation de l'application par le biais d'une tâche d'installation à distance .....	9
2.3. Installation de l'application par le biais d'un SMS .....	20
2.4. Ajout d'un périphérique au groupe .....	22
CHAPITRE 3. ADMINISTRATION DES STRATEGIES .....	25
3.1. Création d'une stratégie .....	25
3.2. Examen et modification des paramètres de la stratégie .....	33
3.2.1. Informations sur l'application .....	34
3.2.2. Affichage des résultats de l'application de la stratégie .....	35
3.2.3. Paramètres de consignation des événements de l'application .....	36
3.2.4. Paramètres d'analyse antivirus .....	38
3.2.5. Paramètres de protection en temps réel .....	39
3.2.6. Sélection de la source de mises à jour des bases de l'application .....	40
3.2.7. Configuration du module Anti-Spam .....	41
3.2.8. Configuration du module Antivol .....	43
3.2.9. Configuration de paramètres avancés .....	44
CHAPITRE 4. CONTROLE DES PARAMETRES D'APPLICATION .....	46
4.1. Informations sur l'application .....	47
4.2. Informations sur les paramètres d'analyse antivirus .....	48
4.3. Information sur la protection en temps réel .....	49
4.4. Informations sur la source de mises à jour .....	50
4.5. Informations sur les paramètres du module Anti-Spam .....	51
4.6. Informations sur les paramètres du module Antivol .....	52
4.7. Informations sur les paramètres avancés .....	53
4.8. Affichage des détails de la clé .....	54
4.9. Affichage d'événements .....	55

ANNEXE A. KASPERSKY LAB .....	57
ANNEXE B. CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB .....	59

---

# CHAPITRE 1. GESTION AVEC KASPERSKY ADMINISTRATION KIT

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

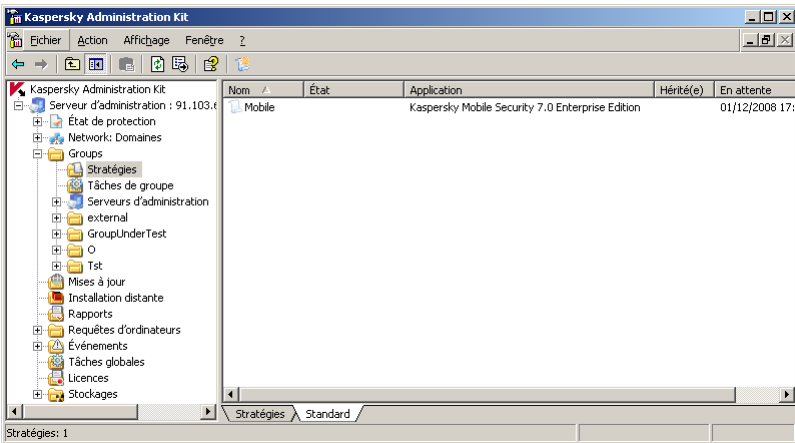


Figure 1. Console d'administration de Kaspersky Administration Kit

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

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

**Une stratégie** est un ensemble de paramètres de Kaspersky Mobile Security associés à un groupe du réseau logique. Les stratégies sont transférées sur le périphérique mobile lors d'une synchronisation de tout type du périphérique avec le Serveur d'administration.

**Note**

Pour vous assurer que Kaspersky Administration Kit détecte les périphériques mobiles, ouvrez l'onglet **Paramètres** des propriétés du serveur d'administration et cochez la case **Ouvrir le port pour les dispositifs mobiles**.

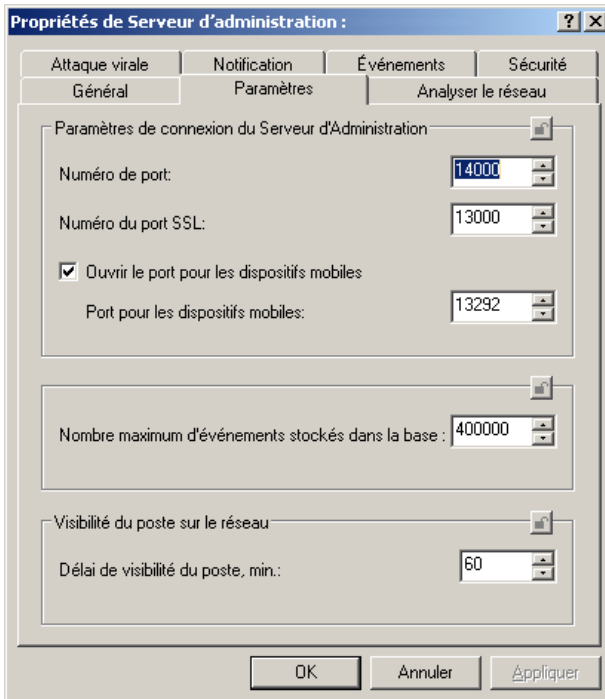


Figure 2. **Paramètres** (onglet)

**Remarque :**

Les périphériques mobiles se connectent au Serveur d'administration avec le protocole SSL. Pour établir ce type de connexion, un certificat est nécessaire sur le serveur.

Pour créer un certificat pour périphériques mobiles :

1. Ouvrez le dossier d'installation de Kaspersky Administration Kit.
2. Exécutez l'utilitaire *klmblcrt.exe*.
3. Spécifiez l'adresse du serveur d'administration dans la fenêtre de l'Assistant pour la création d'un certificat (Figure 3)

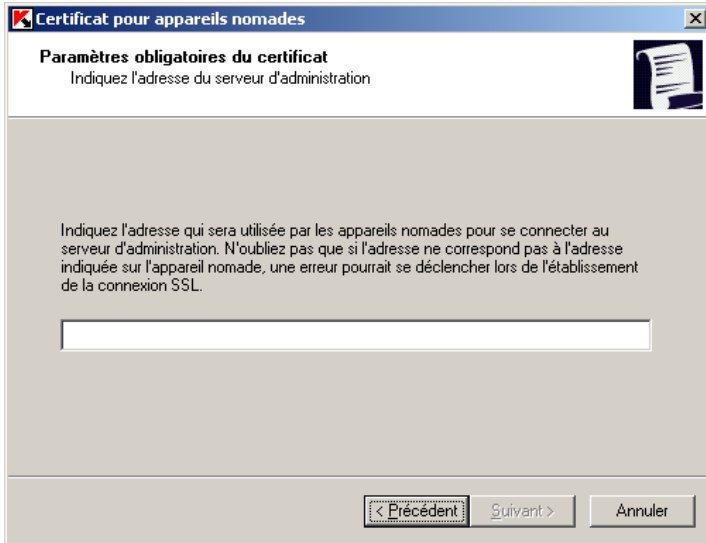


Figure 3. Création d'un certificat pour périphériques mobiles

4. Suivez les instructions de l'Assistant pour la création du certificat.

---

# CHAPITRE 2. DEPLOIEMENT D'APPLICATIONS

## Remarque :

Une installation à distance de Kaspersky Mobile Security est impossible si le plugin (complément logiciel) d'administration de Kaspersky Mobile Security n'a pas été installé sur le poste administrateur. Le paquet d'installation du plugin est inclus dans le kit de distribution de Kaspersky Mobile Security et se trouve sous le dossier Plugin.

Cette section explique l'installation de Kaspersky Mobile Security par le biais d'une tâche d'installation à distance, ou d'un message SMS.

## 2.1. Création d'un paquet d'installation

L'installation à distance de l'application est effectuée à l'aide d'un paquet d'installation.

*Pour créer un paquet d'installation :*

1. Connectez-vous au serveur d'administration.
2. Sélectionnez l'entrée **Installation distante** dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez la commande **Nouveau** → **Paquet d'installation** ou son équivalent dans le menu **Action**. Ceci permet de lancer l'assistant. Suivez ses instructions.
3. Vous pourrez spécifier le nom du paquet d'installation et l'application à installer à l'étape suivante (Figure 4).
4. Dans la liste déroulante, choisissez l'option : **Générer le paquet d'application Kaspersky Lab**. Utilisez **Parcourir** pour sélectionner le fichier contenant la description de l'application (le fichier possède une extension **.kpd** et accompagne le paquet d'installation de l'application). Comme résultat, les champs Nom de l'application et Version de l'application seront automatiquement renseignés.

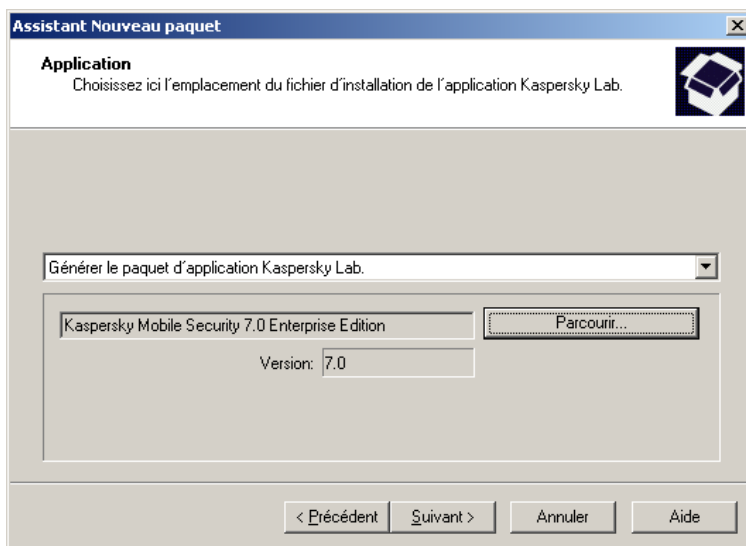


Figure 4. Création d'un paquet d'installation - Choix de l'application à installer

5. Après ceci, un ensemble de fichiers nécessaires pour installer l'application sur les périphériques mobiles sera téléchargée dans un dossier public du Serveur d'administration.

À la fin de l'Assistant, le nouveau paquet d'installation sera ajouté sous l'entrée **Installation distante** et affichée dans le panneau de résultats.

## 2.2. Installation de l'application par le biais d'une tâche d'installation à distance

L'installation de l'application par le biais d'une tâche d'installation à distance est utilisée quand les périphériques mobiles sont connectés aux ordinateurs du réseau logique. L'installation de l'application s'effectue au moment où le périphérique est connecté à l'ordinateur.

Pour exécuter la tâche d'installation distante du logiciel sur les ordinateurs clients, deux méthodes sont possibles : *installation forcée* ou *installation par un script de démarrage*.

L'*installation forcée* est utilisée pour réaliser une installation distante du logiciel sur des ordinateurs clients spécifiques du réseau logique. Lors de l'exécution de la tâche, le Serveur d'administration recopie depuis le dossier public l'ensemble des fichiers nécessaires à l'installation vers chacun des ordinateurs clients, dans un dossier temporaire d'où il exécute le programme d'installation. Le serveur d'administration doit posséder des droits d'administration locaux sur les postes clients du réseau logique afin de pouvoir effectuer la tâche de désinstallation forcée avec succès. Cette méthode est recommandée pour l'installation d'applications sur des ordinateurs sous Microsoft Windows NT/2000/2003/XP compatibles avec cette caractéristique, ou sur des ordinateurs sous Microsoft Windows 98/Me, sur lesquels l'agent réseau est installé.

**Remarque :**

Si le serveur d'administration et un client communiquent entre eux par Internet, ou si la connexion est protégée par un pare-feu, il n'est pas possible d'utiliser de dossiers partagés pour transférer des données. Dans ce cas, l'agent réseau doit être utilisé pour télécharger les fichiers d'installation de l'application sur le client. L'installation de l'Agent réseau sur ces ordinateurs doit se faire en local.

La seconde méthode, l'*installation par un script de démarrage*, permet d'affecter l'exécution de la tâche d'installation à distance à un compte utilisateur (ou à des comptes utilisateurs) en particulier. Après l'exécution de cette tâche, les scripts de démarrage des utilisateurs spécifiés contiennent un enregistrement pour l'exécution de l'installateur se trouvant dans le dossier partagé du Serveur d'administration. Pour la bonne exécution de cette tâche, le compte utilisé pour son exécution ou le Serveur d'administration doivent avoir des droits de modification des scripts de démarrage dans la base du contrôleur du domaine. Ces droits sont accordés à administrateur du domaine, qui doit lancer la tâche ou le Serveur d'administration lui-même. Ainsi, quand l'utilisateur ouvre une session sur le domaine, il se produit un essai d'installation de l'application sur l'ordinateur client utilisé par cet utilisateur. Cette méthode est recommandée pour l'installation d'applications Kaspersky Lab sur des ordinateurs Microsoft Windows 98/ME.

**Remarque :**

Pour une exécution réussie de la tâche d'installation à distance par le biais d'un script de démarrage, les utilisateurs ciblés par les scripts doivent posséder des droits d'administrateur local sur leurs ordinateurs.

Les tâches de groupe pour l'installation distante du logiciel sur des ordinateurs clients ne peuvent être exécutées que par la méthode d'installation forcée. Lors de la création d'une tâche globale, vous pouvez sélectionner la méthode souhaitée : *installation forcée* ou *installation par un script de démarrage*.

Pour créer une tâche globale d'installation à distance moyennant la méthode d'installation forcée :

1. Connectez-vous au serveur d'administration.
2. Sélectionnez l'entrée **Tâches globales** dans l'arborescence de console, ouvrez le menu contextuel et sélectionnez la commande **Nouveau/Tâche** ou son équivalent dans le menu **Action**. Ceci permet de lancer l'assistant. Suivez ses instructions.
3. Indiquez le nom de tâche.
4. Lors du choix de l'application et du type de tâche (Figure 5) définissez les valeurs **Kaspersky Administration Kit** et **Tâche de déploiement d'application**, respectivement.
5. Spécifiez ensuite le paquet d'installation utilisé pour l'exécution de cette tâche (Figure 6). Sélectionnez le paquet créé pour ce Serveur d'administration ou créez un nouveau paquet avec **Nouveau**.

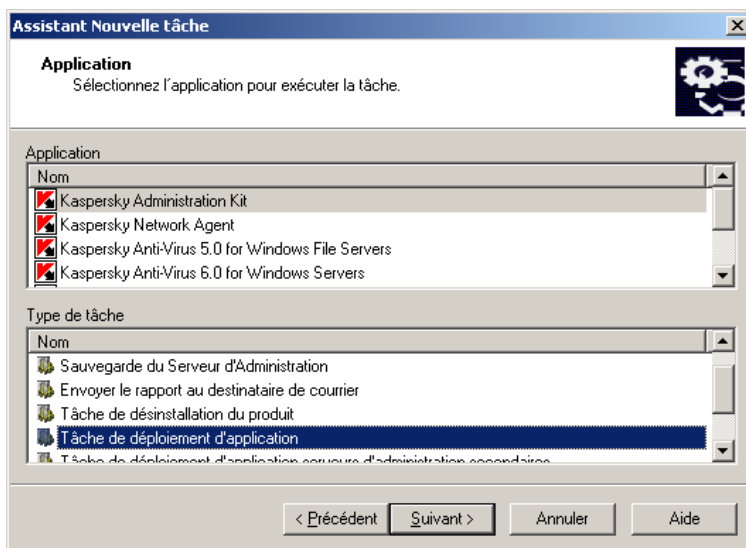


Figure 5. Choix du type de tâche

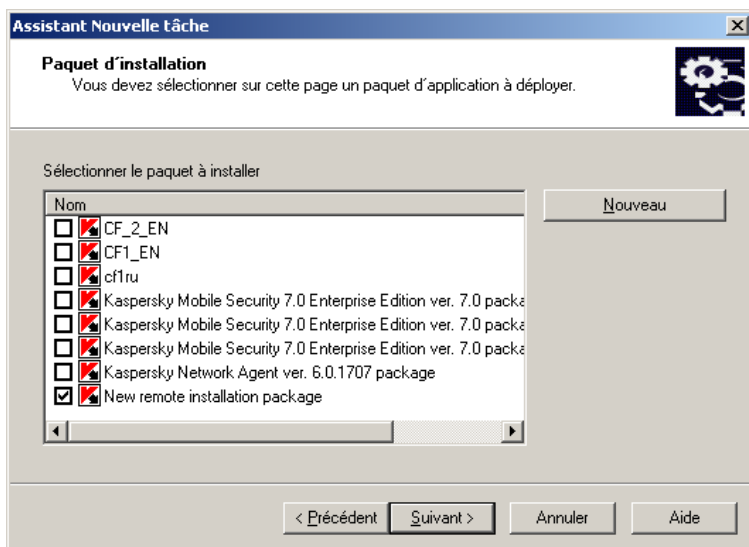


Figure 6. Choix du paquet d'installation à installer

6. À cette étape, sélectionnez **Installation par envoi** (Figure 7).

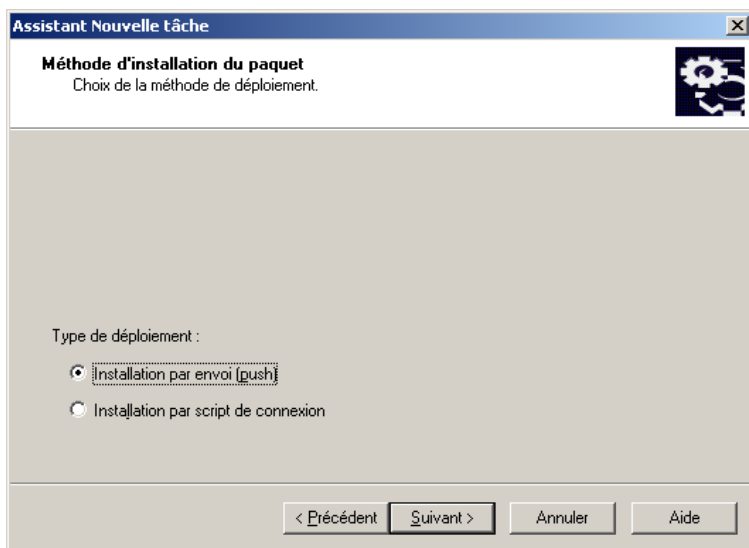


Figure 7. Choix du type d'installation

7. Dans cet écran de l'Assistant (Figure 8) vous pourrez spécifier d'autres options d'installation :

- Déterminer s'il est nécessaire de réinstaller l'application, si déjà installée sur l'ordinateur ;
- Cochez la case **Ne pas installer l'application sur des postes déjà équipés** si vous ne souhaitez pas réinstaller l'application à chaque fois (cochée par défaut). Dans ce cas, la tâche ne sera pas exécutée sur des ordinateurs où l'application a déjà été installée en local ou au cours d'une tâche d'installation distante précédente.

Si la case n'est pas cochée, la tâche d'installation à distance programmée sera exécutée jusqu'au nombre de tentatives prévues.

- Définir la méthode de distribution des fichiers requis pour l'installation de l'application sur les ordinateurs clients ;

Pour ce faire, dans le groupe de champs **Téléchargement le paquet d'installation** :

- Cochez la case **Utilisation des partages administratifs Microsoft Windows** si vous souhaitez recopier les outils de désinstallation de Windows à partir du dossier d'accès public sur les postes clients (par défaut). Cette option de téléchargement est recommandée si l'Agent réseau connecté au Serveur d'administration en particulier n'est pas installé sur l'ordinateur cible de l'installation.
- Cochez la case **Utilisation de l'agent d'administration** si vous souhaitez distribuer les fichiers sur les postes client à l'aide de l'agent d'administration installé sur chacun d'eux (cochée par défaut). L'Agent réseau doit être connecté au Serveur d'administration en particulier.
- Spécifiez le nombre maximum de postes client pouvant télécharger des informations depuis le serveur d'administration dans le champ **Nombre maximum de tâches simultanées**.
- Définissez le nombre de tentatives d'installation dans le cas d'une tâche planifiée, dans le champ **Nombre de tentatives**. Une nouvelle tentative est effectuée si des erreurs se produisent lors de l'installation précédente.

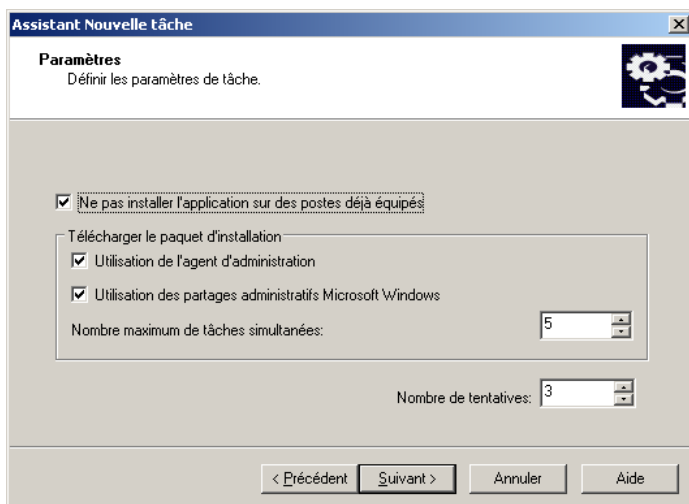


Figure 8. Options d'installation complémentaires

8. Au cours de cette étape (Figure 9) vous aurez le choix d'installer l'Agent réseau en même temps que l'application.

Si l'Agent réseau n'est pas installé sur l'ordinateur réseau auquel le périphérique mobile va être connecté, et vous souhaitez l'installer, incluez le Kit de distribution de l'Agent réseau dans le paquet de distribution de l'application.

Pour ce faire, cochez la case **Installer em même temps que l'agent d'administration** ainsi que le nom du paquet d'installation souhaité. Si nécessaire, créez un nouveau paquet d'installation avec **Créer**.

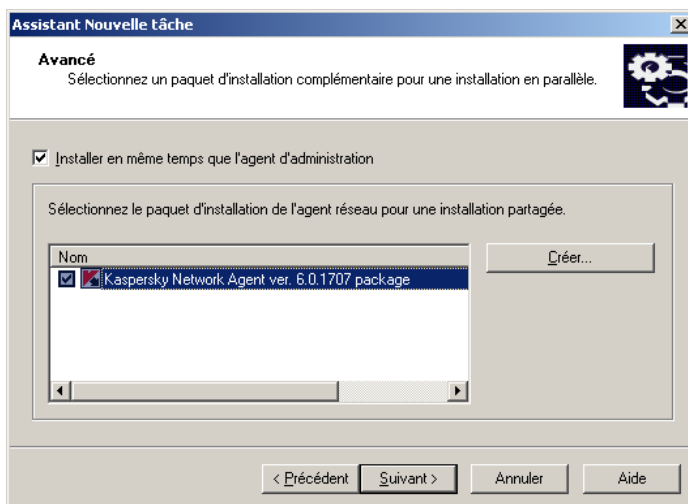


Figure 9. Choix de l'installation conjointe avec l'Agent réseau

9. Déterminez la méthode de sélection des ordinateurs cibles de la tâche à créer (Figure 10) :
  - **Je veux sélectionner des ordinateurs à partir du réseau de Windows.** Dans ce cas les ordinateurs cibles seront sélectionnés d'après les données obtenues par le Serveur d'administration par un sondage du réseau Windows de la société.
  - **Je veux définir les ordinateurs (comme adresse IP, nom NetBIOS ou nom DNS) manuellement.** Dans ce cas, les ordinateurs destinataires de l'installation seront sélectionnés manuellement.

Si les ordinateurs sont sélectionnés d'après les données obtenues par un sondage du réseau Windows, la liste sera créée dans un écran de l'Assistant (Figure 11) comme dans la procédure d'ajout d'ordinateurs au réseau logique (pour plus de détails, consultez le Guide de référence de Kaspersky Administration Kit). Vous pouvez sélectionner des ordinateurs clients du réseau logique (dossier **Groupe**) ou des ordinateurs non encore intégrés dans cette structure (dossier **Réseau**).

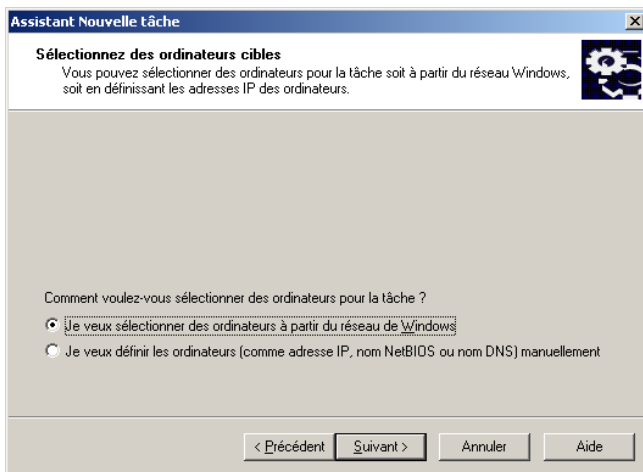


Figure 10. Choix des méthodes de sélection des ordinateurs clients

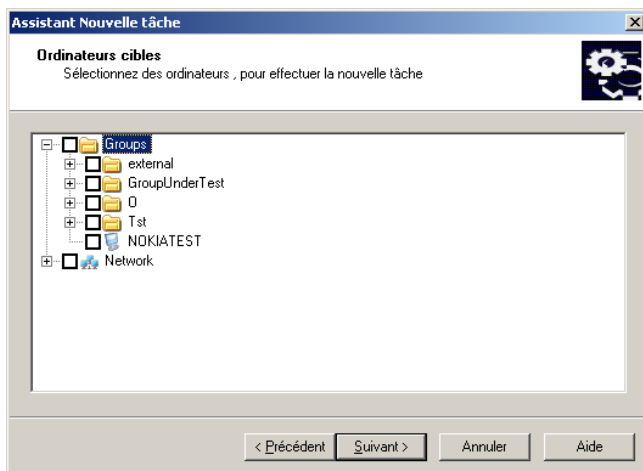


Figure 11. Création d'une liste d'ordinateurs cibles d'installation, d'après les données du réseau Windows

Si les ordinateurs sont sélectionnés manuellement, la liste est créée en indiquant les noms NetBIOS ou DNS, les adresses IP (ou intervalles d'adresses IP) des ordinateurs, ou en important leur liste à partir d'un fichier *.txt* contenant une adresse par ligne (Figure 12).

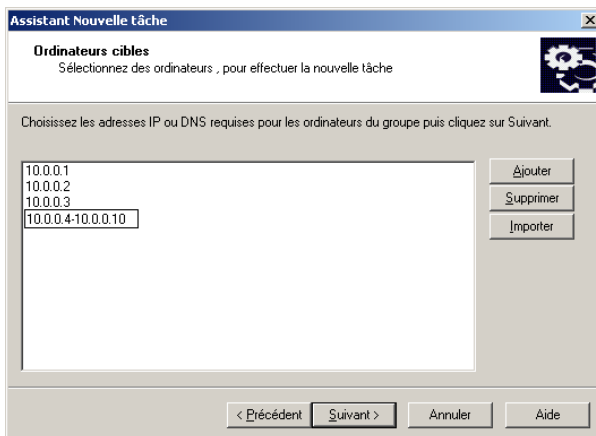


Figure 12. Création d'une liste d'ordinateurs cibles d'installation, d'après les adresses IP

10. Dans la fenêtre suivante de l'Assistant, définissez le compte utilisé pour démarrer la tâche d'installation à distance sur les ordinateurs (Figure 13).

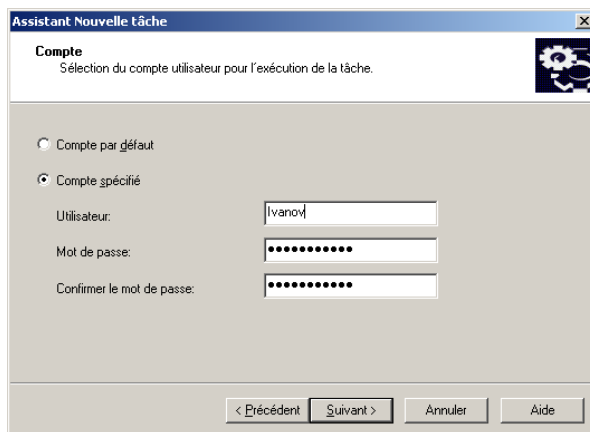


Figure 13. Sélection d'un compte

**Remarque :**

Le compte doit avoir des droits d'administrateur sur tous les ordinateurs sur lesquels vous prévoyez d'exécuter la tâche d'installation à distance.

Pour installer le logiciel sur des ordinateurs appartenant à d'autres domaines, une relation de confiance est nécessaire entre ces domaines et les domaines dans lesquels opère déjà le Serveur d'administration.

Sélectionnez l'une des options suivantes :

- **Compte par défaut** – si le Serveur d'administration est exécuté sous le compte d'un utilisateur du domaine et qu'il possède les droits nécessaires pour l'installation du logiciel.
- **Compte spécifié** – si le Serveur d'administration est exécuté sous un compte système ou si le compte du Serveur d'administration ne possède pas des droits d'exécution de tâches d'installation à distance.

**Remarque :**

Pour installer à distance le logiciel sur des ordinateurs qui n'appartiennent pas au domaine, la tâche d'installation à distance doit être exécutée sous un compte utilisateur possédant des droits d'administrateur sur ces ordinateurs.

Dans les zones inférieures, spécifiez les informations sur l'utilisateur dont le compte satisfait les conditions requises.

11. Planifiez ensuite l'exécution de la tâche (Figure 14).

- Sélectionnez le mode d'exécution souhaité pour la tâche dans la liste déroulante **Exécution planifiée** :
  - **Mode manuel.**
  - **Toutes les N heures.**
  - **Chaque jour.**
  - **Chaque semaine.**
  - **Chaque mois.**
  - **Une fois** (dans ce cas, la tâche d'installation à distance sera exécutée une seule fois, sans tenir compte du résultat de l'opération).

- **Immédiatement** (immédiatement après avoir créé la tâche, après la fin de l'Assistant).
- **Après la fin d'une autre tâche** (dans ce cas, la tâche d'installation à distance ne s'exécute qu'après la fin de la tâche spécifiée).
- Configurez la planification à l'aide du groupe de champs correspondant au mode sélectionné (pour plus de détails, consultez le Guide de référence de Kaspersky Administration Kit ).

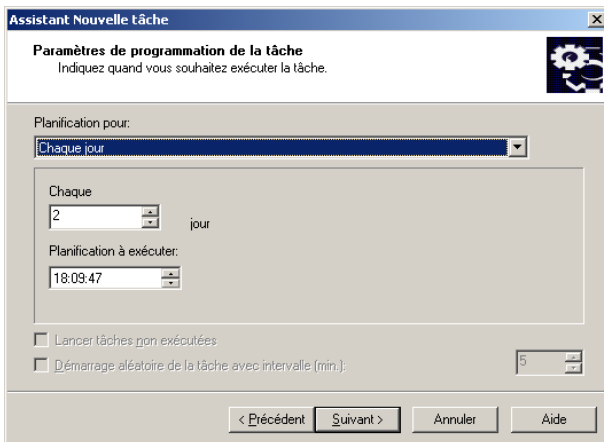


Figure 14. Exécution journalière de la tâche

À la fin de l'Assistant, la nouvelle tâche d'installation à distance sera ajoutée sous l'entrée **Tâches globales** et affichée dans le panneau de résultats.

*Pour démarrer la tâche d'installation à distance.*

sélectionnez **Tâches globales** dans l'arborescence de console, choisissez le paquet d'installation souhaité, puis choisissez **Démarrer** dans le menu contextuel ou dans le menu **Action**.

Une fois l'installation terminée, l'application *kmlisten.exe* s'exécutera en arrière-plan ; cette application surveille la connexion des périphériques mobiles à l'ordinateur. Lorsqu'un périphérique se connecte, une fenêtre s'ouvre (Figure 15) avec une invite pour sélectionner le périphérique sur lequel installer l'application.

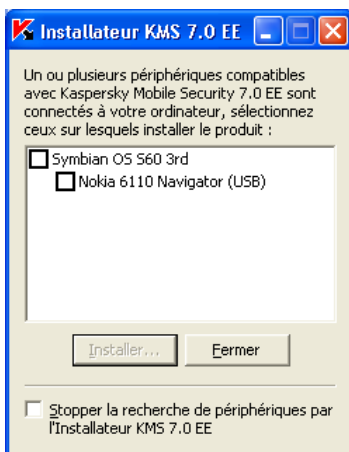


Figure 15. Fenêtre de l'utilitaire KMListen.exe

Cliquez sur **Installer** pour télécharger le paquet d'installation de l'application sur le périphérique mobile. Après la fin du téléchargement, suivez les instructions de l'Assistant qui s'exécute sur le périphérique.

## 2.3. Installation de l'application par le biais d'un SMS

L'installation de l'application sur des périphériques mobiles par le biais d'un SMS est utilisée quand les périphériques mobiles ne sont pas connectés aux ordinateurs du réseau logique.

### Remarque :

Pour pouvoir envoyer un SMS, vous devez disposer d'un modem GSM connecté au Serveur d'administration. En outre, le serveur doit être équipé de Microsoft .NET Framework version 2.0. Dans le cas contraire, l'envoi de messages SMS est impossible

*Pour installer l'application par le biais d'un SMS :*

1. Connectez-vous au serveur d'administration.
2. Sélectionnez l'entrée **Installation distante** dans l'arborescence de console.
3. Sélectionnez l'entrée **Propriétés** dans le menu contextuel du nouveau paquet d'installation de l'application.

4. Ouvrez l'onglet **Paramètres** puis cliquez sur **Installation par SMS**.
5. Dans cette boîte de dialogue (Figure 16) spécifiez les paramètres d'installation :
  - a) Spécifiez les paramètres de connexion modem dans la section **Modem GSM** : port et vitesse.
  - b) Dans le champ **URL du paquet de distribution**, spécifiez un serveur public disposant du paquet de distribution Kaspersky Mobile Security, à partir duquel l'application sera installée.

Par exemple :

[ftp://ftp.domain.com/distrib/KMS7EE/kmsecurity\\_70\\_15\\_beta.sis](ftp://ftp.domain.com/distrib/KMS7EE/kmsecurity_70_15_beta.sis)

ou :

[http://domain\\_name.ru/distrib/KMS7EE/kmsecurity\\_e\\_wm\\_sp\\_7\\_0\\_0\\_49\\_ru.cab](http://domain_name.ru/distrib/KMS7EE/kmsecurity_e_wm_sp_7_0_0_49_ru.cab).

- c) Créez une liste avec les numéros destinataires du message SMS. Pour ce faire, saisissez le numéro dans le champ de saisie puis cliquez sur **Ajouter numéro**. Le numéro saisi est ajouté à la liste.

Pour enregistrer la liste de numéros dans un fichier TXT, ou pour charger cette liste à partir d'un fichier préalablement créé, utilisez **Enregistrer dans un fichier** et **Ajouter depuis fichier**.

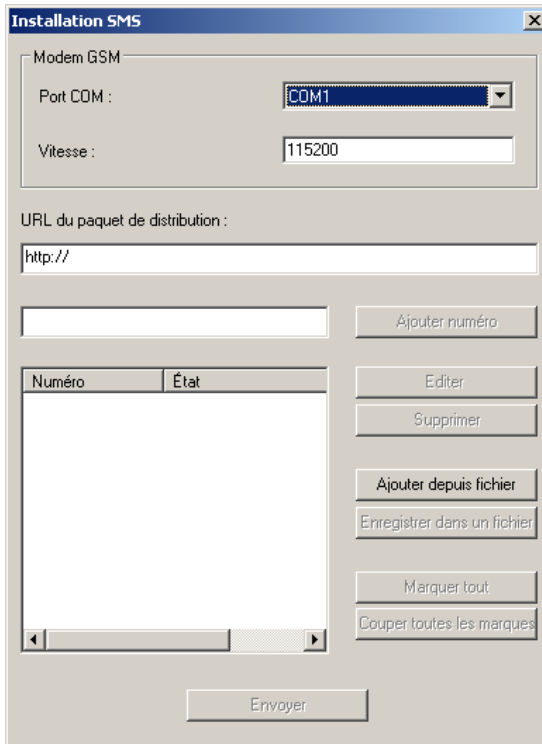


Figure 16. Paramètre d'envoi SMS

6. Cliquez sur **Envoyer** pour transmettre le SMS d'installation de Kaspersky Mobile Security aux numéros spécifiés.

Le message SMS avec le lien URL du paquet d'installation sera transmis aux périphériques mobiles dont les numéros figurent dans la liste. Lorsque le lien URL est ouvert, le paquet d'installation de l'application est téléchargé dans le périphérique. Après la fin du téléchargement, suivez les instructions de l'Assistant qui s'exécute sur le périphérique.

## 2.4. Ajout d'un périphérique au groupe

Après l'installation de Kaspersky Mobile Security, au cours du sondage du réseau, les périphériques mobiles sont tous ajoutés au domaine avec le nom

spécifié lors de la création du paquet d'installation (**PDAGroup**, par défaut). La stratégie créée pour les périphériques mobiles n'est pas appliquée.

**Note**

Un groupe pour périphériques mobiles s'affichera dans le conteneur **Réseau** (dans le mode d'affichage des domaines) après la première connexion du périphérique mobile avec le Serveur d'administration, si Kaspersky Mobile Security est installé sur le périphérique.

Pour déplacer le périphérique mobile dans le groupe d'administration, ouvrez la Console d'administration, ouvrez le conteneur **Réseau** et choisissez le mode d'affichage des domaines. Développez le groupe **PDAGroup** dans la liste des groupes réseau et faites glisser le périphérique mobile vers le groupe d'administration souhaité.

*Pour vous assurer de placer automatiquement les périphériques mobiles dans le groupe souhaité :*

1. Ouvrez le menu Console d'administration et ouvrez l'onglet **Réseau** container.
2. Sélectionnez **PDAGroup** and déployez la fenêtre des propriétés du groupe dans le menu contextuel.
3. Ouvrez l'onglet **Ordinateurs cibles** (Figure 17).

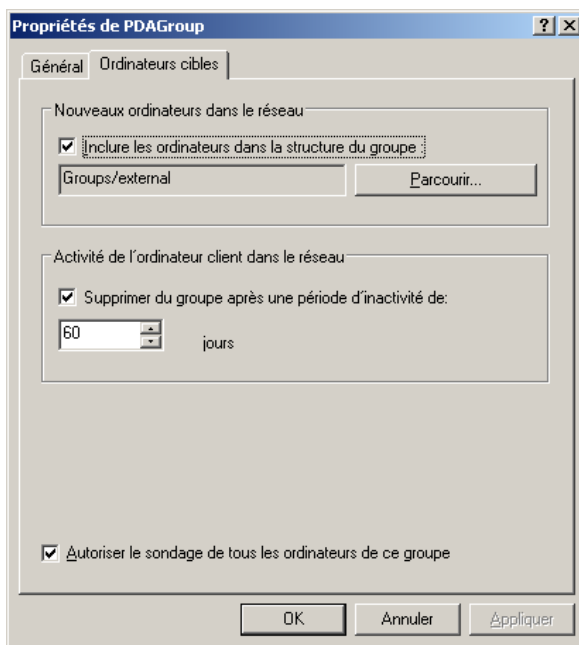


Figure 17. Propriétés du groupe

4. Cochez la case **Inclure les ordinateurs dans la structure du groupe** dans la section **Nouveaux ordinateurs dans le réseau**.
5. Cliquez sur **Parcourir** et dans la fenêtre ouverte, sélectionnez le groupe d'administration dans lequel seront placés les périphériques mobiles qui se connecteront à l'avenir.
6. Enregistrez les modifications.

---

# CHAPITRE 3. ADMINISTRATION DES STRATÉGIES

Cette section explique la création et la configuration de stratégies pour Kaspersky Mobile Security 7.0 Enterprise Edition.

La stratégie s'applique à l'application dans les cas suivants

- lors de la première connexion du périphérique au réseau ;
- lors des connexions suivantes du périphérique, si les paramètres de l'application ou de la stratégie ont été modifiés ;
- lors de synchronisation manuelle (Guide de l'utilisateur Kaspersky Mobile Security).


## 3.1. Création d'une stratégie

*Pour créer une stratégie, procédez de la manière suivante :*

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

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

**Remarque :**

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

## Etape 1. Saisie des données générales sur la stratégie

La première étape de l'Assistant est une introduction. La première fenêtre de l'Assistant permet de spécifier le nom de la stratégie (champ **Nom**), dans la seconde fenêtre, sélectionnez l'application **Kaspersky Mobile Security 7.0 Enterprise Edition** dans la liste déroulante **Nom d'application**. Pour appliquer les paramètres de stratégie immédiatement après leur définition, cochez la case **Stratégie active** dans la section **État de la stratégie** de la troisième fenêtre.

## Etape 2. Définition des paramètres d'analyse antivirus

Au cours de cette étape, vous devez définir les paramètres d'analyse antivirus du périphérique mobile : la couverture et la planification de l'analyse.

Dans la section **Paramètres d'analyse** (Figure 18) vous pouvez sélectionner les types de fichiers compris dans la couverture d'analyse et spécifier les actions appliquées aux objets infectés :

- **Analyser les exécutables uniquement** – analyse les fichiers de programmes exécutables uniquement.
- **Archives** – analyse les fichiers comprimés dans des archives.
- **Tenter de réparer les objets infectés** – tente de réparer les objets infectés rencontrés. Tous les objets ne peuvent pas être désinfectés.

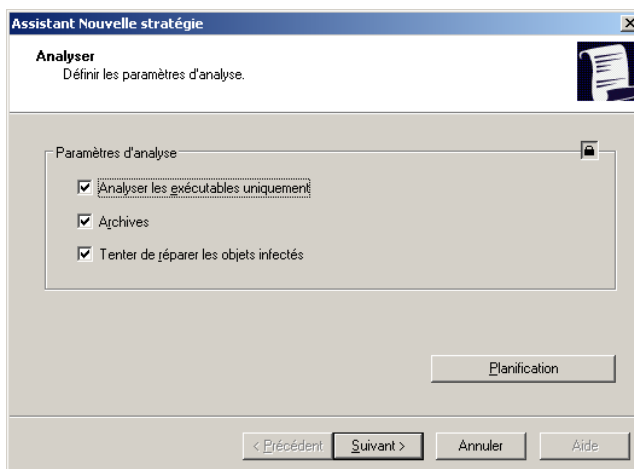


Figure 18. Paramètres de protection antivirus

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

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

### Étape 3. Configuration de la protection en temps réel

Cette étape permet de définir les paramètres de protection en temps réel du système de fichiers et de la mémoire du périphérique.

Cochez la case **Activer la protection en temps réel** (Figure 19) pour que l'application analyse tous les programmes exécutés et les fichiers ouverts par l'utilisateur.

Vous pouvez utiliser la section **Paramètres d'analyse** sélectionner les types de fichiers compris dans la couverture d'analyse :

- **Analyser les exécutable uniquement** – analyse les fichiers de programmes exécutable uniquement.

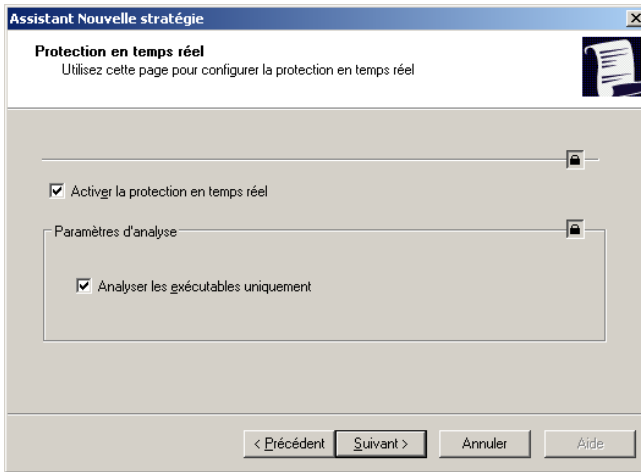


Figure 19. Paramètres de protection en temps réel

#### Etape 4. Sélection de la source de la mise à jour

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

La section **Source des mises à jour** (Figure 20) permet de spécifier les adresses de serveurs sources des mises à jour.

Pour s'assurer que les mises à jour se font depuis les serveurs de mise à jour de Kaspersky Lab, laissez vide le champ **Serveur de mise à jour**.

Pour utiliser une source différente, spécifiez l'adresse de la source des mises à jour dans la section **Source des mises à jour**. Il s'agit de l'adresse URL complète du fichier *mobile.xml*.

Par exemple, <http://domain.com/index/mobile.xml>.

**Remarque :**

La structure des dossiers dans la source de la mise à jour doit être identique à celle du serveur de mise à jour Kaspersky Lab.

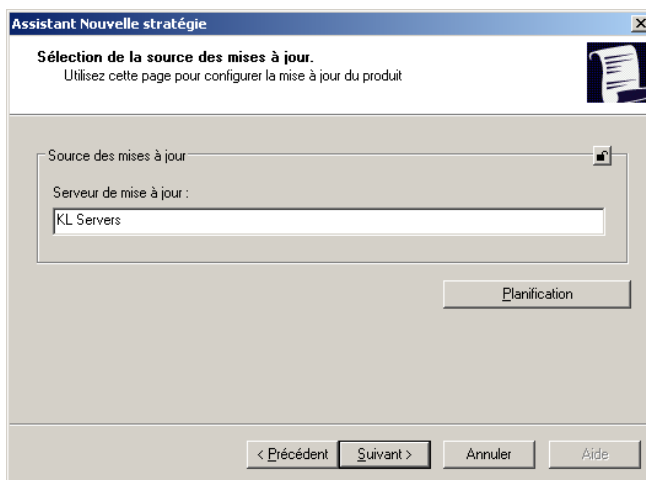


Figure 20. Sélection de la source de la mise à jour

En outre, vous pouvez planifier une mise à jour automatique. Pour ce faire, cliquez sur **Planification**. Ceci ouvrira une boîte de dialogue vous permettant de spécifier la fréquence d'analyse :

- **Manuel** – l'action est lancée manuellement par l'utilisateur.
- **Tous les jours** – l'action s'exécutera tous les jours. Spécifiez l'heure de l'analyse dans le groupe de champs **Heure de démarrage**.
- **Toutes les semaines** – l'action s'exécutera certains de jours de la semaine. Dans le groupe de champs **Heure de démarrage**, spécifiez l'heure et sélectionnez un jour de la semaine pour exécuter l'analyse à la demande.

## Étape 5. Configuration du module Anti-Spam

Au cours de cette étape vous pourrez configurer le module Anti-Spam (Figure 21).

Sélectionnez le mode de fonctionnement du module Anti-Spam dans la section **Protection Anti-Spam** :

- **Désactivé**. L'Anti-Spam est désactivé dans ce mode.

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

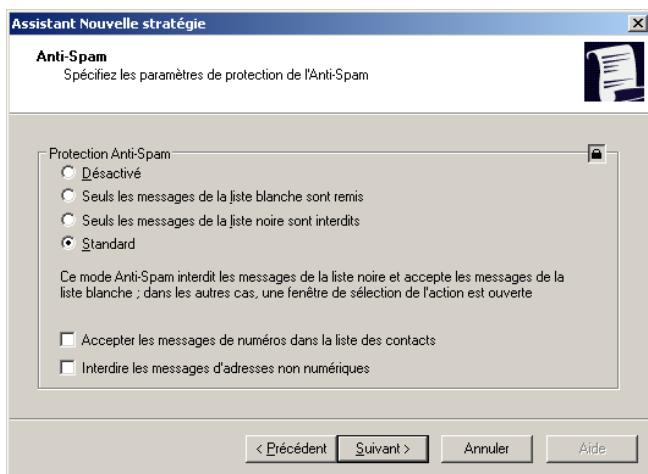


Figure 21. Configuration du module Anti-Spam

Cochez la case **Accepter les messages de numéros dans la liste des contacts** pour s'assurer que le module Anti-Spam laisse passer les messages de numéros présents dans les contacts.

Cochez la case **Interdire les messages d'adresses non numériques** pour que le module Anti-Spam bloque les messages provenant d'expéditeurs non numériques.

## Etape 6. Configuration de paramètres avancés

Au cours de cette étape vous pouvez spécifier le niveau de protection du module Pare-feu et le délai de synchronisation avec le Serveur d'administration.

Spécifiez le niveau de protection du module Pare-feu dans la section **Pare-feu** (Figure 22). Le module Pare-feu assure la protection du périphérique mobile sur les niveaux suivants :

- **Désactivé.** Pare-feu désactivé.
- **Niveau bas.** Le module Pare-feu bloque toutes les connexions entrantes ;toutes les connexions sortantes sont autorisées.
- **Niveau moyen.** Le module Pare-feu bloque toutes les connexions entrantes ;les connexions sortantes sont autorisées à travers les ports HTTP/HTTPS/SMTP/IMAP/SSH.
- **Niveau haut.** Le module Pare-feu interdit toute l'activité réseau, sauf la mise à jour des bases de l'application et la connexion au Serveur d'administration.

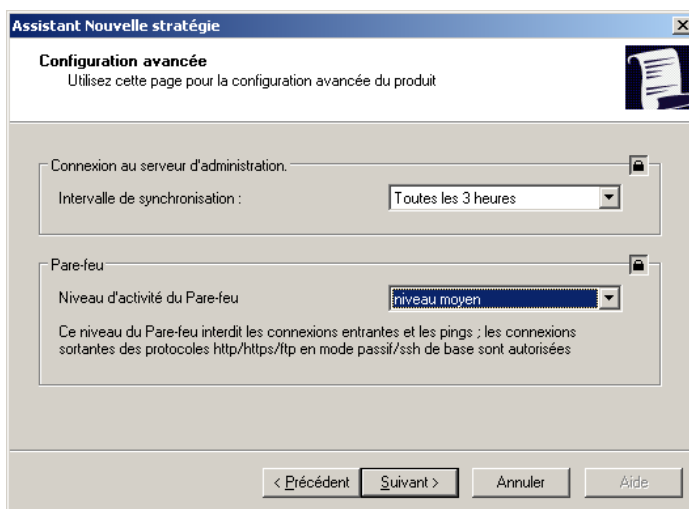


Figure 22. Paramètres d'application avancés

Spécifiez la fréquence de synchronisation dans la liste déroulante **Intervalle de synchronisation** de la section **Connexion au serveur d'administration**. Par défaut, le périphérique mobile essaie de se connecté au Serveur d'administration toutes les 6 heures.

## Etape 7. Choix d'un fichier de clé

Cette étape permet de spécifier un fichier clé utilisé pour activer Kaspersky Mobile Security.

Cliquez sur **Modifier** puis sélectionnez le fichier clé dans la fenêtre ouverte. Ensuite, l'Assistant affiche les informations suivantes sur la clé :

- Numéro ;
- Type de clé ;
- Date d'expiration de la licence.
- Restrictions de licence.


**Remarque :**

Pour s'assurer que le fichier clé est transféré aux périphériques mobiles, vous devez confirmer la sélection avec le bouton . Dans le cas contraire, Kaspersky Mobile Security ne sera pas activé.

## Étape 8. Fin de la création de la stratégie

Le dernier écran de l'Assistant informe sur la réussite du processus de création de la stratégie (Figure 23).

À la fin de l'Assistant, les stratégies de Kaspersky Mobile Security 7.0 Enterprise Edition seront ajoutées au dossier **Stratégies** du groupe correspondant et affichées dans le panneau de résultats.

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

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

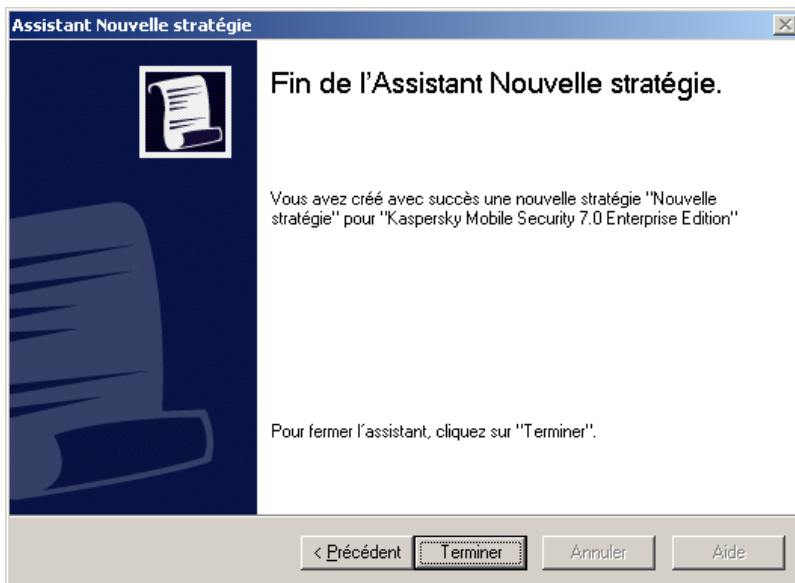


Figure 23. Fin de la création de la stratégie

## 3.2. Examen et modification des paramètres de la stratégie

A cette étape, vous pouvez introduire des modifications dans la stratégie et interdire la modification de certains paramètres dans la stratégie d'application et de tâche des groupes imbriqués.


1. Dans l'explorateur de console, dans le dossier **Groupes**, sélectionnez le groupe de périphériques mobiles dont vous souhaitez modifier les paramètres.
2. Sélectionnez le dossier **Stratégie** faisant partie de ce groupe ;ceci affiche toutes les stratégies du groupe dans le panneau de résultats.
3. Sélectionnez la stratégie requise pour **Kaspersky Mobile Security 7.0 Enterprise Edition** dans la liste (le nom de l'application est indiqué dans le champ **Nom**).
4. Sélectionnez la commande **Propriétés** dans le menu contextuel de la stratégie sélectionnée.

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

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

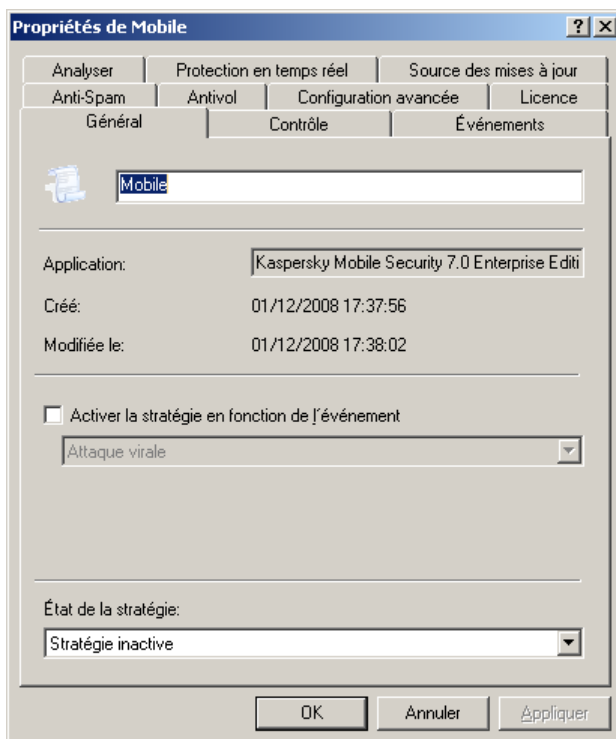
Le reste des onglets contient des contrôles pour paramétrer Kaspersky Mobile Security 7.0 Enterprise Edition. La présentation de chacun des onglets figure dans la suite.

#### Note

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

### 3.2.1. Informations sur l'application

L'information suivante sur la stratégie est affichée dans l'onglet **Général** (Figure 24) : nom de la stratégie, nom de l'application associée, date et heure de création de la stratégie et de sa dernière modification.

Figure 24. Onglet **Général**

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

### 3.2.2. Affichage des résultats de l'application de la stratégie

The **Contrôle** tab (Figure 25) contient des informations générales sur l'application de la stratégie sur les périphériques mobiles présents dans le groupe et indique le nombre de dispositifs pour lesquels la stratégie :

- n'est pas définie ;
- est exécutée ;
- n'est pas encore exécutée ;

- ne peut pas être exécutée en raison d'une erreur.

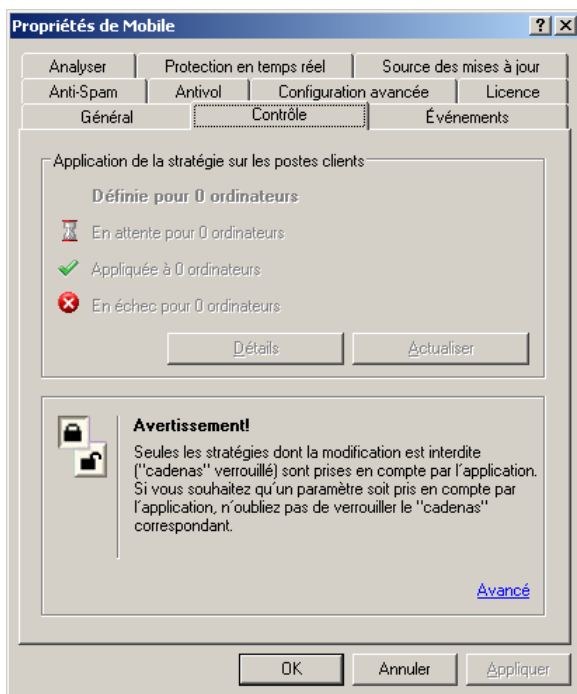


Figure 25. Onglet **Contrôle**

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

### 3.2.3. Paramètres de consignation des événements de l'application

Pendant son fonctionnement, Kaspersky Mobile Security génère un certain nombre d'événements. Chaque événement possède une caractéristique qui reflète son niveau d'importance. Il y a quatre degrés de gravité : événement critique, échec de fonctionnement, avertissement et message d'information.

Les événements de même type peuvent avoir différents degrés de gravité, en fonction de la situation où l'événement se produit.

L'onglet **Événements** (Figure 26) affiche les types d'événements générés par le fonctionnement de l'application et qui sont enregistrés dans le rapport, ainsi que l'emplacement disque du rapport et le mode de notification à l'administrateur ou aux autres utilisateurs.

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

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

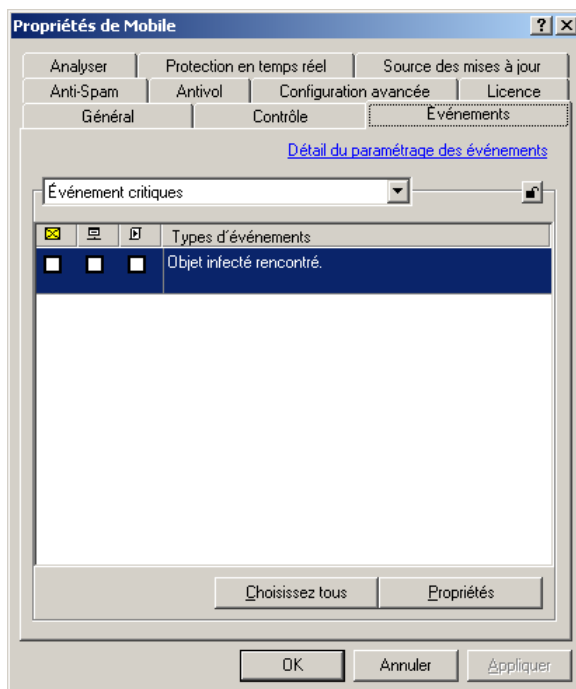


Figure 26. Onglet **Événements**

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

## 3.2.4. Paramètres d'analyse antivirus

L'onglet **Analyser** (Figure 27) permet de configurer l'analyse à la demande : couverture de l'analyse, actions à réaliser sur les objets infectés et planification de son exécution.

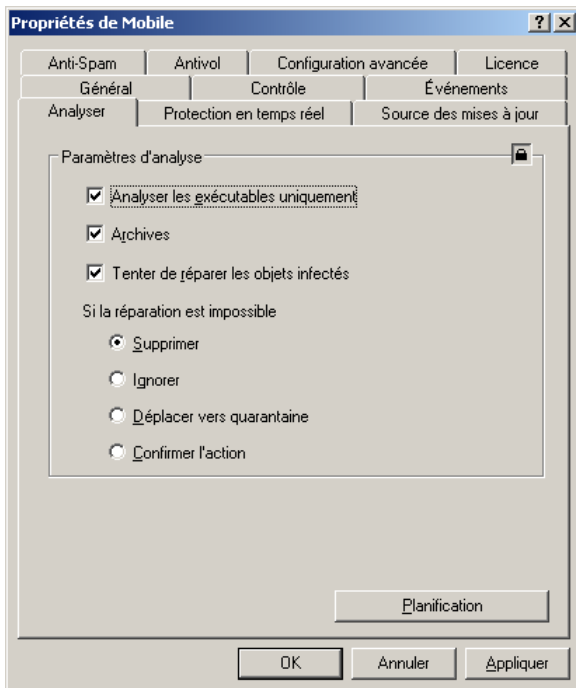


Figure 27. Onglet **Analyser**

Dans la section **Si la réparation est impossible** sélectionnez l'action exécutée en présence d'un objet infecté.

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

Si le paramètre **Tenter de réparer les objets infectés** est activé, l'action sélectionnée ne sera exécutée que si l'objet n'a pas pu être réparé.

Les autres paramètres sont similaires à ceux déjà décrits dans la section 3.1 à la page 25.

## 3.2.5. Paramètres de protection en temps réel

L'onglet **Protection en temps réel** (Figure 28) permet de configurer la protection en temps réel : couverture de l'analyse, actions à réaliser sur les objets infectés.

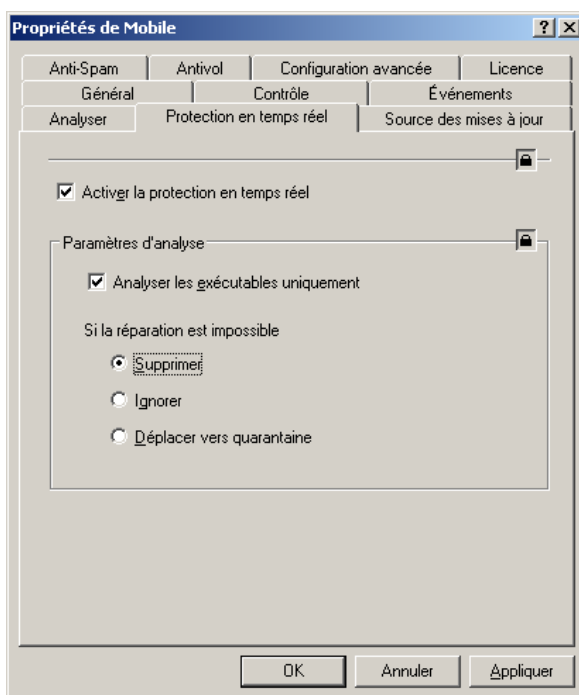


Figure 28. L'onglet **Protection en temps réel**

### 3.2.6. Sélection de la source de mises à jour des bases de l'application

L'onglet **Source des mises à jour** (Figure 29) permet de spécifier la source de téléchargement des mises à jour des bases antivirus. Cet onglet sert également à planifier l'exécution des mises à jour.

Pour s'assurer que les mises à jour se font depuis les serveurs de mise à jour de Kaspersky Lab, laissez vide le champ **Serveur des mises à jour**.

Pour utiliser une source différente, spécifiez l'adresse de la source des mises à jour dans la section **Source de mise à jour**. Il s'agit de l'adresse URL complète du fichier *mobile.xml*.

Par exemple, <http://domain.com/index/mobile.xml>.

**Remarque :**

La structure des dossiers dans la source de la mise à jour doit être identique à celle du serveur de mise à jour Kaspersky Lab.

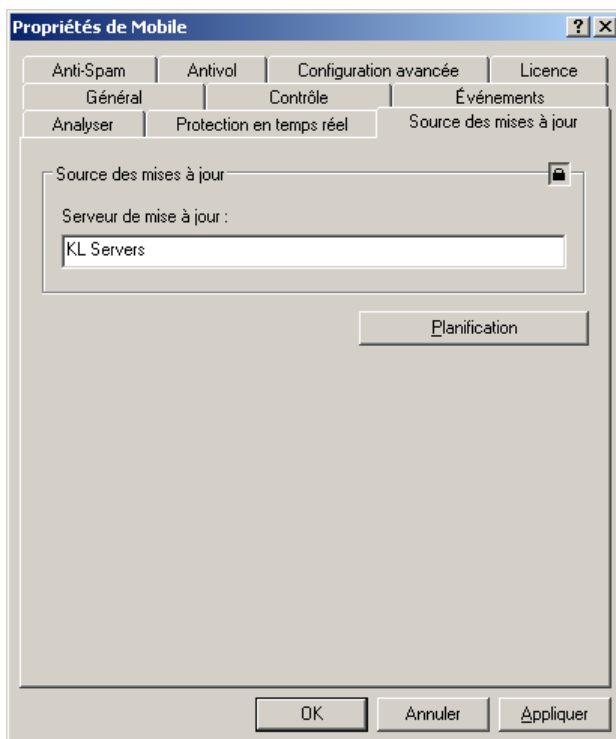


Figure 29. Onglet **Source des mises à jour**

### 3.2.7. Configuration du module Anti-Spam

L'onglet **Anti-Spam** (Figure 30) permet de configurer le module Anti-Spam.

Sélectionnez le mode de fonctionnement du module Anti-Spam dans la section **Anti-Spam** :

- **Désactivé** – désactive le module Anti-Spam.
- **Seuls les messages de la liste blanche sont remis** – le module Anti-Spam vérifie les messages avec la liste blanche. Si le numéro de

l'expéditeur ou le texte du message est présent dans la liste, le module Anti-Spam laisse passer le message.

- **Seuls les messages de la liste noire sont interdits** – le module Anti-Spam vérifie les messages avec la liste noire. Si le numéro de l'expéditeur ou le texte du message est présent dans la liste, le module Anti-Spam interdit le message.
- **Standard** – Le module Anti-Spam interdit les messages de la liste noire, laisse passer les messages de la liste blanche ; dans les autres cas, une fenêtre permet à l'utilisateur du périphérique de sélectionner l'action à réaliser sur le message.

Cochez la case **Accepter les messages de numéros dans la liste des contacts** pour s'assurer que le module Anti-Spam laisse passer les messages de numéros présents dans les contacts.

Cochez la case **Interdire les messages d'adresses non numériques** pour que le module Anti-Spam bloque les messages provenant d'expéditeurs non numériques.

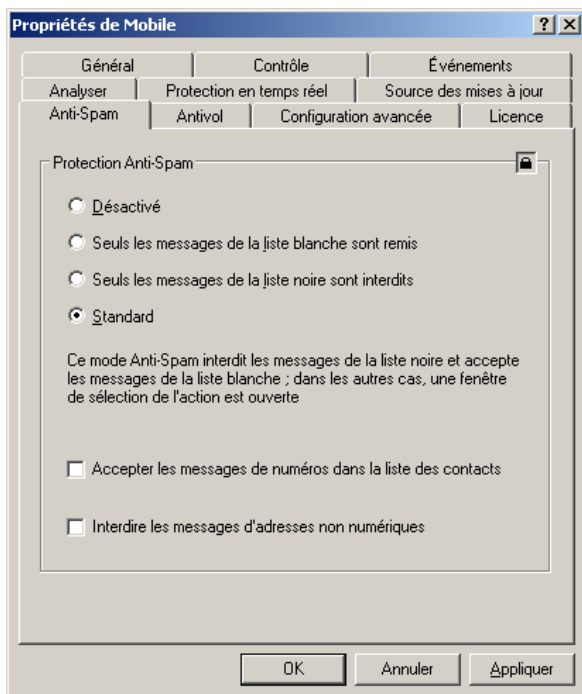


Figure 30. L'onglet **Anti-Spam**

### 3.2.8. Configuration du module Antivol

Le module Antivol (section **Antivol** (Figure 31)) permet de configurer le module Antivol pour éviter l'accès non autorisé aux données conservées dans le périphérique mobile, en cas de perte ou de vol.

Cochez la case **Activer le mode Suppression** pour activer la fonction Suppression. Cette fonction permet d'effacer les données personnelles de l'utilisateur (contacts, messages, fichiers, données sur la carte mémoire, paramètres de connexion réseau). Pour activer la fonction Suppression, envoyez un message SMS avec le texte "`clean:code`" au périphérique.

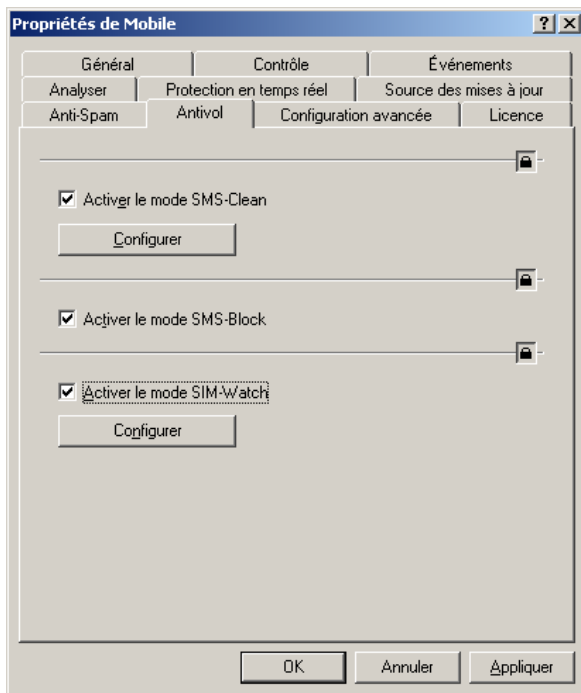
Cliquez sur **Configurer** puis dans la fenêtre ouverte, sélectionnez les catégories d'informations qui doivent être supprimées par la fonction Suppression :

- **Supprimer contacts** – suppression du répertoire.
- **Supprimer messages** – suppression des messages.
- **Supprimer documents** – suppression des données personnelles.
- **Suppression données de la carte mémoire** – suppression des fichiers sur la carte mémoire.
- **Suppression paramètres du réseau et du point d'accès** – suppression des paramètres réseau personnels.

Cochez la case **Activer le mode Verrouillage** pour activer la fonction Verrouillage. Cette fonction permet de déverrouiller le périphérique. Le déverrouillage n'est possible qu'après avoir saisi le code. Pour déverrouiller le périphérique avec la fonction Verrouillage, envoyez un message SMS avec le texte : "`block:code`" au périphérique.

Cochez la case **Activer le mode SIM-Surveillance** pour activer la fonction SIM-Surveillance. Cette fonction permet, quand la carte SIM est remplacée dans le périphérique, d'envoyer aux numéros spécifiés le nouveau numéro du téléphone et de verrouiller le périphérique volé.

Cliquez sur **Configurer** puis dans la fenêtre ouverte, configurez la fonction Suppression. Dans les champs **Téléphone principal** et **Téléphone supplémentaire**, spécifiez les numéros de téléphone destinataires du message SMS contenant le nouveau téléphone en cas de remplacement de la carte SIM. En outre, la case correspondante permet d'activer la fonction de verrouillage du périphérique si la carte SIM est remplacée.

Figure 31. Onglet **Antivol**

### 3.2.9. Configuration de paramètres avancés

L'onglet **Configuration avancée** (Figure 32) permet de spécifier le niveau de protection du module Pare-feu et le délai de synchronisation avec le Serveur d'administration.

Spécifiez la fréquence de synchronisation dans la liste déroulante **Intervalle de synchronisation** de la section **Connexion au serveur d'administration**.

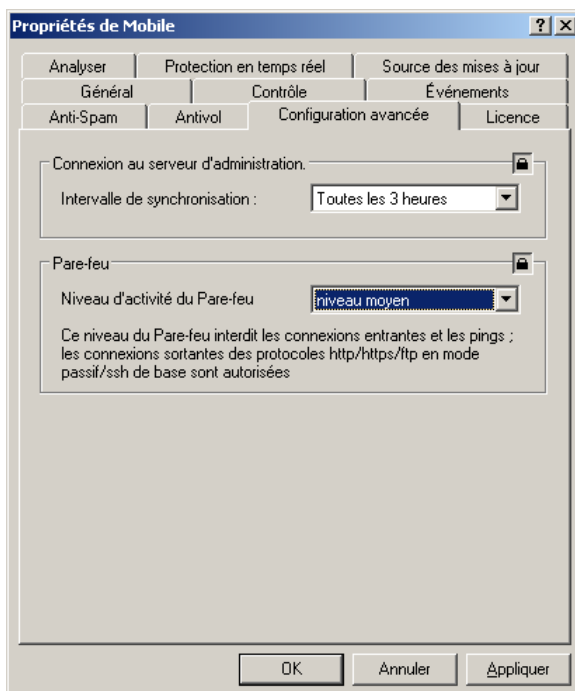


Figure 32. Configuration avancée

Spécifiez le niveau de protection du module Pare-feu dans la section **Pare-feu**.

- **Désactivé** – désactive le module Pare-feu.
- **Niveau bas** – Le module Pare-feu bloque toutes les connexions entrantes ;toutes les connexions sortantes sont autorisées.
- **Niveau moyen** – Le module Pare-feu bloque toutes les connexions entrantes ;les connexions sortantes sont autorisées à travers les ports HTTP/HTTPS/SMTP/IMAP/SSH.
- **Niveau haut** – Le module Pare-feu interdit toute l'activité réseau, sauf la mise à jour des bases de l'application et la connexion au Serveur d'administration.

---

# CHAPITRE 4. CONTROLE DES PARAMETRES D'APPLICATION

Les paramètres d'application permettent de modifier la configuration de l'application Kaspersky Mobile Security installée sur un périphérique mobile. Vous ne pouvez modifier que les paramètres qui ne sont pas verrouillés par une stratégie (pour plus de détails voir section 3.1 à la page 25).

*Pour modifier les paramètres d'application :*

1. Sélectionnez le nom du groupe contenant le périphérique mobile, dans le dossier **Groupes**.
2. Dans le panneau de résultats sélectionnez le périphérique dont vous souhaitez modifier les paramètres d'application. Sélectionnez la commande **Propriétés** dans le menu contextuel ou dans le menu **Actions**.
3. La boîte de dialogue **Propriétés de <nom de l'ordinateur>** s'affiche dans la fenêtre principale de l'application. Sélectionnez l'onglet **Applications** (Figure 33).

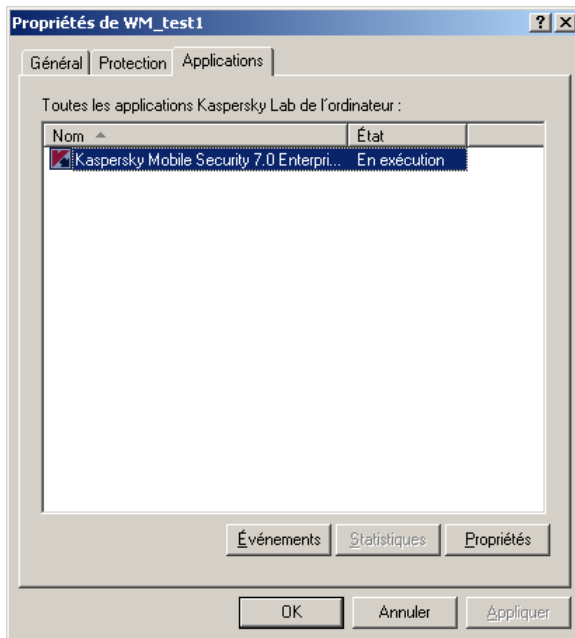


Figure 33. Fenêtre de propriétés du périphérique mobile.  
Onglet **Applications**

4. Sélectionnez l'application **Kaspersky Mobile Security 7.0 Enterprise Edition**. Les boutons suivants se trouvent dans la partie inférieure gauche de la fenêtre :
  - **Événements** – affiche la liste des événements apparus pendant le fonctionnement de l'application sur les périphériques mobiles et enregistrés par le Serveur d'administration.
  - **Statistiques** – affiche les statistiques sur le fonctionnement de l'application.
  - **Propriétés** – configure l'application dans la fenêtre de paramètres de l'application **Kaspersky Mobile Security 7.0 Enterprise Edition**.

## 4.1. Informations sur l'application

L'onglet **Général** (Figure 34) permet d'afficher des informations sur l'application Kaspersky Mobile Security 7.0 Enterprise Edition.

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

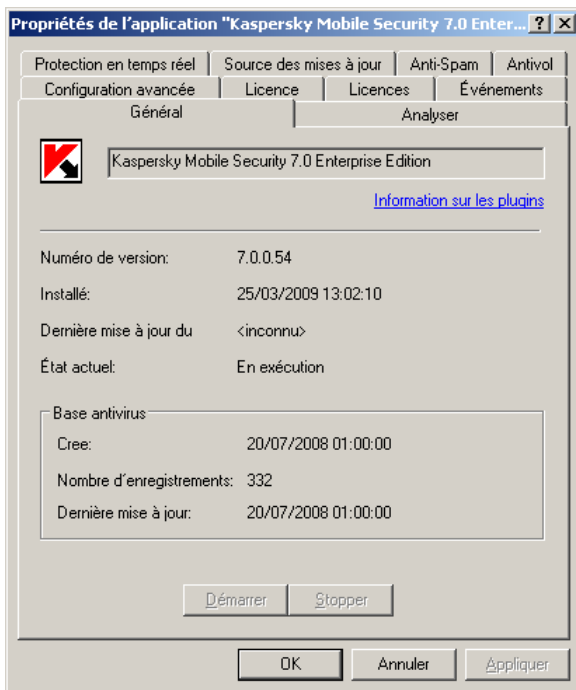


Figure 34. Fenêtre de configuration des paramètres d'application.  
Onglet **Général**

## 4.2. Informations sur les paramètres d'analyse antivirus

L'onglet **Analyser** (Figure 35) permet d'afficher et de modifier les paramètres d'analyse à la demande : couverture de l'analyse, actions à réaliser sur les objets infectés et planification de son exécution.

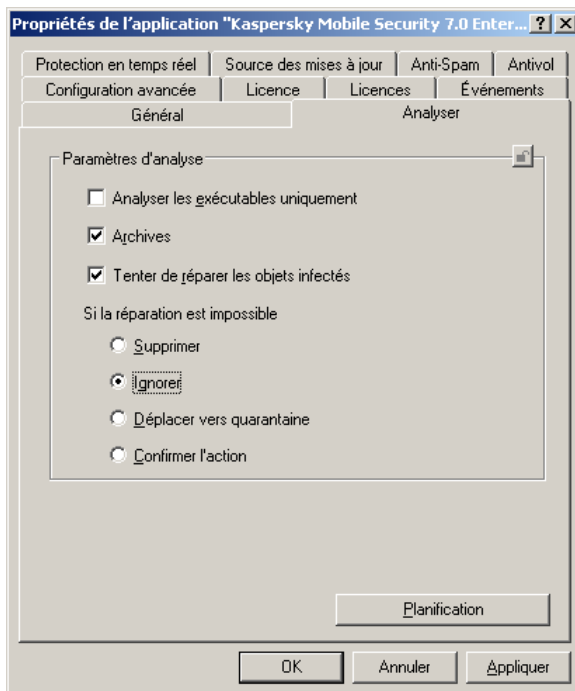


Figure 35. Onglet Analyser

## 4.3. Information sur la protection en temps réel

L'onglet **Protection en temps réel** (Figure 36) permet d'afficher et de modifier les paramètres de protection en temps réel : couverture de l'analyse et actions à réaliser sur les objets infectés.

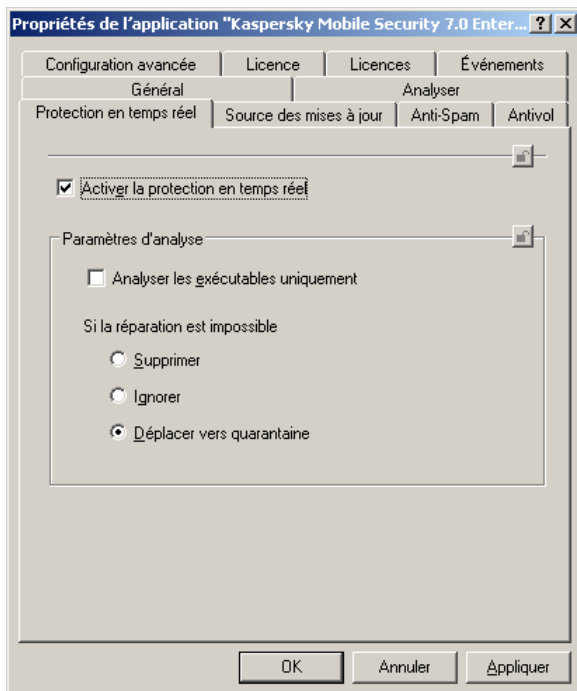


Figure 36. L'onglet **Protection en temps réel**

## 4.4. Informations sur la source de mises à jour

L'onglet **Source des mises à jour** (Figure 37) permet d'afficher et de modifier les paramètres de téléchargement des mises à jour d'un périphérique mobile en particulier.

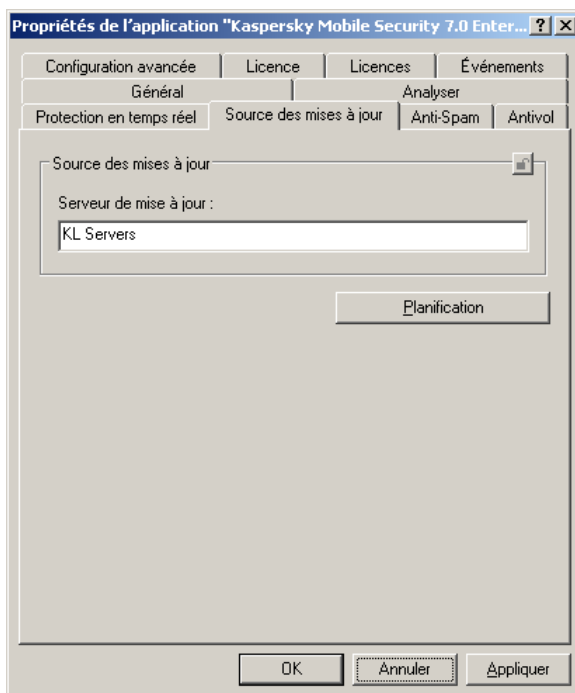


Figure 37. L'onglet **Source des la mises à jour**

## 4.5. Informations sur les paramètres du module Anti-Spam

L'onglet **Anti-Spam** (Figure 38) permet d'afficher et de modifier les paramètres de protection antisпам de votre périphérique mobile.

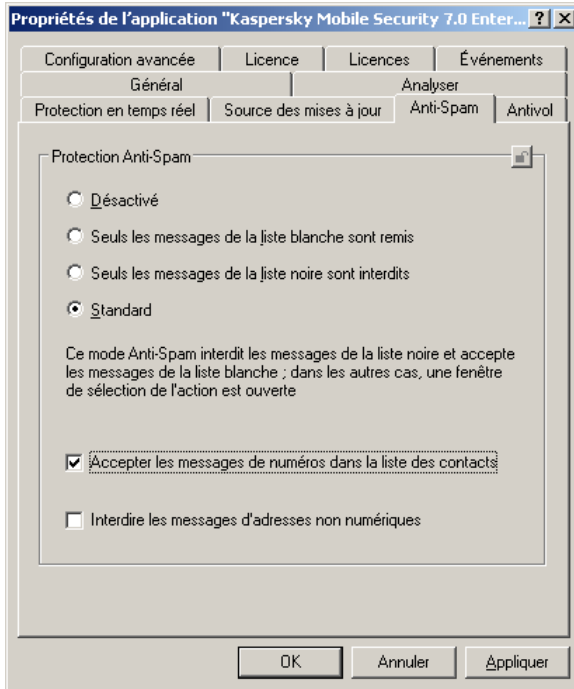
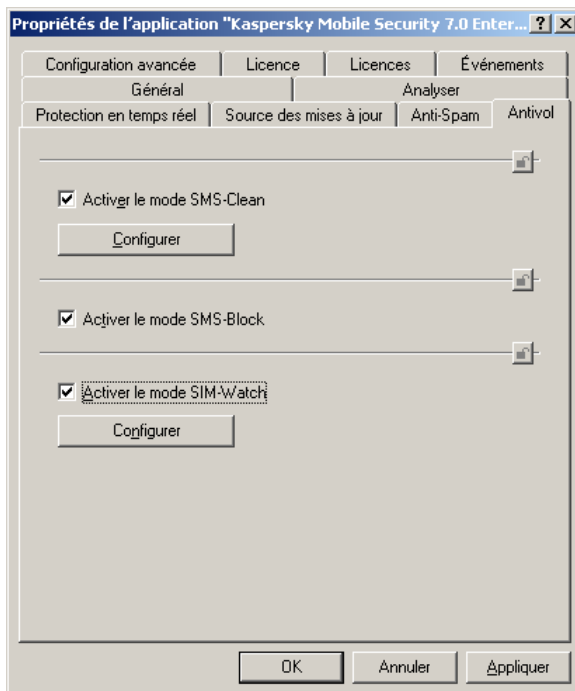


Figure 38. L'onglet **Anti-Spam**

## 4.6. Informations sur les paramètres du module Antivol

L'onglet **Antivol** (Figure 39) permet d'afficher et de modifier les paramètres du module Antivol : Vous pouvez :

- activer les modules : Suppression, Verrouillage , SIM-Surveillance ;
- configurer les paramètres de la fonction Antivol avec les boutons **Configurer** de chaque section.

Figure 39. Onglet **Antiviol**

## 4.7. Informations sur les paramètres avancés

L'onglet **Configuration avancée** (Figure 40) permet d'afficher et de modifier les paramètres du module Pare-feu ainsi que la fréquence de connexion avec le Serveur d'administration.

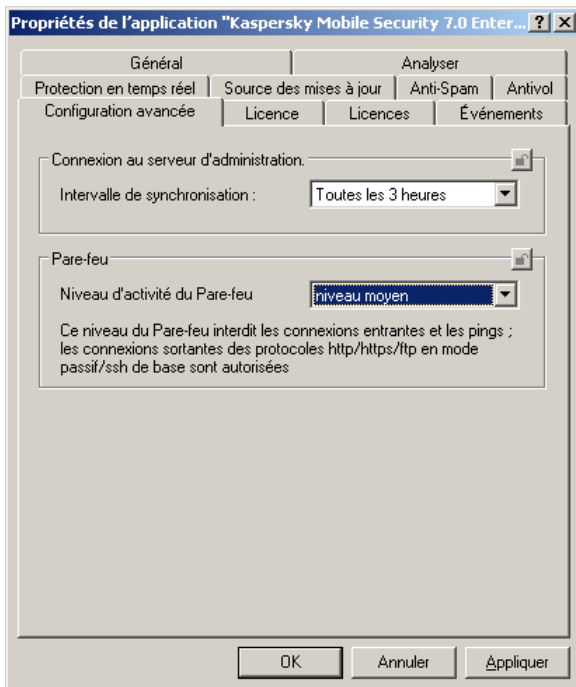
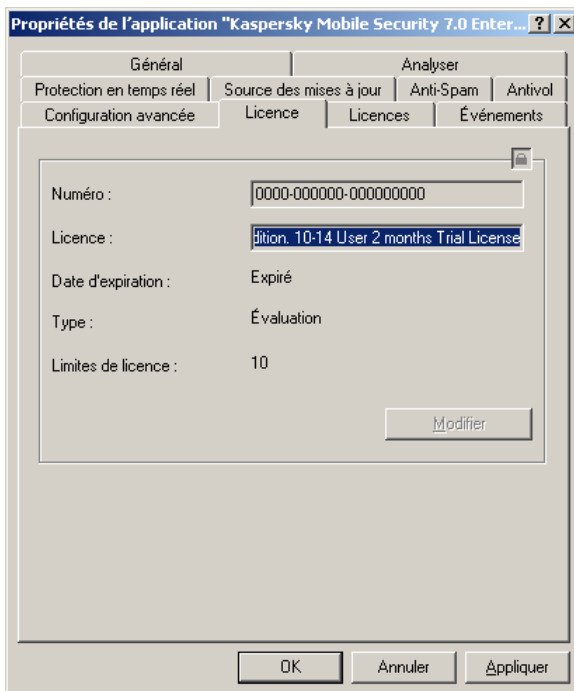


Figure 40. Configuration avancée (onglet)

## 4.8. Affichage des détails de la clé

L'onglet **Licence** (Figure 41) contient des informations sur la clé installée sur le périphérique mobile.

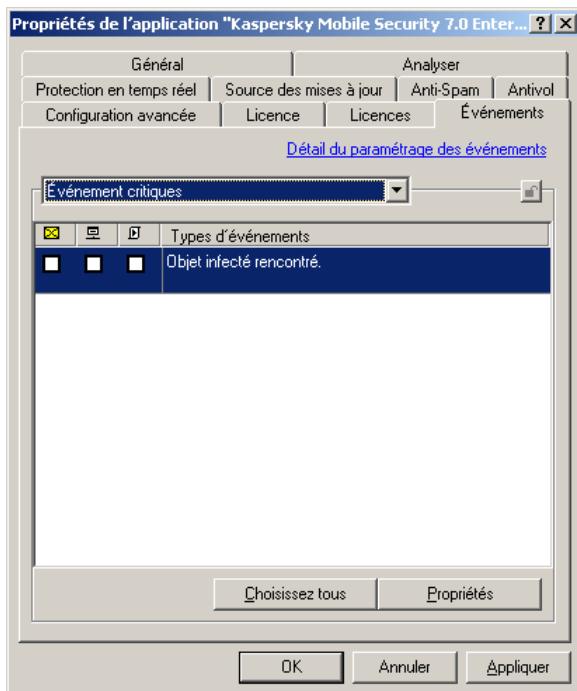
Figure 41. Onglet **Licence**

## 4.9. Affichage d'événements

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

Les événements de même type peuvent avoir différents degrés de gravité, en fonction de la situation où l'événement se produit.

L'onglet **Événements** (Figure 42) affiche les types d'événements générés par le fonctionnement de l'application et qui sont enregistrés dans le rapport, ainsi que l'emplacement disque du rapport et le mode de notification à l'administrateur ou aux autres utilisateurs.

Figure 42. Onglet **Événements**

---

# ANNEXE A. KASPERSKY LAB

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

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

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

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

Site officiel de <http://www.kaspersky.com/fr>  
Kaspersky  
Lab :

Encyclopédie <http://www.viruslist.com/fr/>  
de virus :

Laboratoire [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)  
Anti-Virus :  
(uniquement pour l'envoi des objets suspects archivés)  
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>  
(pour les demandes auprès des experts de virus)

---

# ANNEXE B. CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

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

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

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

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

## 1. Définitions

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

- 1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.
- 1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les « téléphones intelligents », les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.
- 1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, « Vous » signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme « entité », sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.
- 1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.
- 1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patch, les modifications, les copies, les ajouts ou les packs de maintenance, etc.
- 1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.
- 1.8. **Acquisition du logiciel** signifie son achat ou acquisition à des conditions définies dans un contrat additionnel, y compris une acquisition gratuite.

## **2. Concession de la Licence**

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

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

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

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

- 2.2. Si le Logiciel a été acheté sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel ou comme spécifié dans le Contrat additionnel.
- 2.3. Si le Logiciel a été acheté sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'achat de la Licence du Logiciel ou comme spécifié dans le Contrat additionnel.
- 2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.
- 2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques ou morales dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que

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

- 2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acheté sur un support physique) ou stipulée pendant l'achat (si le Logiciel a été acheté sur Internet) :
- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
  - Assistance technique en ligne et assistance technique par téléphone.

### **3. Activation et durée de validité**

- 3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.
- 3.2. Si le Logiciel a été acheté sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat ou comme spécifié dans le Contrat additionnel.
- 3.3. Si le Logiciel a été acheté sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'achat ou comme spécifié dans le Contrat additionnel.
- 3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

- 3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.
- 3.6. Si vous avez acheté le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.
- 3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.
- 3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.
- 3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

#### **4. Assistance technique**

L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).

Service d'assistance technique : <http://support.kaspersky.com>

#### **5. Recueil d'informations**

- 5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.
- 5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

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

- 5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.
- 5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

## **6. Limitations**

- 6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.
- 6.2. Vous ne devez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.
- 6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.
- 6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

- 6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.
- 6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.
- 6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

## **7. Garantie limitée et avis de non-responsabilité**

- 7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément déchargé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.
- 7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.
- 7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.
- 7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.
- 7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la

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

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

## **8. Exclusion et Limitation de responsabilité**

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

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

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

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

## **9. Licence GNU et autres licences de tierces parties**

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

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

## **10. Droits de propriété intellectuelle**

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

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

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

## **11. Droit applicable ; arbitrage**

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

## **12. Délai de recours.**

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

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

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

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

#### **14. Service clientèle du titulaire des droits**

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

Kaspersky Lab ZAO, 10 build. 1, 1<sup>st</sup> Volokolamsky Proezd  
Moscou, 123060  
Fédération de Russie  
Tél. : +7-495-797-8700  
Fax : +7-495-645-7939  
E-mail : [info@kaspersky.com](mailto:info@kaspersky.com)  
Site Internet : [www.kaspersky.com](http://www.kaspersky.com)

© 1997-2009 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et toute documentation l'accompagnant font l'objet de droits d'auteur et sont protégés par les lois sur la protection des droits d'auteur et les traités internationaux sur les droits d'auteur, ainsi que d'autres lois et traités sur la propriété intellectuelle.