Guide de l'utilisateur

KASPERSKY MOBILE SECURITY 8.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que cette documentation vous sera utile dans votre travail et vous apportera toutes les réponses sur notre produit logiciel.

Ce document peut être modifié sans préavis. Pour obtenir la dernière version de ce document, reportez-vous au site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.

+7 (495) 645-79-39,
Vocal, fax : +7 (495) 797-87-00,
+7 (495) 956-70-00

http://www.kaspersky.com/fr
http://support.kaspersky.fr/

Date de révision : 17 avril 2009

TABLE DES MATIÈRES

KASPERSKY MOBILE SECURITY 8.0 7
Affichage d'informations sur l'application 8
Sources de données pour des consultations indépendantes 8
Contacter le Département commercial 9
Contacter le Service d'assistance technique 9
Forums de discussion sur les applications Kaspersky Lab 10
Spécifications matérielles et logicielles 10
Kit de distribution 10
KASPERSKY MOBILE SECURITY POUR SYMBIAN OS 11
Installation de Kaspersky Mobile Security 11
Premiers pas 13
Activation du logiciel 13
Démarrage du logiciel 14
Interface utilisateur 15
Code secret 16
Informations sur le programme 17
Protection en temps réel 17
À propos de la protection en temps réel 18
Activation et désactivation de la protection en temps réel 18
Sélection des objets à analyser 19
Sélection d'actions sur les objets 20
Affichage de l'icône de protection 21
Analyse à la demande 22
À propos de l'analyse à la demande 23
Exécution manuelle d'une analyse 23
Configuration d'analyses planifiées 25
Sélection des objets à analyser 26
Sélection des actions à appliquer sur les objets 27
Configuration de l'analyse de la ROM 29
Configuration de l'analyse de fichiers compressés 30
Contrôle du rétro éclairage 31
Quarantaine 32
À propos de la quarantaine 32
Affichage des objets en quarantaine 33
Restauration d'objets de la quarantaine 34
Suppression d'un objet de la quarantaine 34
Anti-Spam 35
À propos du composant Anti-Spam 36
Modes du composant Anti-Spam 36
Création d'une liste noire 37
Ajout d'une nouvelle entrée 37
Modification d'une entrée existante 38
Suppression d'une entrée unique 39
Suppression de toutes les entrées 40
Création d'une liste blanche 41

Ajout d'une nouvelle entrée 41
Modification d'une entrée existante 42
Suppression d'une entrée unique 43
Suppression de toutes les entrées 44
Réponse aux messages et appels présents dans l'annuaire téléphonique 45
Réponse aux messages d'expéditeurs non numériques 45
Sélection de l'action à appliquer sur des messages entrants 47
Sélection de l'action à appliquer sur des appels entrants 48
Contrôle parental 48
À propos du contrôle parental 48
Modes du contrôle parental 49
Création d'une liste noire 50
Ajout d'une nouvelle entrée 50
Modification d'une entrée existante 51
Suppression d'une entrée unique 52
Suppression de toutes les entrées 53
Création d'une liste blanche 54
Ajout d'une nouvelle entrée 54
Modification d'une entrée existante 55
Suppression d'une entrée unique 56
Suppression de toutes les entrées 57
Antivol 58
À propos du composant Antivol 58
Fonction Verrouillage 59
Verrouillage de l'appareil 59
Fonction Suppression 60
Suppression de données personnelles 61
Fonction SIM-Surveillance 62
Fonction Localisation 63
Détermination des coordonnées de l'appareil 64
Fonction SMS Invisible 65
Pare-feu 66
À propos du Pare-feu 66
Sélection du niveau de sécurité du Pare-feu 67
Notifications sur les tentatives de connexion 68
Chiffrement 68
À propos du chiffrement 68
Chiffrement des données 69
Déchiffrement de données 70
Informations sur les données chiffrées 70
Interdiction d'accès aux données chiffrées 71
Mise à jour des bases du programme 72
À propos de la mise à jour des bases 73
Affichage d'informations sur les bases 73
Mise à jour manuelle 73
Mise à jour planifiée 74
Mise à jour en itinérance 75
Configuration de la connexion 76
Journaux du logiciel 77

À propos des journaux ... 77
Affichage des événements du journal ... 78
Suppression d'événements dans les journaux ... 78
Affichage de la fenêtre d'état ... 78
Notifications sonores ... 79
Gestion de la licence ... 80
Affichage des informations de licence ... 80
Renouvellement de la licence ... 81
Désinstallation du programme ... 82

KASPERSKY MOBILE SECURITY POUR MICROSOFT WINDOWS MOBILE ... 86
Installation de Kaspersky Mobile Security ... 86
Premiers pas ... 87
Activation du logiciel ... 88
Démarrage du logiciel ... 89
Interface graphique utilisateur ... 90
Code secret ... 91
Informations sur le programme ... 92
Protection en temps réel ... 92
À propos de la protection en temps réel ... 93
Activation et désactivation de la protection en temps réel ... 93
Sélection des actions à appliquer sur des objets ... 94
Analyse à la demande ... 95
À propos de l'analyse à la demande ... 96
Exécution manuelle d'une analyse ... 96
Configuration d'analyses planifiées ... 99
Sélection des objets à analyser ... 99
Sélection des actions à appliquer sur des objets ... 101
Quarantaine ... 102
À propos de la quarantaine ... 102
Affichage des objets en quarantaine ... 103
Restauration d'objets de la quarantaine ... 103
Suppression d'objets de la quarantaine ... 104
Anti-Spam ... 105
À propos du composant Anti-Spam ... 106
Modes du composant Anti-Spam ... 106
Création d'une liste noire ... 107
Ajout d'une nouvelle entrée ... 107
Modification d'une entrée existante ... 108
Suppression d'une entrée ... 109
Création d'une liste blanche ... 110
Ajout d'une nouvelle entrée ... 110
Modification d'une entrée existante ... 111
Suppression d'une entrée ... 112
Réponse aux messages et appels présents dans l'annuaire téléphonique ... 113
Réponse aux messages d'expéditeurs non numériques ... 114
Sélection de l'action à appliquer sur des messages entrants ... 116
Sélection de l'action à appliquer sur des appels entrants ... 117
Contrôle parental ... 117

À propos du contrôle parental ... 118
Modes du contrôle parental ... 118
Création d'une liste noire ... 119
Ajout d'une nouvelle entrée ... 119
Modification d'une entrée existante ... 120
Suppression d'une entrée ... 121
Création d'une liste blanche ... 122
Ajout d'une nouvelle entrée ... 122
Modification d'une entrée existante ... 123
Suppression d'une entrée ... 124
Antivol ... 125
À propos du composant Antivol ... 126
Fonction Verrouillage ... 126
Verrouillage de l'appareil ... 127
Fonction Suppression ... 128
Suppression de données personnelles ... 129
Fonction SIM-Surveillance ... 130
Fonction Localisation ... 131
Détermination des coordonnées de l'appareil ... 132
Fonction SMS invisible ... 133
Pare-feu ... 134
À propos du Pare-feu ... 135
Sélection du niveau de sécurité du Pare-feu ... 135
Chiffrement ... 136
À propos du chiffrement ... 136
Chiffrement des données ... 137
Déchiffrement des données ... 138
Interdiction d'accès aux données chiffrées ... 139
Mise à jour des bases du programme ... 141
À propos de la mise à jour des bases ... 141
Affichage d'informations sur les bases ... 142
Mise à jour manuelle ... 142
Planification des mises à jour ... 143
Journaux du logiciel ... 144
À propos des journaux ... 144
Affichage des événements du journal ... 144
Suppression d'événements dans les journaux ... 145
Gestion de la licence ... 146
Affichage des informations de licence ... 147
Renouvellement de la licence ... 147
Désinstallation du programme ... 148
GLOSSAIRE ... 151
KASPERSKY LAB ... 154
CRYPTO EX LTD. ... 155
INDEX ... 156

KASPERSKY MOBILE SECURITY 8.0

Kaspersky Mobile Security 8.0 est conçu pour assurer la protection en temps réel d'appareils mobiles exploités sous Symbian OS et Microsoft Windows Mobile contre les logiciels malveillants ainsi que les appels et messages indésirables : Le programme dispose des fonctionnalités suivantes :

- **Protection en temps réel** du système de fichiers de l'appareil – 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 l'appareil mobile ;
  - programmes installés dans l'interface de l'appareil.
- **analyse des objets du système de fichiers** sur l'appareil mobile ou sur les cartes d'extension connectées, à la demande de l'utilisateur, ou de manière planifiée ;
- **isolement sécurisé des objets infectés** dans une 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 appels et messages SMS entrants ou sortants indésirables**.
- **verrouillage ou effacement des données utilisateur** en cas d'actions non autorisées avec l'appareil, comme par exemple, en cas de vol.
- **protection des connexions réseau de l'appareil mobile**.
- **protection par chiffrement** d'un dossier (sauf les dossiers système) dans la mémoire de l'appareil ou dans une carte d'extension mémoire s'appuie sur les fonctions de chiffrement incorporées dans le système.
- **Réception des coordonnées géographiques** de l'appareil.

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

Le programme possède un menu système et une interface utilisateur conviviale.

En cas de détection d'un logiciel malveillant, Kaspersky Mobile Security peut réparer l'objet infecté (si la réparation est possible), le supprimer ou le placer en quarantaine. Dans ce cas, aucune copie de l'objet supprimé n'est conservée.

Dans cette section

Affichage d'informations sur l'application....8

Spécifications matérielles et logicielles....10

Kit de distribution....10

Affichage d'informations sur l'application

Pour toute question sur l'achat, l'installation ou l''utilisation de Kaspersky Mobile Security, des réponses sont disponibles.

Kaspersky Lab propose plusieurs sources d'information sur le programme. Vous pouvez sélectionner la source la plus appropriée à vos besoins, en fonction de l'importance ou de l'urgence de votre question.

Dans cette section

Sources de données pour des consultations indépendantes 8

Contacter le Département commercial 9

Contacter le Service d'assistance technique 9

Forums de discussion sur les applications Kaspersky Lab 10

Sources de données pour des consultations indépendantes

Vous disposez des informations suivantes sur le programme :

- page du logiciel, sur le site Web de Kaspersky Lab ;
- page du logiciel, sur le site du serveur du Support technique (Knowledge Base)
- système d'aide en ligne ;
- documentation.

Page du programme sur le site Web de Kaspersky Lab.

http://www.kaspersky.com/fr/mobile_downloads

Utilisez cette page pour obtenir des informations générales sur Kaspersky Mobile Security, ses possibilités et ses caractéristiques de fonctionnement. Pour acheter ou renouveler la licence d'utilisation de Kaspersky Mobile Security, utilisez notre boutique en ligne (E-Store).

Page de l'application sur le serveur du Support technique (Knowledge Base)

http://support.kaspersky.com/fr/desktop

Cette page contient des articles publiés par les experts du Service d'assistance technique.

Les articles contiennent des informations utiles, des instructions et des réponses aux questions fréquentes concernant l'achat, l'installation et l'utilisation de Kaspersky Mobile Security. Ils sont organisés par rubriques, telles que « Work with key files » (Utilisation de fichiers clé), « Database updates » (Mises à jour de bases de données) ou « Troubleshooting » (Dépannage). Les articles répondent non seulement à des questions sur Kaspersky Mobile Security, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

Système d'aide en ligne

En cas de question sur une fenêtre ou sur un onglet spécifiques de Kaspersky Mobile Security, vous disposez de l'aide contextuelle.

Pour accéder à l'aide contextuelle, ouvrez l'onglet correspondant et sélectionnez **Aide**.

Documentation

Le Guide de l'utilisateur contient des informations détaillées sur les fonctions de l'application, comment l'utiliser, avec des conseils et des recommandations de configuration.

Des fichiers de documentation au format PDF sont fournis dans le paquet du produit Kaspersky Mobile Security (CD d'installation).

Vous pouvez télécharger les fichiers numériques de la documentation depuis le site de Kaspersky Lab.

Contacter le Département commercial

En cas de questions sur le choix, l'achat ou le renouvellement de la licence de Kapsersky Mobile Security, vous pouvez contacter nos spécialistes du Département commercial via l'URL suivante :

http://www.kaspersky.com/fr/contacts

Vous pouvez transmettre vos questions au Département commercial à l'adresse de messagerie info@kaspersky.fr.

Contacter le Service d'assistance technique

Si vous avez déjà acheté Kaspersky Mobile Security, des informations peuvent être obtenues auprès du Service d'assistance technique par téléphone ou par Internet.

Les experts du Service d'assistance technique répondront à vos questions sur l'installation et l'utilisation du logiciel et, si votre appareil mobile est infecté par une activité malveillante, ils vous aideront à en éliminer les conséquences.

Avant de prendre contact avec le Service d'assistance technique, prenez connaissance des Règles de support (http://support.kaspersky.com/support/rules).

Écrire sa question au Service d'assistance technique

Vous pouvez transmettre votre demande aux spécialistes du Service d'assistance technique en remplissant le formulaire du Helpdesk à l'adresse :https://my.kaspersky.com/fr

Vous pouvez rédiger votre demande en allemand, anglais, espagnol, français ou en russe.

Pour traiter votre demande par messagerie, vous devez indiquer le **numéro de client** reçu en même temps que votre **mot de passe** lors de votre enregistrement sur le site du Service d'assistance technique.

Si vous n'êtes pas encore inscrit en tant qu'utilisateur d'applications Kaspersky Lab, vous disposez d'un formulaire pour ce faire sur le site du Helpdesk (https://my.kaspersky.com/fr/registration). Pendant votre inscription, saisissez le *code d'activation* du logiciel ou le fichier *clé de licence*.

Vous recevrez la réponse d'in spécialiste du Service d'assistance technique dans votre Espace personnel (https://my.kaspersky.com/fr) et à l'adresse de messagerie précisée dans votre demande.

Décrivez votre problème avec tous les détails possibles dans le formulaire de saisie de votre demande. Spécifiez dans les champs obligatoires :

- **Le type de demande.** Choisissez la rubrique la plus proche du problème rencontré, par exemple, « Installation/Désinstallation du produit » ou « Analyse antivirus/Problème de suppression ». En l'absence de rubrique appropriée, sélectionnez « Question générale ».
- **Nom et version de l'application.**

- **Zone de texte.** Décrivez le problème rencontré avec le plus de détails possible.
- **Numéro client et mot de passe.** Saisissez l'Identifiant client et le mot de passe reçus lors de votre inscription sur le site du Service d'assistance technique.
- **Adresse de messagerie.** Les experts du Service d'assistance technique enverront leur réponse à cette adresse.

Assistance technique téléphonique

Si le problème est urgent, appelez le Service d'assistance technique de votre région. Avant de connecter localement (http://support.kaspersky.com/fr/desktop (Rubrique Contacter le Support Technique)) ou à l'international (http://support.kaspersky.com/fr/support/international) le Service d'assistance technique, préparez des informations (http://support.kaspersky.com/fr/support/details) sur votre appareil et sur l'application antivirus dont il est équipé. Ces informations réduiront le temps de réponse de nos spécialistes.

Forums de discussion sur les applications Kaspersky Lab

Si votre question n'est pas urgente, vous pouvez en débattre avec les spécialistes Kaspersky Lab ou avec d'autres utilisateurs de l'application antivirus Kaspersky Lab sur le forum du site Internet de Kaspersky Lab http://support.kaspersky.com/fr/forums.

Le forum permet de lire les conversations existantes, d'ajouter des commentaires, de créer de nouvelles rubriques et il dispose d'une fonction de recherche.

Spécifications matérielles et logicielles

Kaspersky Mobile Security 8.0 peut être installé sur des appareils mobiles avec l'un des systèmes d'exploitation suivants :

- Symbian OS 9.1, 9.2 et 9.3 Series 60 UI.
- Microsoft Windows Mobile 5.0, 6.0, 6.1.

Kit de distribution

Vous pouvez acquérir Kaspersky Mobile Security par Internet (le kit de distribution et la documentation du programme sont au format numérique). Vous pouvez également acquérir Kaspersky Mobile Security revendeurs de téléphonie mobile. Pour des détails sur la méthode d'achat et le kit de distribution, contactez notre Département commercial au info@kaspersky.fr.

KASPERSKY MOBILE SECURITY POUR SYMBIAN OS

Cette section décrit le fonctionnement de Kaspersky Mobile Security 8.0 sur des Smartphone équipés de Symbian OS version 9.1, 9.2, 9.3 ou Séries 60 UI.

Dans cette section

Installation de Kaspersky Mobile Security 11

Premiers pas 12

Protection en temps réel 17

Analyse à la demande 22

Contrôle du rétro éclairage 31

Anti-Spam 35

Contrôle parental 48

Antivol 58

Pare-feu 66

Chiffrement 68

Mise à jour des bases du programme 72

Journaux du logiciel 77

Affichage de la fenêtre d'état 78

Notifications sonores 79

Gestion de la licence 80

Désinstallation du programme 82

Installation de Kaspersky Mobile Security

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

1. Copiez le paquet de distribution du programme dans votre Smartphone. Pour ce faire, appliquez l'une des méthodes suivantes :
   - depuis la page de téléchargement du site de Kaspersky Lab ;
   - avec le programme Nokia PC Suite ;
   - avec une carte d'extension mémoire.
2. Lancez l'installation avec l'une des méthodes suivantes :

- avec le programme Nokia PC Suite ;
- en exécutant le paquet de distribution sur l'appareil.

3. Un message (voir figure suivante) s'affiche à l'écran ; choisissez **Oui** pour confirmer l'installation du programme.

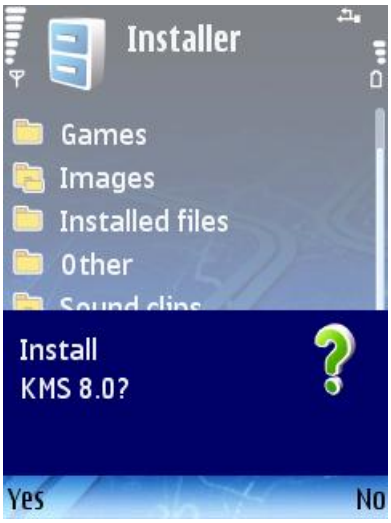

Figure 1 : Confirmation de l'installation

4. Visualisation des informations complémentaires du programme : nom, version, certificats. Appuyez sur **Continuer**.
5. Si la langue du système d'exploitation et celle de la version de Kaspersky Mobile Security ne correspondent pas, un message s'affiche à l'écran. Pour continuer l'installation en français, appuyez sur **OK**.
6. Lisez le contrat de licence (figure suivante). Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. En cas de désaccord avec les conditions du contrat de licence, choisissez **Annulation**. L'installation de Kaspersky Mobile Security sera interrompue.

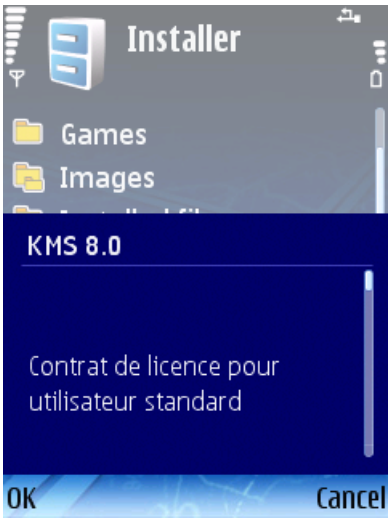

Figure 2 : Contrat de licence

7. Vérifiez qu'aucun autre logiciel antivirus n'est installé dans votre téléphone. Appuyez sur **OK**. Kaspersky Mobile Security sera installé dans l'appareil.

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

Premiers pas

Cette section décrit le démarrage du programme, les pré requis de son activation, l'utilisation de son interface et la définition du code secret.

Dans cette section

Activation du logiciel 13

Lancement du programme 14

Interface utilisateur 15

Code secret 16

Informations sur le programme 17

Activation du logiciel

Avant de démarrer. il faut d'abord activer Kaspersky Mobile Security. La procédure d'activation suppose de saisir le code d'activation puis de recevoir une clé que le logiciel utilise pour déterminer vos droits et la durée d'utilisation du programme.

Le code d'activation est disponible à l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html ou auprès des distributeurs Kaspersky Lab.

Pour activer Kaspersky Mobile Security, votre smartphone doit disposer d'une connexion Internet.

Avant de lancer l'activation, assurez-vous que la date et l'heure système de l'appareil sont correctes.

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

1. Ouvrez le menu principal de l'appareil.
2. Ouvrez le menu **Applications**.
3. Sélectionnez **KMS 8.0** et lancez le logiciel avec la commande **Ouvrir** dans le menu **Options**.
4. Sélectionnez **Saisissez le code** dans le menu **Options**.

La fenêtre d'activation de Kaspersky Mobile Security s'affiche à l'écran (voir figure suivante).

Figure 3 : Fenêtre d'activation du programme

5. Saisissez le code dans les 4 champs contigus. Le code d'activation est composé de lettres en alphabet latin et de chiffres, et n'est pas sensible à la casse. Après avoir saisi le code d'activation, sélectionnez **Activer** dans le menu **Options**.

6. Au moment de spécifier un point d'accès, sélectionnez le type de connexion utilisé pour la connexion au serveur.

   Le programme envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe le fichier clé.

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

Si l'installation du fichier clé réussit, les informations de licence sont affichées à l'écran. Pour commencer à utiliser le programme, appuyez sur **OK**.

Démarrage du logiciel

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

1. Ouvrez le menu principal de l'appareil.

2. Ouvrez le menu **Applications**.

3. Sélectionnez **KMS 8.0** et lancez le logiciel avec la commande **Ouvrir** dans le menu **Options**.

Après son démarrage, les principaux composants Kaspersky Mobile Security sont présentés dans une fenêtre (voir figure suivante) affichée à l'écran.

- **Protection en temps réel** – État de la protection en temps réel (voir section « Protection en temps réel » à la page 17).

- **Dernière analyse complete** – date et heure de la dernière analyse anti-virus de l'appareil (voir section « Analyse à la demande » à la page 22).

- **Mise à jour des bases** – date de publication des bases installées dans l'appareil (voir section « Mise à jour des bases du programme » à la page 72).

- **Anti-Spam** – état de la protection contre des messages entrants non sollicités (voir section « Anti-Spam » à la page 35).

- **Pare-feu** – niveau de protection de l'appareil contre des activités réseau indésirables (voir section « Pare-feu » à la page 66).

Figure 4 : La fenêtre d'état des composants du programme

Pour passer à l'interface du programme, appuyez sur **OK**.

Interface utilisateur

Les composants logiciels sont organisés par groupes, et leurs paramètres sont disponibles sur sept onglets :

- **Anti-Virus** – paramètres de protection en temps réel, d'analyse à la demande, de mise à jour des bases logicielles et de la quarantaine ainsi que les paramètres de planification des tâches d'analyse et de mise à jour.
- **Antivol** – paramètres nécessaires pour verrouiller l'appareil et effacer les données en cas de perte ou de vol.
- **Chiffrement** – paramètres de chiffrement permettant de protéger les informations présentes dans l'appareil.
- **Anti-Spam** – paramètres permettant de filtrer les appels et messages entrants indésirables.
- **Contrôle parental** – paramètres utilisés pour interdire les appels et messages sortants indésirables.
- **Pare-feu** – tous les paramètres de protection de l'activité réseau de l'appareil.
- **Informations** – paramètres généraux de fonctionnement ainsi que des informations sur le programme et sur les bases utilisées. L'onglet comprend également des informations sur la licence installée et la disponibilité de son renouvellement.

Pour vous déplacer d'un onglet à l'autre, utilisez le joystick de l'appareil ou sélectionnez **Ouvrir onglet** dans le menu **Options** (voir figure suivante).

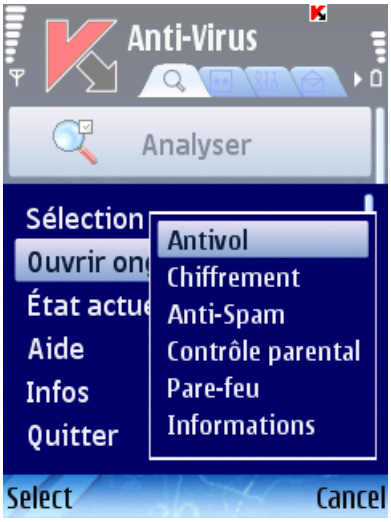

*Figure 5 : Le menu **Options***

➡ *Pour revenir à la fenêtre d'état des composants logiciels,*

Sélectionnez **État actuel** dans le menu **Options**.

Code secret

Le code secret est utilisé pour empêcher l'accès non autorisé aux paramètres des composants Antivol, Contrôle parental et Chiffrement ainsi que pour la création d'un SMS invisible, la désinstallation du logiciel et l'accès aux données chiffrées.

Pour définir le code secret, appliquez l'une des méthodes suivantes :

- Dans les paramètres des composants **Antivol**, **Contrôle parental** ou **Chiffrement**.
- Avec la commande **Changer le code** du menu **Paramètres** dans l'onglet **Informations.**

Nous recommandons d'utiliser un code secret composé d'au moins 7 chiffres.

➡ *Pour définir le code secret dans l'onglet **Informations**, procédez comme suit :*

1. Sélectionnez l'onglet **Informations**.
2. Dans l'onglet, sélectionnez **Paramètres**, puis **Changer le code**.
3. Dans la zone **Saisissez le code**, tapez les chiffres qui composeront votre code et appuyez sur **OK**. Tapez de nouveau ce code dans la zone **Confirmer**.

En outre, si le code n'est pas encore défini, vous pourrez le faire lors de votre accès aux paramètres des composants Antivol, Chiffrement ou Contrôle parental. En outre, les zones **Saisissez le nouveau code** et **Confirmation du code** seront affichées.

➡ *Pour changer le code secret, procédez comme suit :*

1. Sélectionnez l'onglet **Informations**.
2. Dans l'onglet, sélectionnez **Paramètres**, puis **Changer le code**.

3. Tapez le code actuel dans la zone **Saisissez le code**. Tapez le nouveau code dans la zone **Saisissez le nouveau code** puis de nouveau dans la zone **Confirmation du code** pour le confirmer.

En cas d'oubli du code secret, vous ne pourrez ni utiliser les fonctions de Kaspersky Mobile Security qui le demandent, ni désinstaller le logiciel.

Informations sur le programme

Vous pouvez afficher des informations générales sur le logiciel, ainsi que les détails de version et de copyright.

Pour afficher les informations sur le logiciel,

Sélectionnez **Infos** dans l'onglet **Informations** (voir figure suivante).

Figure 6 : Informations sur le programme

Protection en temps réel

Cette section décrit la protection en temps réel de votre appareil, comment l'activer et configurer ses paramètres.

Dans cette section

À propos de la protection en temps réel 18

Activation et désactivation de la protection en temps réel 18

Sélection des objets à analyser 19

Sélection d'actions sur les objets 20

Affichage de l'icône de protection 21

À propos de la protection en temps réel

La protection en temps réel est lancée au démarrage du système d'exploitation, elle reste chargée en permanence dans la mémoire RAM de l'appareil et surveille tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte toutes les tentatives d'accès aux fichiers de la part de l'utilisateur ou d'un autre programme.

2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés en les comparant aux bases de données du logiciel. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Après l'analyse, Kaspersky Mobile Security peut appliquer les actions suivantes :

   - Si du code malveillant est détecté dans un fichier, Kaspersky Mobile Security bloque le fichier et exécute l'action prévue dans la configuration.

   - Si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Des informations sur les résultats de l'analyse sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Activation et désactivation de la protection en temps réel

Le programme permet de contrôler l'état de protection en temps réel de l'appareil contre les objets malveillants.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour activer la protection en temps réel, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.

2. Sélectionnez **Protection en temps réel** dans la fenêtre **Paramètres**.

3. Sélectionnez **Actif** pour la protection en temps réel.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

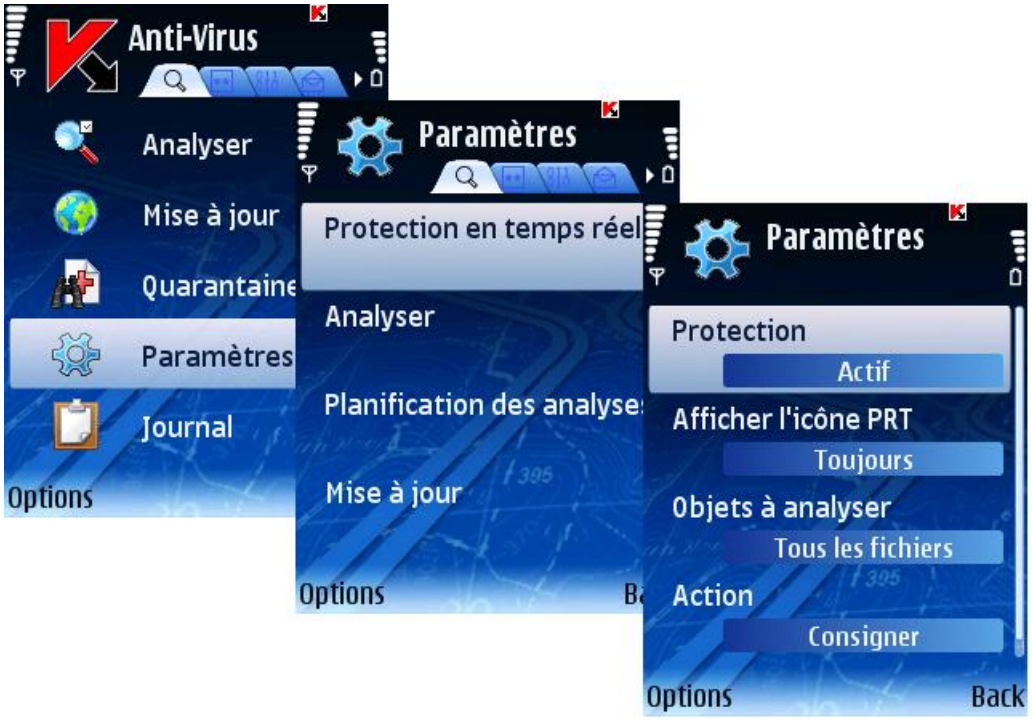

Figure 7 : Activation de la protection en temps réel

➡ *Pour désactiver la protection en temps réel, procédez de la manière suivante :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Protection en temps réel** dans la fenêtre **Paramètres**.
3. Sélectionnez **Inactif** pour la protection en temps réel.
4. Appuyez sur **Précédent** pour enregistrer les modifications.

Les spécialises de Kaspersky Lab recommandent vivement de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

Sélection des objets à analyser

Vous pouvez sélectionner le type d'objets à analyser par la protection en temps réel .

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

➡ *Pour sélectionner le type d'objets à analyser, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Protection en temps réel** dans la fenêtre **Paramètres**.

3. Sélectionnez le type de fichiers à analyser par la protection en temps réel avec les paramètres **Objets à analyser** :

   - **Tous les fichiers** : analyse tous les types de fichiers.
   - **Exécutables seuls** : analyse uniquement les fichiers exécutables (par exemple : *.exe, *.sis, *.mdl, *.app).

4. Sélectionnez **OK** pour enregistrer les modifications.

Figure 8 : Sélection d'objets à analyser

Sélection d'actions sur les objets

Vous pouvez configurer la réaction du programme en cas de détection d'un objet malveillant.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

➡ *Pour configurer la réponse du programme quand il détecte un objet malveillant, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Protection en temps réel** dans la fenêtre **Paramètres**.
3. Sélectionnez la réponse du programme quand il détecte un objet infecté dans le paramètre **Action**.

- **Consigner** : ignore l'objet malveillant et consigne des informations sur sa détection dans le journal du programme.
- **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
- **Quarantaine** : place en quarantaine les objets malveillants.

4. Sélectionnez **OK** pour enregistrer les modifications.

Figure 9 : Configuration de la réponse du programme quand il détecte un objet malveillant

Affichage de l'icône de protection

L'icône est un indicateur de l'état de protection en temps réel sur l'écran de l'appareil. Si la protection en temps réel est activée, l'icône sera affichée en couleur, dans le cas contraire, elle s'affichera en gris.

Vous pouvez configurer l'affichage de l'icône indicateur de l'état de protection sur l'écran de l'appareil.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

➡ *Pour configurer l'affichage de l'icône indicateur de l'état de protection, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Protection en temps réel** dans la fenêtre **Paramètres**.

3. Sélectionnez **Afficher l'icône PRT**. Configurez l'affichage de l'icône indicateur de l'état de protection sur l'écran de l'appareil :

   - **Toujours** : affiche l'icône du programme sur l'écran de l'appareil.
   - **Menu uniquement** : affiche l'icône du programme dans le menu de l'appareil et dans le menu de Kaspersky Mobile Security.
   - **Jamais** : l'icône n'est pas affichée.

4. Sélectionnez **OK** pour enregistrer les modifications.

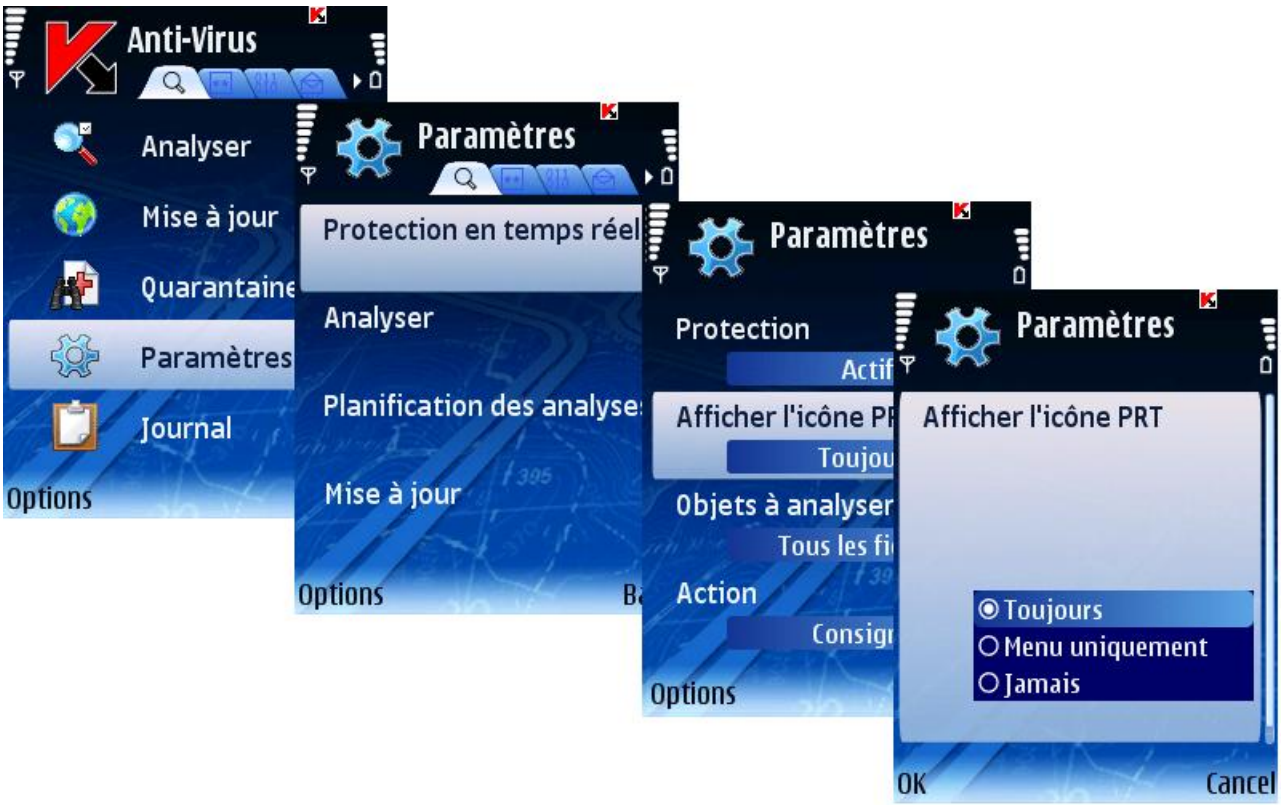

Figure 10 : Configuration de l'icône indicateur de l'état de protection

Analyse à la demande

Cette section décrit le composant **Analyser**, comment exécuter dans votre appareil une analyse antivirus de l'appareil, configurer les paramètres d'analyse et planifier l'exécution automatique des analyses.

Dans cette section

À propos de l'analyse à la demande 23

Exécution manuelle d'une analyse 23

Configuration d'analyses planifiées 25

Sélection des objets à analyser 26

Sélection des actions à appliquer sur les objets 27

Configuration de l'analyse de la ROM 29

Configuration de l'analyse de fichiers compressés 30

Contrôle du rétro éclairage 31

À propos de l'analyse à la demande

Kaspersky Mobile Security permet de faire une analyse complète ou partielle de la mémoire de l'appareil, de ses cartes d'extension, des messages et de la mémoire du système à la recherche d'objets malveillants.

Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés en les comparant aux bases de données logicielles. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour. Si du code malveillant est détecté dans un fichier, Kaspersky Mobile Security bloque le fichier et exécute l'action prévue dans la configuration.

L'exécution de l'analyse peut se faire manuellement ou de manière planifiée.

Des informations sur les résultats de l'analyse à la demande sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Exécution manuelle d'une analyse

Une analyse peut être lancée manuellement à tout moment approprié, par exemple, quand l'appareil n'est pas occupé par d'autres tâches.

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

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.
2. Dans la fenêtre **Analyse** (voir figure suivante) définissez la couverture d'analyse de l'appareil :
   - **Analyse tout** : analyse toute la mémoire de l'appareil et des cartes d'extension.
   - **Analyser RAM :** analyse des processus exécutés dans la mémoire du système et des fichiers correspondants.
   - **Analyser msgs** : analyse tous les messages.
   - **Analyser dossier** : sélection et analyse d'un certain dossier dans le système de fichiers ou dans les cartes d'extension de mémoire connectées à l'appareil.

     Quand l'option **Analyser dossier** est sélectionnée, une fenêtre présente le système de fichiers de l'appareil. Utilisez les boutons du joystick pour vous déplacer dans le système de fichiers. Pour analyser un

dossier, positionnez le curseur sur le répertoire que vous souhaitez analyser et sélectionnez **Analyser** dans le menu **Options**.

*Figure 11 : Onglet **Analyser***

Après le démarrage de l'analyse, une fenêtre affiche l'état de progression courante de la tâche : nombre d'objets analysés, chemin de l'objet en cours d'analyse et pourcentage d'objets analysés (voir figure suivante).

*Figure 12 : La fenêtre **Analyser***

Quand un objet infecté est détecté, l'action définie par le paramètre **Action** est appliquée (voir section « Sélection de l'action appliquée à un objet » à la page 27) conformément à la configuration de l'analyse.

Le logiciel ne demandera l'action à réaliser sur l'objet (voir figure suivante) que si la valeur **Interroger** est sélectionnée pour le paramètre **Action**.

Figure 13 : Message de détection d'un virus

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

Par défaut, le rétro éclairage est automatiquement désactivé pendant l'analyse, pour économiser les batteries. Vous pouvez activer le rétro éclairage avec le paramètre **Rétro éclairage** du menu **Paramètres**, dans l'onglet **Informations**.

Configuration d'analyses planifiées

Kaspersky Mobile Security permet de planifier des analyses automatiques de l'appareil à des heures programmées. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, l'action définie par le paramètre **Analyser** est exécutée sur cet objet.

Par défaut, la planification est désactivée.

Pour configurer l'affichage de l'icône indicateur de l'état de protection, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Planification des analyses** dans la fenêtre ouverte.
3. Configurez le paramètre **Analyse auto** :
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Spécifiez l'**Heure d'analyse auto.** dans le champ de saisie.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Spécifiez le **Jour d'analyse auto** et l'**Heure d'analyse auto**.
   - **Inactif** : désactive le démarrage de l'analyse planifiée.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 14 : Planification d'une analyse

Sélection des objets à analyser

Le programme permet de spécifier le type des objets analysés à la recherche de code malveillant.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour sélectionner les objets à analyser, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Analyser** dans la fenêtre ouverte.
3. Spécifiez le paramètre **Objets à analyser** :
   - **Tous les fichiers** : analyse tous les fichiers.
   - **Exécutables seuls** : analyse uniquement les fichiers exécutables (par exemple : *.exe, *.sis, *.mdl, *.app).

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

Figure 15 : Sélection d'objets à analyser

Sélection des actions à appliquer sur les objets

Vous pouvez configurer les actions appliquées par le programme quand il détecte un objet malveillant.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

➧ *Pour configurer la réponse du programme, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.

2. Sélectionnez **Analyser** dans la fenêtre **Paramètres** (voir figure suivante).

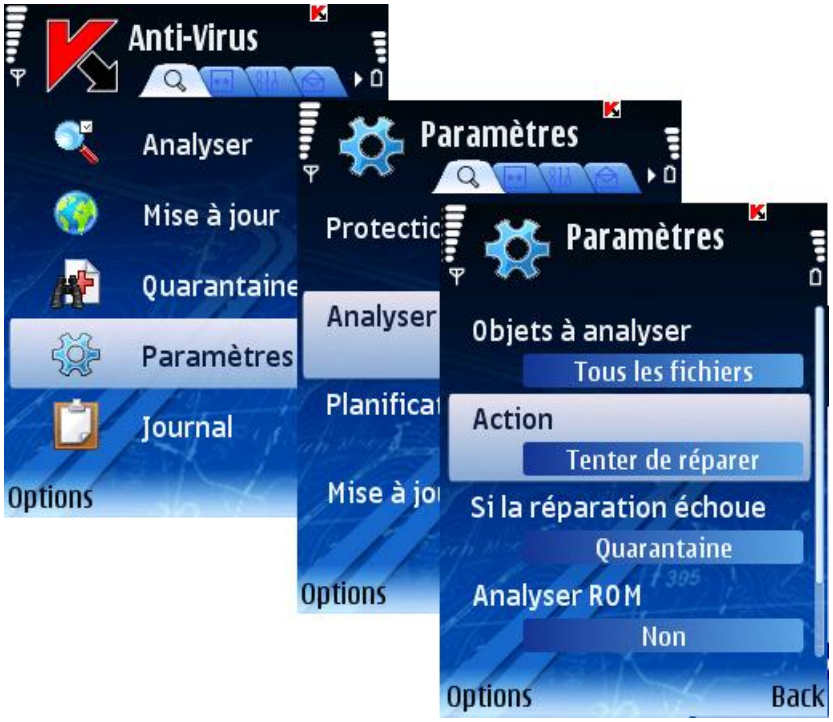

Figure 16 : Configuration des actions à appliquer sur les objets

3. Dans **Action**, sélectionnez la réponse de l'application en présence d'un objet malveillant (voir figure suivante) :

   - **Supprimer** : supprime les objets malveillants détectés sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants détectés.
   - **Interroger** : Quand un objet infecté est détecté, le programme demande à l'utilisateur de choisir une action.
   - **Consigner** : ignore l'objet malveillant et consigne des informations sur sa détection dans le journal du programme.
   - **Tenter de réparer** – répare les objets malveillants. Si la désinfection n'est pas possible, exécute l'action spécifiée dans la zone **Si la réparation échoue**.

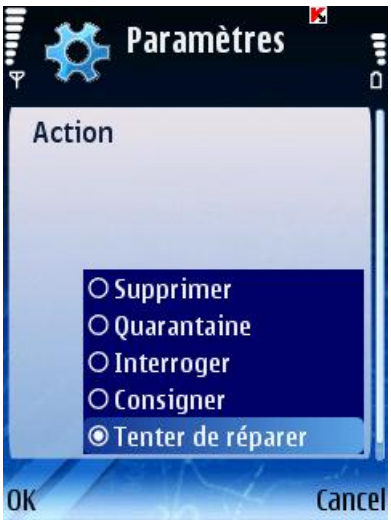

Figure 17 : Sélection des actions à appliquer sur les objets

4. Si vous avez choisi **Tenter de réparer** en tant que réponse de l'application, utilisez **Si la réparation échoue** (voir figure suivante) pour sélectionner l'action à appliquer quand il est impossible de désinfecter l'objet :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine des objets.
   - **Interroger** : demande à l'utilisateur de choisir une action quand un objet infecté est détecté.
   - **Consigner** : consigne des informations sur la détection d'objets infectés dans le journal de l'application.

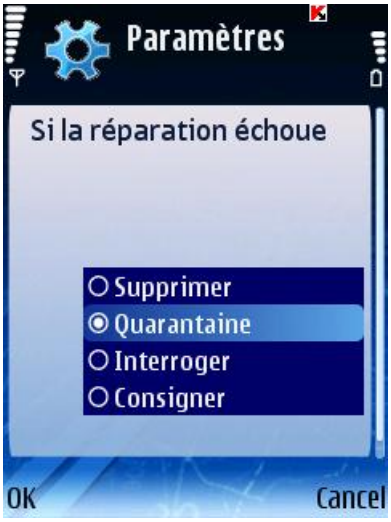

Figure 18 : Sélection de l'action secondaire

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

Configuration de l'analyse de la ROM

La mémoire ROM contient des fichiers système nécessaires au chargement du système de fichiers de l'appareil. Vous pouvez activer ou désactiver l'analyse de la ROM.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour activer l'analyse de la mémoire ROM de l'appareil, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Analyser** dans la fenêtre **Paramètres**.
3. Choisissez la valeur **Oui** pour le paramètre **Analyser ROM**.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

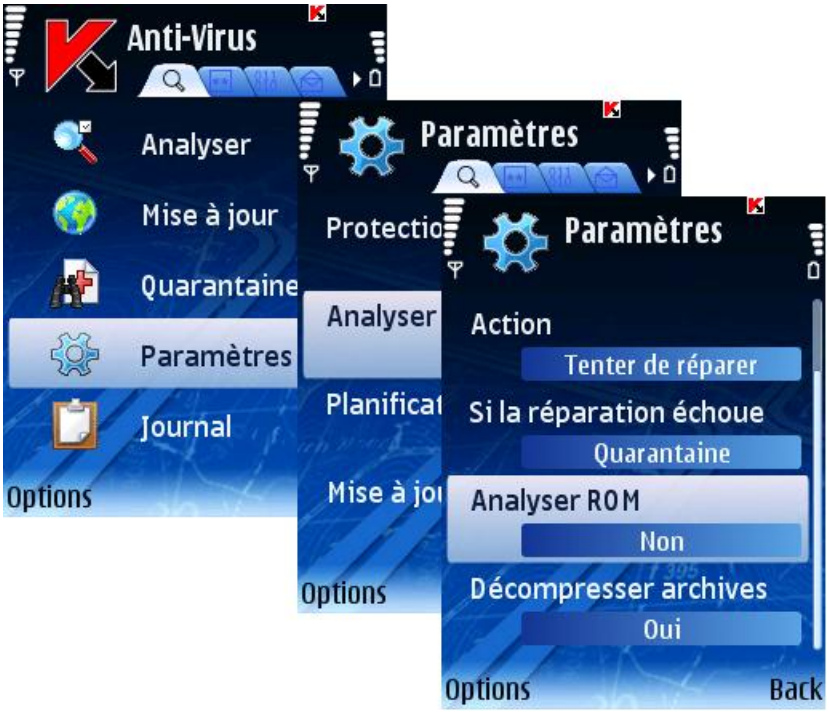

Figure 19 : Activation de l'analyse de la mémoire ROM de l'appareil

➡ *Pour désactiver l'analyse de la mémoire ROM de l'appareil, procédez de la manière suivante :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Analyser** dans la fenêtre **Paramètres**.
3. Choisissez la valeur **Non** pour le paramètre **Analyser ROM**.
4. Appuyez sur **Précédent** pour enregistrer les modifications.

Configuration de l'analyse de fichiers compressés

Vous pouvez activer ou désactiver l'extraction des archives compressées pour analyser leur contenu.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

➡ *Pour activer l'extraction des archives, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Analyser** dans la fenêtre **Paramètres**.
3. Choisissez la valeur **Oui** pour le paramètre **Décompresser archives**.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

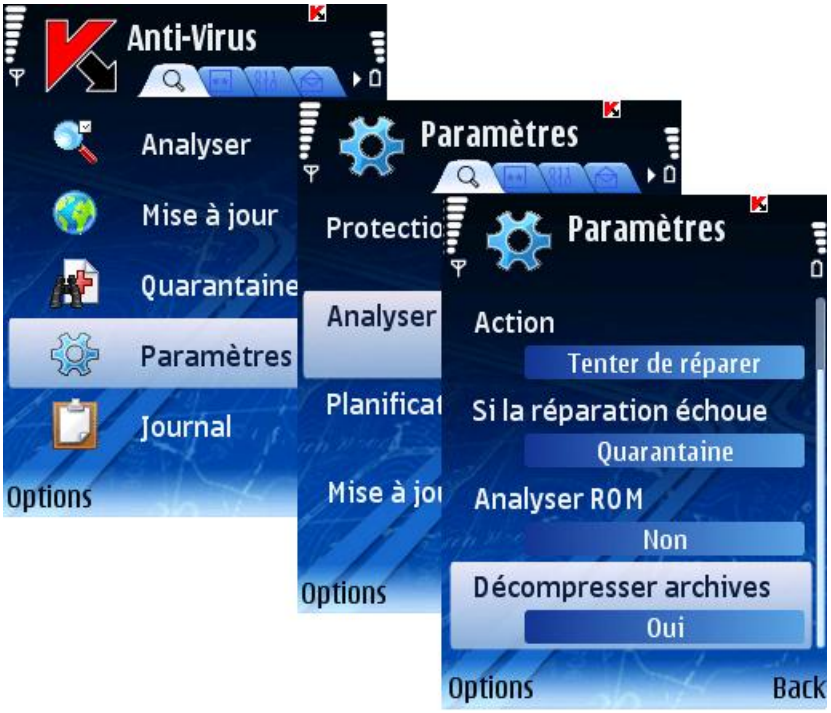

Figure 20 : Configuration de l'analyse des archives compressées

Contrôle du rétro éclairage

Le programme permet de configurer l'activation du rétro éclairage pendant l'exécution d'une analyse antivirus.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil 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 les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour configurer le rétro éclairage, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Informations**.
2. Sélectionnez la valeur requise pour le paramètre **Rétro éclairage** dans la fenêtre ouverte :
   - Si vous souhaitez que le rétro éclairage reste allumé en permanence pendant l'exécution d'une analyse antivirus, sélectionnez la valeur **Oui**.
   - Si vous souhaitez éteindre automatiquement le rétro éclairage, choisissez **Non**.

3. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 21 : Contrôle du rétro éclairage

Quarantaine

Cette section décrit la quarantaine et la gestion des objets infectés placés en quarantaine.

Dans cette section

À propos de la quarantaine 32

Affichage des objets en quarantaine 33

Restauration d'objets de la quarantaine 34

Suppression d'un objet de la quarantaine 34

À propos de la quarantaine

La quarantaine est une zone de stockage spécialisée dans laquelle Kaspersky Mobile Security place les objets potentiellement malveillants détectés lors d'une analyse ou par la protection en temps réel.

Les objets placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil. Les objets peuvent par la suite être supprimés ou restaurés par l'utilisateur.

Affichage des objets en quarantaine

➡ *Pour afficher la liste des objets en quarantaine,*

Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus** (voir figure suivante).

*Figure22 : Onglet **Anti-Virus***

La fenêtre **Quarantaine** ouverte contient une liste d'objets conservés dans la quarantaine (voir figure suivante).

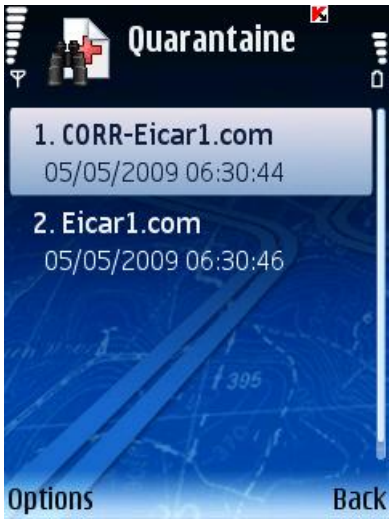

*Figure 23 : La fenêtre **Quarantaine***

Voir aussi

À propos de la quarantaine 32

Restauration d'objets de la quarantaine 34

Suppression d'un objet de la quarantaine 34

Restauration d'objets de la quarantaine

*Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.*

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.
2. Dans la fenêtre **Quarantaine** ouverte, sélectionnez l'objet que vous souhaitez restaurer.
3. Sélectionnez **Restaurer** dans le menu **Options**. L'objet sélectionné dans la quarantaine est restauré dans son dossier d'origine.

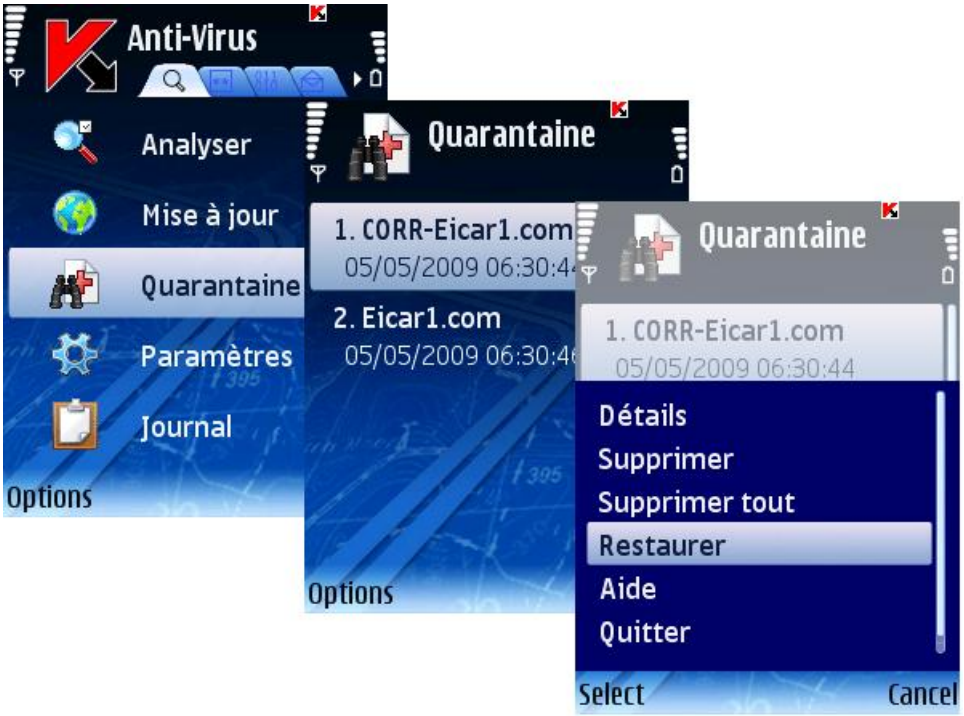

Figure 24 : Restauration d'objets depuis la quarantaine

Suppression d'un objet de la quarantaine

Pour supprimer un certain objet de la quarantaine, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.
2. Dans la fenêtre **Quarantaine** ouverte, sélectionnez l'objet que vous souhaitez supprimer.

3. Sélectionnez **Supprimer** dans le menu **Options**. L'objet sélectionné sera supprimé.

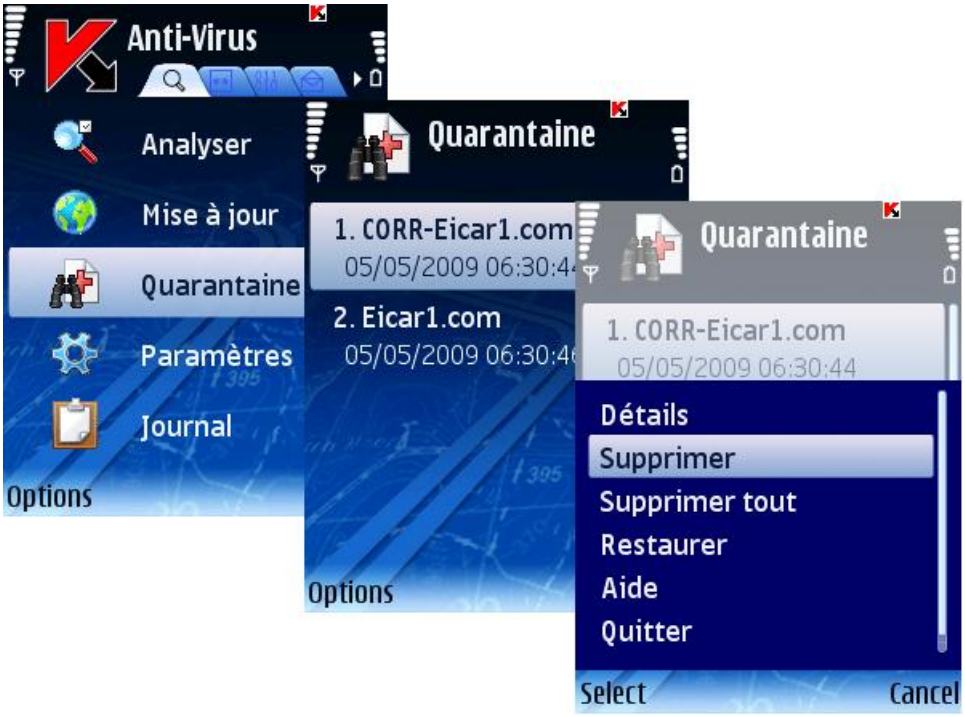

Figure 25 : Suppression d'un objet de la quarantaine

Pour supprimer tous les objets en quarantaine :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.
2. Dans le menu **Options**, choisissez **Supprimer tout**. Tous les objets en quarantaine seront éliminés.

Anti-Spam

Cette section décrit le composant Anti-Spam et la méthode à suivre pour composer les listes noire et blanche, configurer les modes de fonctionnement et d'autres paramètres du composant Anti-Spam.

Dans cette section

À propos du composant Anti-Spam 36

Anti-Spam modes 36

Création d'une liste noire 37

Création d'une liste blanche 41

Réponse aux messages et appels présents dans l'annuaire téléphonique 45

Réponse aux messages d'expéditeurs non numériques 45

Sélection de l'action à appliquer sur des messages entrants 47

Sélection de l'action à appliquer sur des appels entrants 48

À propos du composant Anti-Spam

Le composant Anti-Spam permet de protéger l'appareil contre la réception de messages et d'appels indésirables. Cette protection s'appuie sur le filtrage des messages SMS et des appels entrants au moyen d'une liste noire et d'une liste blanche. Ces listes contiennent respectivement des numéros de téléphone ou des échantillons de phrases typiques de messages SMS indésirables ou normaux.

Si une correspondance au moins est détectée avec un numéro de téléphone ou une phrase de la liste blanche, aucune vérification supplémentaire n'est réalisée et l'appel ou le message est transmis à l'appareil. Un message SMS ou un appel provenant d'un numéro de téléphone présent dans la liste noire ou un message SMS contenant du texte présent dans la liste noire sont interdits.

Des informations sur les messages SMS et les appels interdits sont enregistrés dans le journal (voir section « Journaux du logiciel Journaux » à la page 77).

Modes du composant Anti-Spam

Un mode de fonctionnement Anti-Spam est un ensemble de paramètres qui déterminent la protection de votre appareil contre les messages indésirables et les appels non sollicités.

Liste les modes de fonctionnement Anti-Spam disponibles :

- **Les deux listes** – filtrage des messages SMS et des appels entrants au moyen des listes noire et blanche. Quand un message SMS ou un appel provient d'un numéro qui ne figure dans aucune de ces listes, le module Anti-Spam affiche un message proposant de l'interdire ou de l'autoriser et d'ajouter ce numéro de téléphone à la liste blanche ou noire. Ce niveau est celui par défaut.
- **Liste noire** – interdiction des messages SMS et des appels présents dans la liste noire. Tous les autres messages SMS et appels sont autorisés.
- **Liste blanche** – autorisation des messages SMS et des appels présents dans la liste blanche. Tous les autres messages SMS et appels sont interdits.
- **Désactiver** – aucun filtrage de messages SMS ou d'appels n'est réalisé.

Pour sélectionner un mode Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Ouvrez l'onglet **Anti-Spam**.
2. Sélectionnez **Paramètres** puis **Anti-Spam** dans le menu.

3. Dans la fenêtre ouverte, sélectionnez le mode souhaité et appuyez sur **OK** pour enregistrer les modifications et quitter la fenêtre.

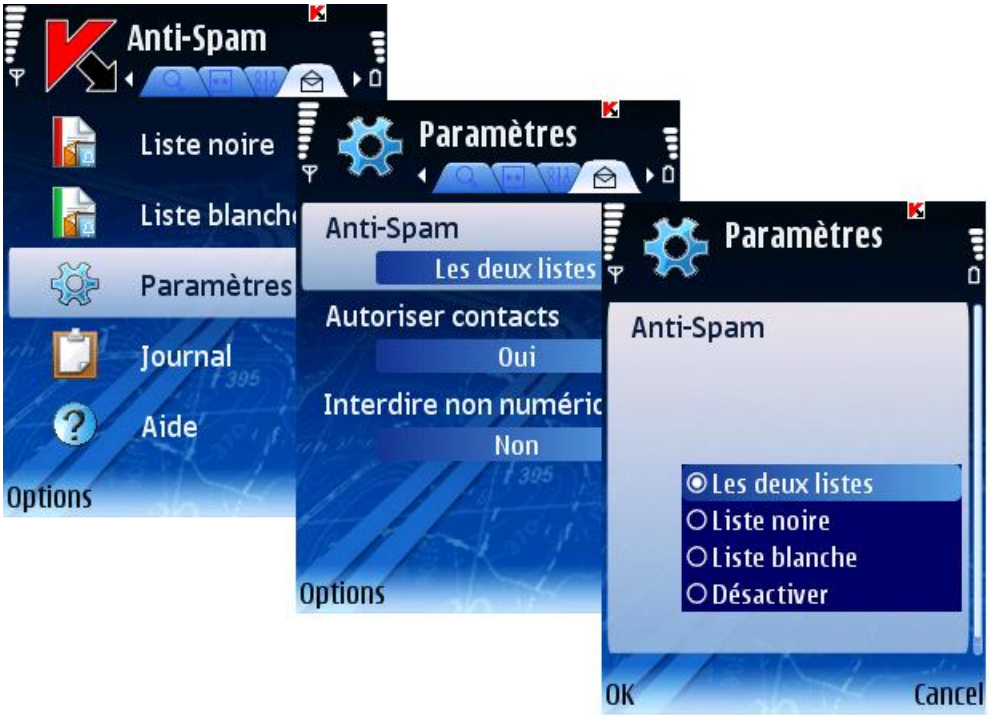

Figure 26 : Sélection de mode de fonctionnement Anti-Spam

Création d'une liste noire

Les enregistrements de cette liste contiennent les numéros de téléphone des SMS et des appels entrants qui seront interdits par le composant Anti-Spam, ainsi que les échantillons de texte qui, s'ils figurent dans un message SMS reçu, entraînent l'interdiction de celui-ci.

Des informations sur les messages SMS et les appels interdits sont enregistrés dans le journal (voir section « Journaux du logiciel » à la page 77).

Dans cette section

Ajout d'une nouvelle entrée 37

Modification d'une entrée existante 38

Suppression d'une entrée unique 39

Suppression de toutes les entrées 40

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste noire Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.
2. Sélectionnez **Ajouter entrée** dans le menu **Options**.
3. Définissez les paramètres suivants dans la fenêtre ouverte :

- **Type de message** – action à appliquer sur un message ou un appel :
  - **SMS seuls** : interdit les messages SMS entrants uniquement.
  - **Appels uniquement :** interdiction des appels entrants uniquement.
  - **SMS et appels** : interdit les appels et les messages SMS entrants.
- **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est interdite. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * » représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).
- **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, permet d'en interdire la réception. Ce paramètre n'est disponible que si la valeur **SMS seuls** est sélectionnée.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

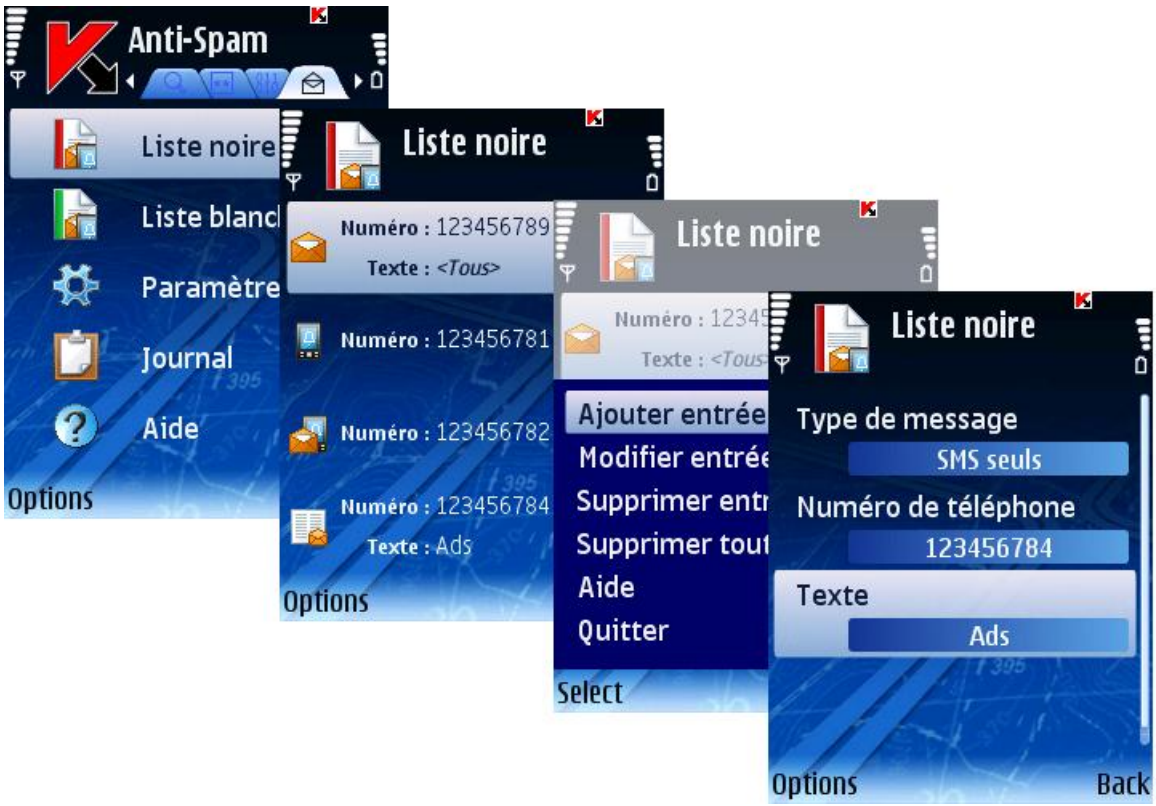

Figure 27 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier les paramètres d'une entrée existante, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.
2. Sélectionnez **Modifier entrée** dans le menu **Options**.
3. Définissez les paramètres suivants de l'entrée dans la fenêtre ouverte :
   - **Type de message** – action à appliquer sur un message ou un appel :

- **SMS seuls** : interdit les messages SMS entrants uniquement.
- **Appels uniquement :** interdit les appels entrants uniquement.
- **SMS et appels** : interdit les appels et les messages SMS entrants.

- **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est interdite. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * » représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).
- **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, permet d'en interdire la réception. Ce paramètre n'est disponible que si la valeur **SMS seuls** est sélectionnée.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 28 : Modification d'une entrée existante

Suppression d'une entrée unique

Pour supprimer une seule entrée de la liste noire, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.
2. Sélectionnez une entrée à supprimer dans la liste.

3. Sélectionnez **Supprimer entrée** dans le menu **Options**.

Figure 29 : Suppression d'une entrée existante

Suppression de toutes les entrées

➡ *Pour supprimer toutes les entrées, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

2. Sélectionnez **Supprimer tout** dans le menu **Options**.

Figure 30 : Suppression de toutes les entrées

Création d'une liste blanche

Les enregistrements de la **Liste blanche** contiennent les numéros de téléphone des SMS et des appels entrants autorisés par le composant Anti-Spam, ainsi que les échantillons de texte qui, s'il leur présence est détectée dans le message SMS reçu, permet de l'autoriser.

Dans cette section

Ajout d'une nouvelle entrée 41

Modification d'une entrée existante 42

Suppression d'une entrée unique 43

Suppression de toutes les entrées 44

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste blanche Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.
2. Sélectionnez **Ajouter entrée** dans le menu **Options**.
3. Définissez les paramètres de la nouvelle entrée dans la fenêtre ouverte :
   - **Type de message** – action à appliquer sur un message ou un appel :
     - **SMS seuls** : autorise les messages SMS entrants uniquement.

- **Appels uniquement** : autorise les appels entrants uniquement.
- **SMS et appels** : autorise les appels et les messages SMS entrants.

- **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * » représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).
- **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, en autorise la réception. Ce paramètre n'est disponible que si la valeur **SMS seuls** est sélectionnée.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

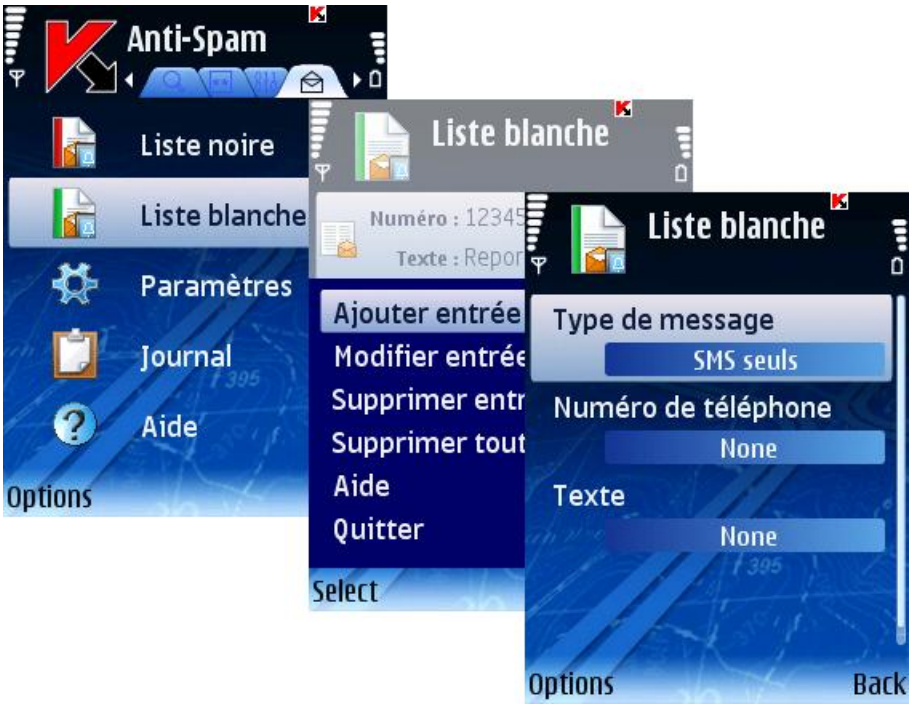

Figure 31 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier les paramètres d'une entrée existante, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.
2. Sélectionnez **Modifier entrée** dans le menu **Options**.
3. Définissez les paramètres suivants de l'entrée dans la fenêtre ouverte :
   - **Type de message** – action à appliquer sur un message ou un appel :
     - **SMS seuls** : autorise les messages SMS entrants uniquement.
     - **Appels uniquement :** autorise les appels entrants uniquement.
     - **SMS et appels** : autorise les appels et les messages SMS entrants.
   - **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut

contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * »représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).

- **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, en autorise la réception. Ce paramètre n'est disponible que si la valeur **SMS seuls** est sélectionnée.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 32 : Modification d'une entrée existante

Suppression d'une entrée unique

➧ *Pour supprimer une seule entrée de la liste noire, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

2. Sélectionnez une entrée à supprimer dans la liste.

3. Sélectionnez **Supprimer entrée** dans le menu **Options**.

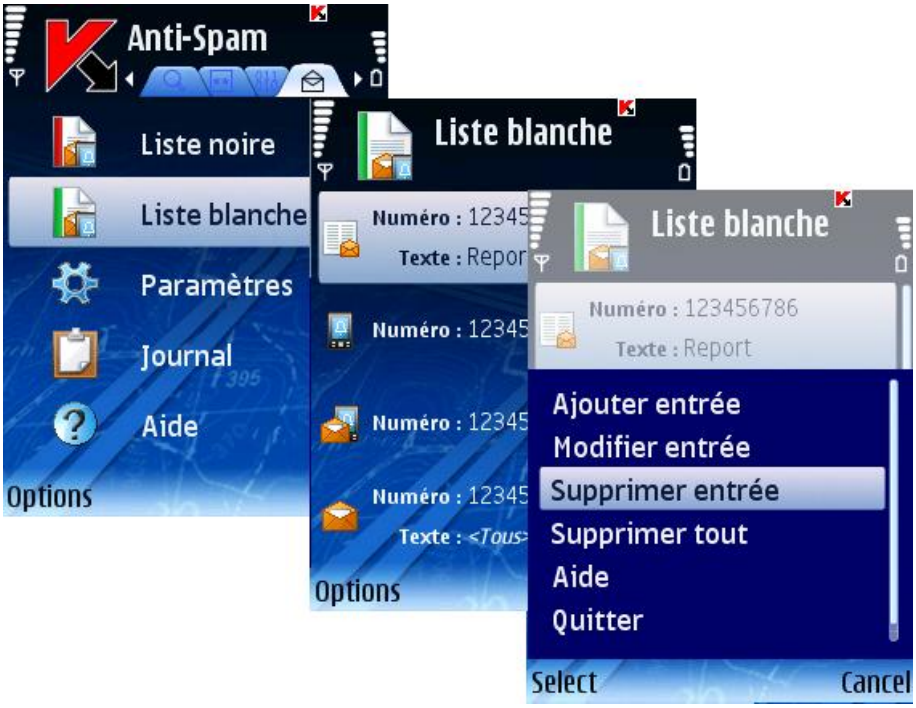

Figure 33 : Suppression d'une entrée existante

Suppression de toutes les entrées

➡ *Pour supprimer toutes les entrées, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.
2. Sélectionnez **Supprimer tout** dans le menu **Options**.

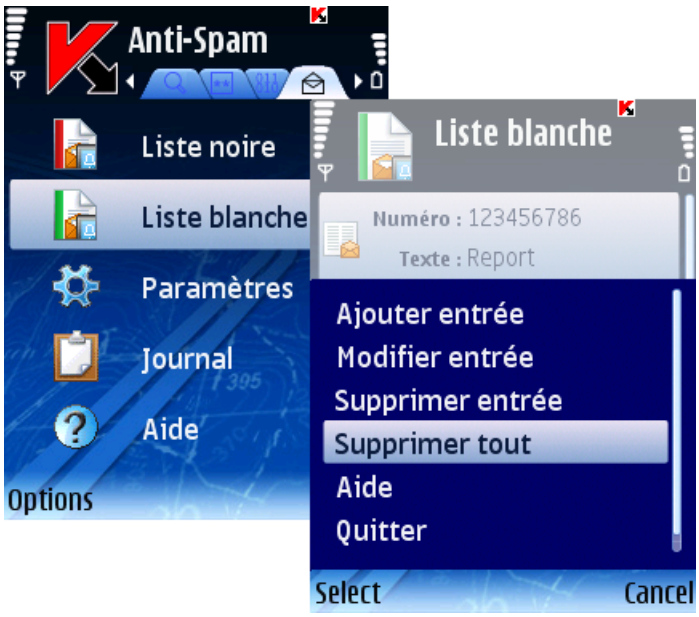

Figure 34 : Suppression de toutes les entrées

Réponse aux messages et appels présents dans l'annuaire téléphonique

Vous pouvez configurer la réponse du composant Anti-Spam aux messages SMS ou appels provenant de numéros présents dans l'annuaire téléphonique, sans prendre en compte les listes noire et blanche.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour configurer la réponse Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Spam**.
2. Dans la fenêtre ouverte, sélectionnez la valeur du paramètre **Autoriser contacts :**
   - Si vous souhaitez que le composant Anti-Spam autorise la réception de messages SMS ou d'appels provenant de numéros présents dans l'annuaire téléphonique, choisissez **Oui**.
   - Si vous souhaitez que le composant Anti-Spam assure le filtrage d'un numéro de téléphone en fonction de sa présence dans l'une des listes blanche ou noire, choisissez **Non**.
3. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 35 : Autorisation des contacts présents dans l'annuaire téléphonique

Réponse aux messages d'expéditeurs non numériques

Il est possible de configurer la réponse du programme lorsque des messages SMS proviennent d'expéditeurs non numériques (ne comprenant que des lettres).

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour configurer la réponse Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Spam**.
2. Dans la fenêtre ouverte, sélectionnez la valeur du paramètre **Interdire non numériques :**
   - Pour activer la suppression automatique des messages d'expéditeurs non numériques, choisissez **Oui**.
   - Si vous souhaitez que le composant Anti-Spam réagisse au numéro de téléphone en fonction de sa présence dans l'une des listes blanche ou noire, choisissez **Non**.
3. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 36: Interdiction des messages ou appels d'expéditeurs non numériques

Sélection de l'action à appliquer sur des messages entrants

Le composant Anti-Spam suggère de configurer la réponse aux messages SMS dont le numéro de téléphone ne figure dans aucune des listes noire ou blanche. Ce type de message sera intercepté par le composant Anti-Spam si le mode **Les deux listes** est sélectionné (voir section « Anti-Spam modes » à la page 36), et une notification est affichée sur l'écran de l'appareil (voir figure suivante).

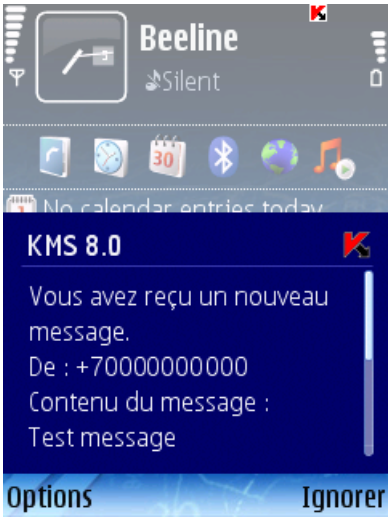

Figure 37 : Avertissement du module Anti-Spam

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

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

Des informations sur les messages interdits sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Sélection de l'action à appliquer sur des appels entrants

Le composant Anti-Spam suggère de configurer la réponse aux messages SMS dont le numéro de téléphone ne figure dans aucune des listes noire ou blanche. À la fin de l'appel, une notification est affichée sur l'écran de l'appareil (voir figure suivante).

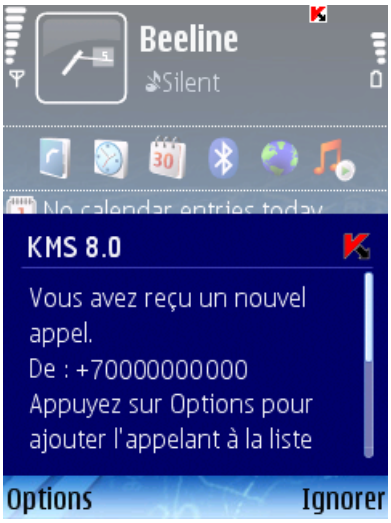

Figure 38 : Sélection des actions à appliquer sur des appels entrants

Utilisez le menu **Options** pour choisir l'une des actions suivantes à appliquer au numéro de téléphone de l'appelant :

- **Ajouter à la liste blanche** – ajoute le numéro de téléphone de l'appelant à la liste blanche.
- **Ajouter à la liste noire** – ajoute le numéro de téléphone de l'appelant à la liste noire.
- **Ignorer** – le numéro de l'appelant n'est pas ajouté à l'une ou l'autre des listes.

Des informations sur les appels interdits sont consignées dans le journal du logiciel (voir section « Journaux du logiciel» à la page 77).

Contrôle parental

Cette section décrit le composant Contrôle parental et la méthode à suivre pour composer les listes noire et blanche, configurer les modes de fonctionnement et d'autres paramètres du composant Contrôle parental.

Dans cette section

À propos du contrôle parental 48

Modes du contrôle parental 49

Création d'une liste noire 50

Création d'une liste blanche 54

À propos du contrôle parental

Le fonctionnement du composant Contrôle parental s'appuie sur le filtrage des messages SMS et des appels sortants au moyen d'une liste noire et d'une liste blanche.

Si une correspondance est détectée, l'analyse est interrompue. Les messages SMS et appels qui correspondent à n'importe quelle entrée de la liste noire sont interdits, tandis que ceux qui correspondent à une entrée de la Liste blanche sont autorisés.

Le contrôle parental n'interdit que les messages SMS envoyés uniquement à l'aide des fonctions standards de l'appareil.

La première fois que vous accédez au contrôle parental, vous devez définir un code secret (à la page 16) (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé aux Paramètres du Contrôle parental. Le code permet également d'accéder à la configuration du chiffrement et de l'Antivol.

Des informations sur l'activité du composant sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Modes du contrôle parental

Un mode de fonctionnement du contrôle parental est un ensemble de paramètres qui déterminent la protection de votre appareil contre les messages indésirables et les appels non sollicités.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Liste noire** – interdiction des messages SMS et des appels dont seuls les numéros sont présents dans la liste noire. Tous les autres messages sont autorisés.
- **Liste blanche** – autorisation des messages SMS et des appels dont seuls les numéros sont présents dans la liste blanche. Tous les autres messages sont interdits.
- **Inactif** – le contrôle parental est à l'arrêt. Aucun filtrage de messages SMS ou d'appels n'est réalisé.

Pour sélectionner le mode de fonctionnement du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez l'onglet **Contrôle parental**.
2. Sélectionnez **Paramètres** puis **Contrôle parental** dans le menu.

3. Sélectionnez le mode souhaité puis appuyez sur **OK** pour enregistrer les modifications.

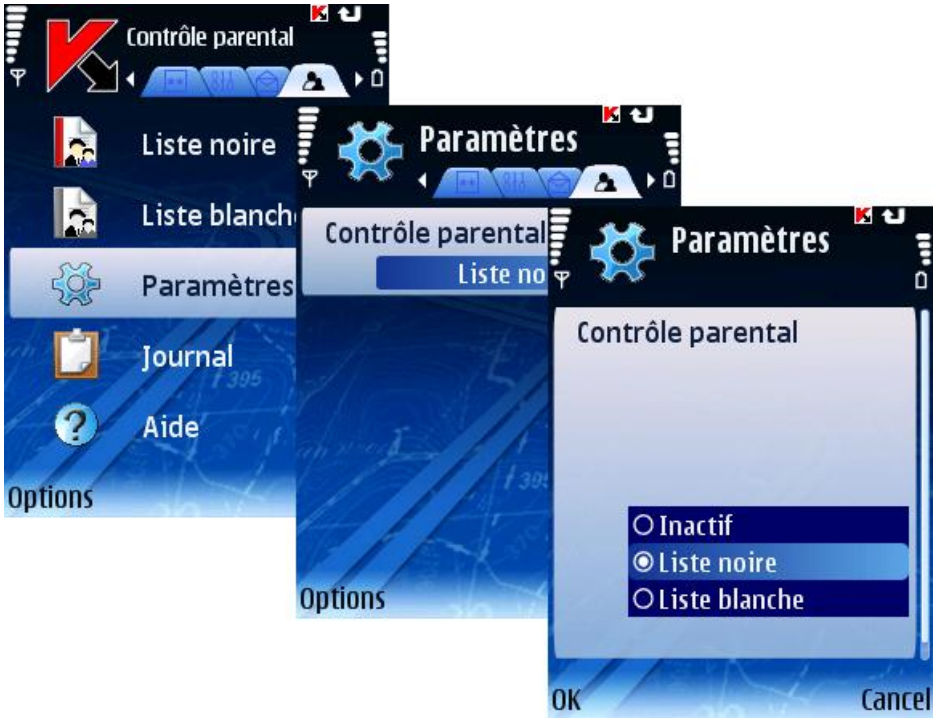

Figure 39 : Modes de fonctionnement du contrôle parental

Création d'une liste noire

Les entrées de la liste noire contiennent les numéros de téléphone des SMS ou des appels qui seront interdits par le contrôle parental.

Des informations sur les messages SMS et les appels interdits sont enregistrés dans le **Journal** (voir section « Journaux du logiciel» à la page 77).

Dans cette section

Ajout d'une nouvelle entrée 50

Modification d'une entrée existante 51

Suppression d'une entrée unique 52

Suppression de toutes les entrées 53

Ajout d'une nouvelle entrée

Pour ajouter une entrée à la liste noire du Contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.
2. Sélectionnez **Ajouter entrée** dans le menu **Options**.
3. Définissez les paramètres de la nouvelle entrée dans la fenêtre ouverte :
   - **Type de message** – action à appliquer sur un message ou un appel :

- **SMS seuls** : interdit les messages SMS sortants uniquement.
- **Appels uniquement** : interdit les appels sortants uniquement.
- **SMS et appels** : interdit les appels et les messages SMS sortants.

- **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels sortants est interdit. Ce numéro peut commencer par un chiffre ou par le signe « + » et ne peut contenir que des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * »représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 40 : Ajouter d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier les paramètres d'une entrée existante, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.
2. Sélectionnez **Modifier entrée** dans le menu **Options**.
3. Définissez les paramètres suivants de l'entrée dans la fenêtre ouverte :

- **Type de message** – action à appliquer sur un message ou appel :
  - **SMS seuls** : interdit les messages SMS sortants uniquement.
  - **Appels uniquement** : interdit les appels sortants uniquement.
  - **SMS et appels** : interdit les appels et les messages SMS sortants.
- **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels sortants est interdit. Ce numéro peut commencer par un chiffre ou par le signe « + » et ne peut contenir que des chiffres. En outre, pour

indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * »représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 41 : Modification d'une entrée existante

Suppression d'une entrée unique

Pour supprimer une entrée individuelle dans la liste noire :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.

2. Sélectionnez une entrée à supprimer.

3. Sélectionnez **Supprimer entrée** dans le menu **Options**.

Figure 42 : Suppression d'une entrée existante

Suppression de toutes les entrées

➡ *Pour supprimer toutes les entrées, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.

2. Sélectionnez **Supprimer tout** dans le menu **Options**.

Figure 43 : Suppression de toutes les entrées

Création d'une liste blanche

Les enregistrements de la **Liste blanche** contiennent les numéros de téléphone des SMS et des appels autorisés par le contrôle parental.

Dans cette section

Ajout d'une nouvelle entrée 54

Modification d'une entrée existante 55

Suppression d'une entrée unique 56

Suppression de toutes les entrées 57

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste blanche du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.
2. Sélectionnez **Ajouter entrée** dans le menu **Options**.
3. Définissez les paramètres du nouvel enregistrement dans la fenêtre ouverte :
   - **Type de message** – action à appliquer sur un message ou un appel :
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Appels uniquement** : autorise les appels sortants uniquement.
- **SMS et appels** : autorise les appels et les messages SMS sortants.

- **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels sortants est autorisé. Ce numéro peut commencer par un chiffre ou par le signe « + » et ne peut contenir que des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * »représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 44 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier les paramètres d'une entrée existante, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.
2. Sélectionnez **Ajouter entrée** dans le menu **Options**.
3. Définissez les paramètres suivants de l'entrée dans la fenêtre ouverte :

- **Type de message** – action à appliquer sur un message ou un appel :
  - **SMS seuls** : autorise les messages SMS sortants uniquement.
  - **Appels uniquement** : autorise les appels sortants uniquement.
  - **SMS et appels** : autorise les appels et les messages SMS sortants.
- **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels sortants est autorisé. Ce numéro peut commencer par un chiffre ou par le signe « + » et ne peut contenir que des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * » (où « * »représente une suite de caractères quelconques et « ? » - n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 45 : Modification d'une entrée existante

Suppression d'une entrée unique

Pour supprimer une entrée individuelle dans la liste blanche, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.
2. Sélectionnez une entrée à supprimer.

3. Sélectionnez **Supprimer entrée** dans le menu **Options**.

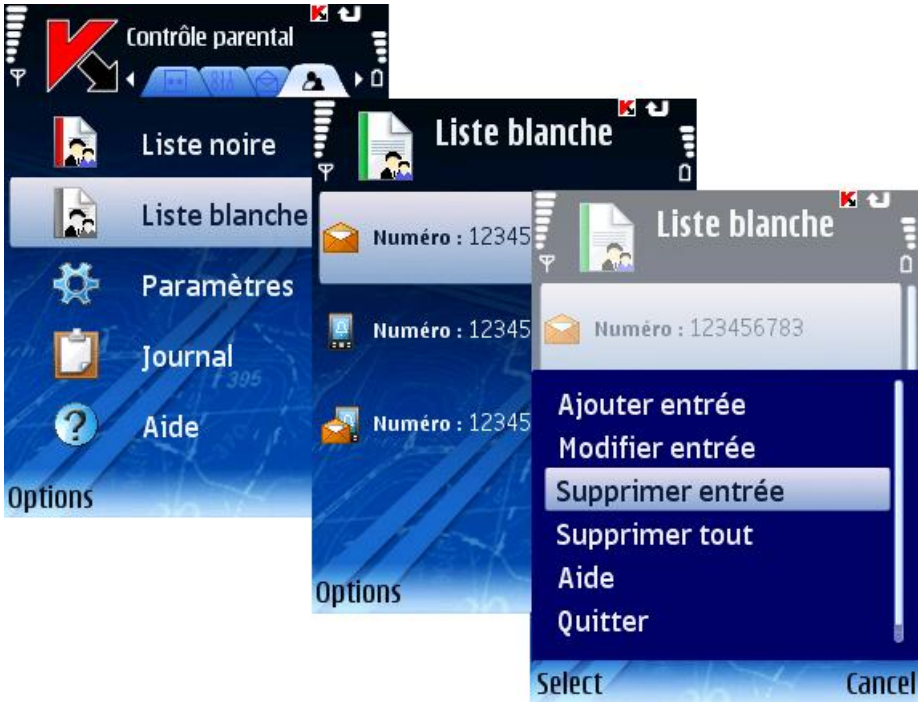

Figure 46 : Suppression d'une entrée existante

Suppression de toutes les entrées

➡ *Pour supprimer toutes les entrées, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.

2. Sélectionnez **Supprimer tout** dans le menu **Options**.

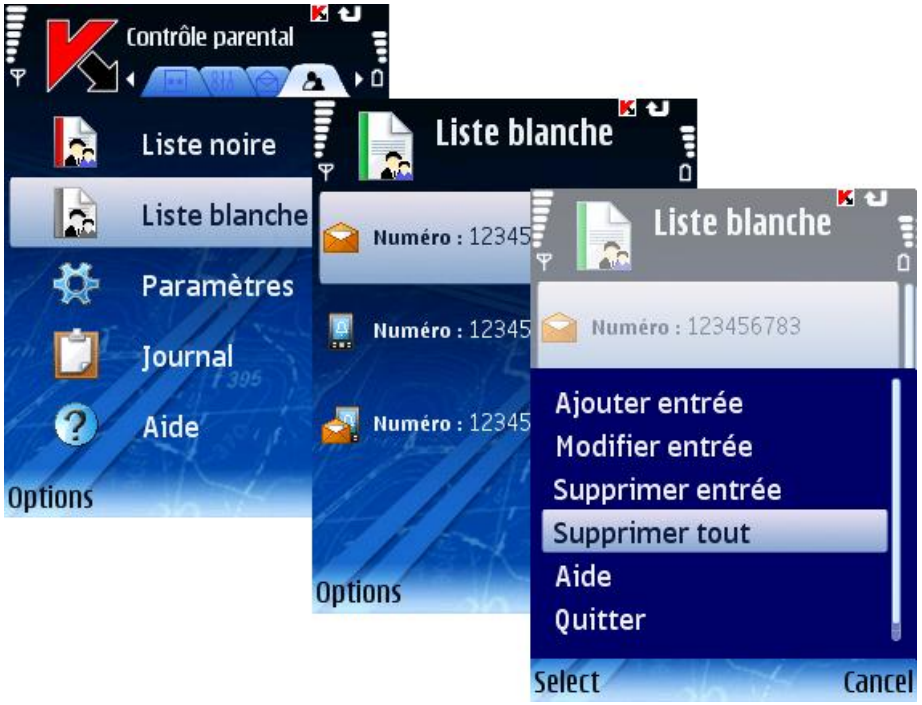

Figure 47 : Suppression de toutes les entrées

Antivol

Cette section décrit le fonctionnement du composant Antivol, conçu pour protéger les informations en cas de vol de l'appareil.

Dans cette section

À propos du composant Antivol 58

Fonction Verrouillage 59

Verrouillage de l'appareil 59

Fonction Suppression 60

Suppression de données personnelles 61

Fonction SIM-Surveillance 62

Fonction Localisation 63

Détermination des coordonnées de l'appareil 64

Fonction SMS Invisible 65

À propos du composant Antivol

Le composant Antivol est conçu pour protéger les données de l'appareil contre tout accès non autorisé en cas de perte ou de vol.

Ce composant dispose des fonctions suivantes :

- **Verrouillage** – verrouillage l'appareil à la demande de l'utilisateur.
- **Suppression** – suppression des informations personnelles (tous les contacts, messages, galerie, calendrier, journal, paramètres de connexion réseau), les données des cartes d'extension et les fichiers du dossier C:\Data.
- **SIM-Surveillance** – permet, en cas de remplacement ou de mise en marche de l'appareil sans la carte SIM, de récupérer le nouveau téléphone au numéro ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil volé.
- **Localisation** – permet de récupérer les coordonnées géographiques de l'appareil volé par message SMS sur un autre appareil ou dans une adresse de messagerie spécifiée. Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré.
- **SMS invisible** – permet de créer un message SMS spécial pour verrouiller l'appareil, supprimer les données personnelles et déterminer ses coordonnées géographiques.

La première fois que vous accédez au composant Antivol, vous devez définir un code secret (à la page 16) (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé aux paramètres Antivol. Ce code permet également d'accéder à la configuration du chiffrement et du contrôle parental ainsi qu'à la création d'un SMS invisible.

Des informations sur l'activité du composant sont consignées dans le journal du logiciel (voir section « Journaux du logiciel» à la page 77).

Fonction Verrouillage

La fonction **Verrouillage** permet de verrouiller l'appareil si nécessaire. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Pour activer la fonction Verrouillage, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Antivol**.
2. Sélectionnez **Verrouillage** dans la fenêtre ouverte.
3. Utilisez **Changer** dans le menu **Options** et choisissez **Actif**.
4. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 48 : Activation de la fonction Verrouillage

Verrouillage de l'appareil

Pour verrouiller un appareil, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- à l'aide de la fonction SMS invisible sur un autre appareil avec Kaspersky Mobile Security installé ;
- à l'aide des fonctions standards de création de messagerie SMS de votre téléphone.

Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Sélectionnez **Verrouillage** et appuyez sur **Suivant**.
3. Tapez le numéro de téléphone de l'appareil à verrouiller. Cliquez sur **Suivant**.

4. Entrez le code secret et appuyez sur **Envoi**.

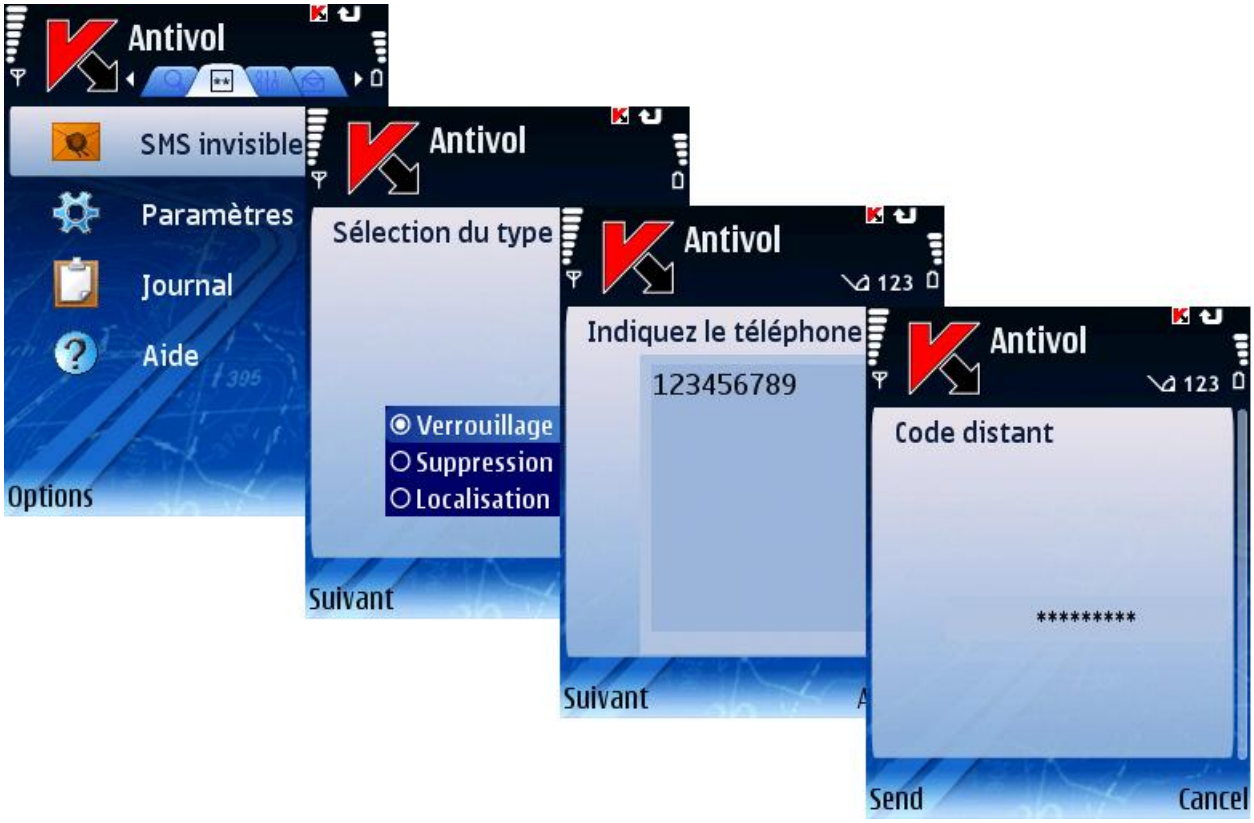

Figure 49 : Verrouillage de l'appareil

Pour créer un message SMS avec les fonctions standards de votre téléphone :

envoyez à l'appareil un message SMS avec le texte `block:<code>` (où `<code>` est le code secret défini sur l'appareil à verrouiller). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Fonction Suppression

La fonction **Suppression** permet de supprimer les informations personnelles (tous les contacts, messages, galerie, calendrier, journal, paramètres de connexion réseau), les données des cartes d'extension et les fichiers du dossier C:\Data dès que l'appareil reçoit un message SMS spécial.

Pour configurer le fonctionnement de la fonction Suppression, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Antivol**.
2. Dans la fenêtre ouverte choisissez **Suppression**.
3. Dans la fenêtre ouverte sélectionnez les données qui seront supprimés dès la réception du message SMS spécial par l'appareil.
   - Pour supprimer vos données personnelles, sélectionnez **Supprimer données** et choisissez **Oui**.

     Les contacts seront éliminés sur l'annuaire téléphonique et sur la carte SIM de l'appareil.

   - Pour que vos fichiers personnels (dossier C:\Data) soient supprimés, sélectionnez **Supprimer fichiers** et choisissez **Oui**.

- Pour supprimer les données de toutes les cartes mémoire installées, sélectionnez **Suppr. fichiers cartess** et définissez la valeur à **Oui**.

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

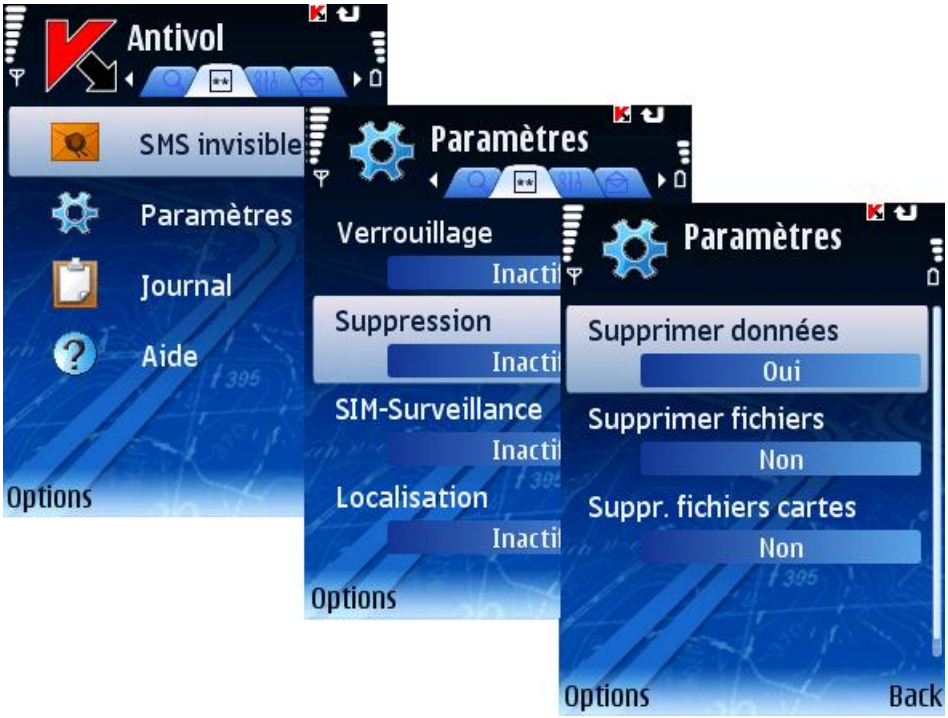

Figure 50 : Configuration de la fonction Suppression

Suppression de données personnelles

Pour supprimer les données personnelles de l'appareil, si la fonction Suppression est activée, vous disposez des méthodes suivantes :

- à l'aide de la fonction SMS invisible sur un autre appareil avec Kaspersky Mobile Security installé ;
- à l'aide des fonctions standards de messagerie SMS de votre téléphone.

Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Sélectionnez **Suppression** et appuyez sur **Suivant**.
3. Tapez le numéro de téléphone de l'appareil dont vous souhaitez supprimer les données. Cliquez sur **Suivant**.

4. Entrez le code secret défini sur l'appareil destinataire du message et appuyez sur **Envoi**.

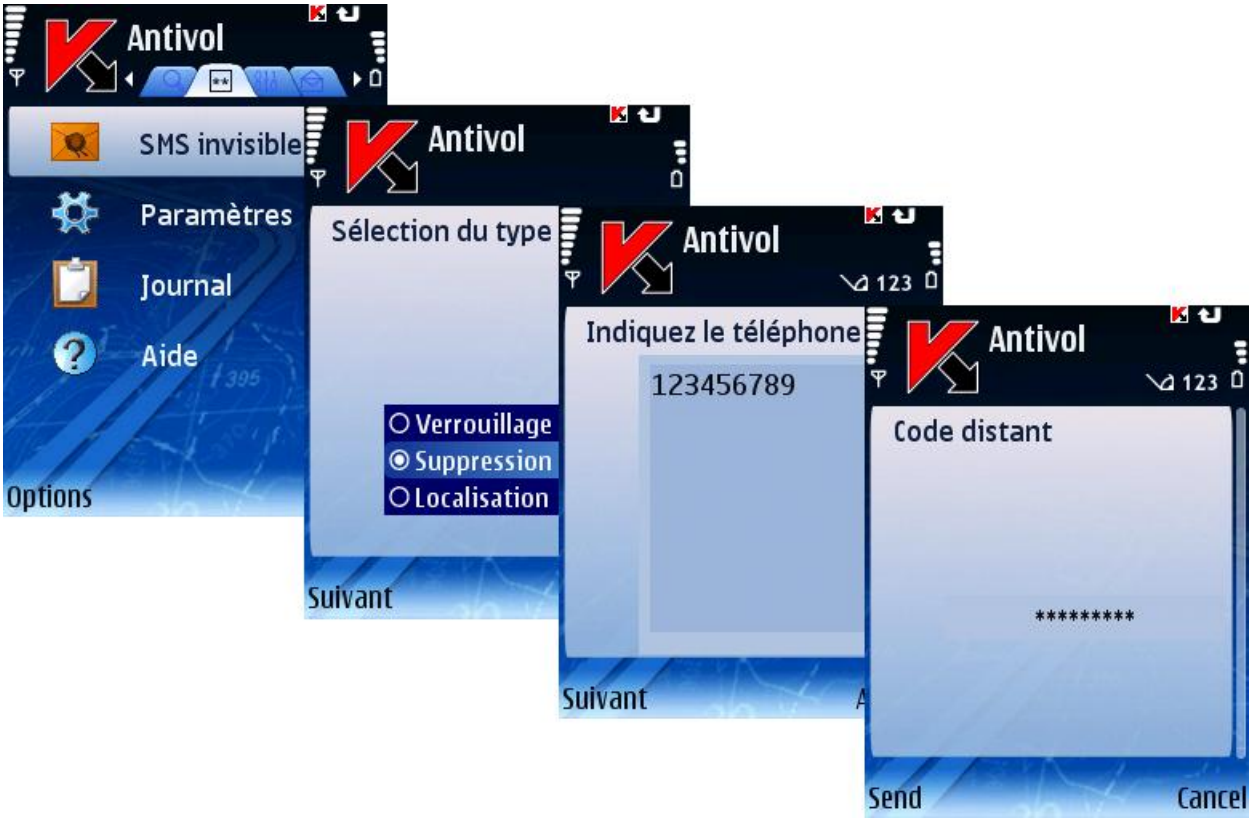

Figure 51 : Suppression de données personnelles

➡ *Pour créer un message SMS avec les fonctions standards de votre téléphone :*

envoyez à l'appareil un message SMS contenant le texte `clean:<code>` (où `<code>` est le code secret défini sur l'appareil récepteur. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Fonction SIM-Surveillance

SIM-Surveillance permet, en cas de remplacement de la carte SIM, de récupérer le nouveau téléphone au numéro ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil perdu ou volé.

Par défaut la fonction **SIM-Surveillance** est désactivée.

➡ *Pour configurer le fonctionnement de la fonction SIM-Surveillance, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Antivol**.

2. Sélectionnez **SIM-Surveillance** dans la fenêtre ouverte.

3. Dans le menu qui s'affiche (voir figure suivante) configurez les paramètres de surveillance en cas de remplacement de la carte SIM de l'appareil.

   - Dans la zone **Numéro de téléphone**, tapez le numéro de téléphone destinataire du message contenant le nouveau numéro de téléphone en cas de remplacement de la carte SIM de votre appareil. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.

   - Dans la zone **Adresse courriel**, tapez l'adresse de messagerie destinataire du message contenant le nouveau numéro de téléphone.

- Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, définissez le paramètre **Verrouiller l'appareil** à **Oui**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret. Par défaut, le verrouillage de l'appareil est désactivé.

4. Appuyez sur **OK** pour enregistrer les modifications apportées.

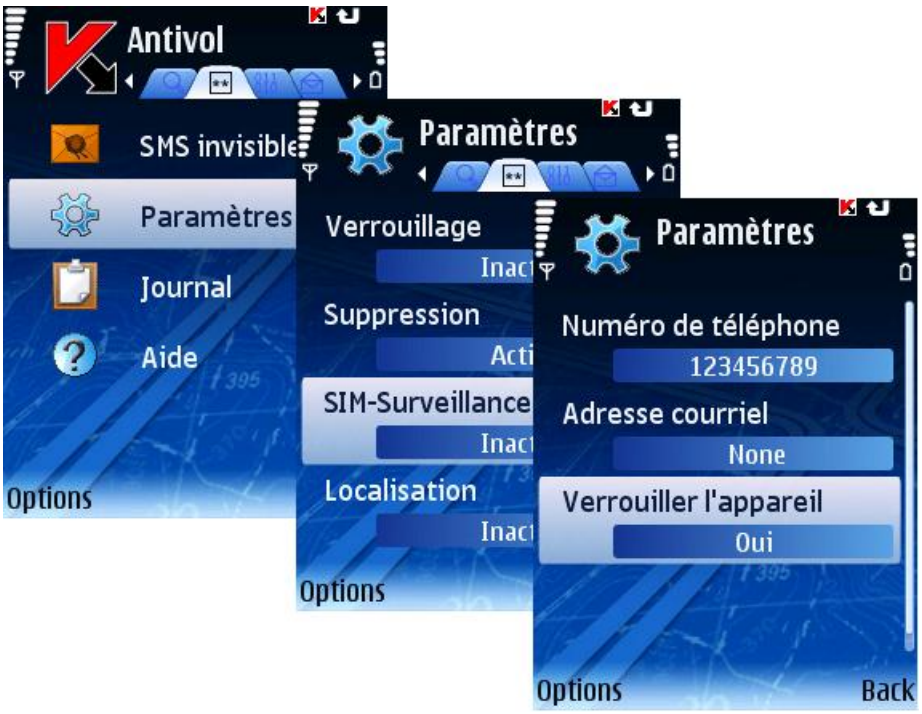

Figure 52 : Configuration de la fonction SIM-Surveillance

Fonction Localisation

La fonction **Localisation** permet de récupérer les coordonnées géographiques de l'appareil volé par message SMS sur un autre appareil ou dans une adresse de messagerie spécifiée.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. Si nécessaire, le récepteur sera activé automatiquement.

Vous ne pouvez recevoir les coordonnées que si l'appareil se trouve dans une zone couverte par satellite. Si aucun satellite n'est disponible au moment de la requête, des tentatives de localisation régulières sont répétées jusqu'au redémarrage de l'appareil.

➡ *Pour activer la fonction Localisation, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Antivol**.

2. Dans la fenêtre ouverte choisissez **Localisation**.

3. Dans la fenêtre ouverte, précisez l'adresse de messagerie (paramètre **Adresse courriel**) destinataire des coordonnées de l'appareil, en plus du message SMS, et appuyez sur **OK**.

4. Sélectionnez **Oui** dans la fenêtre ouverte.

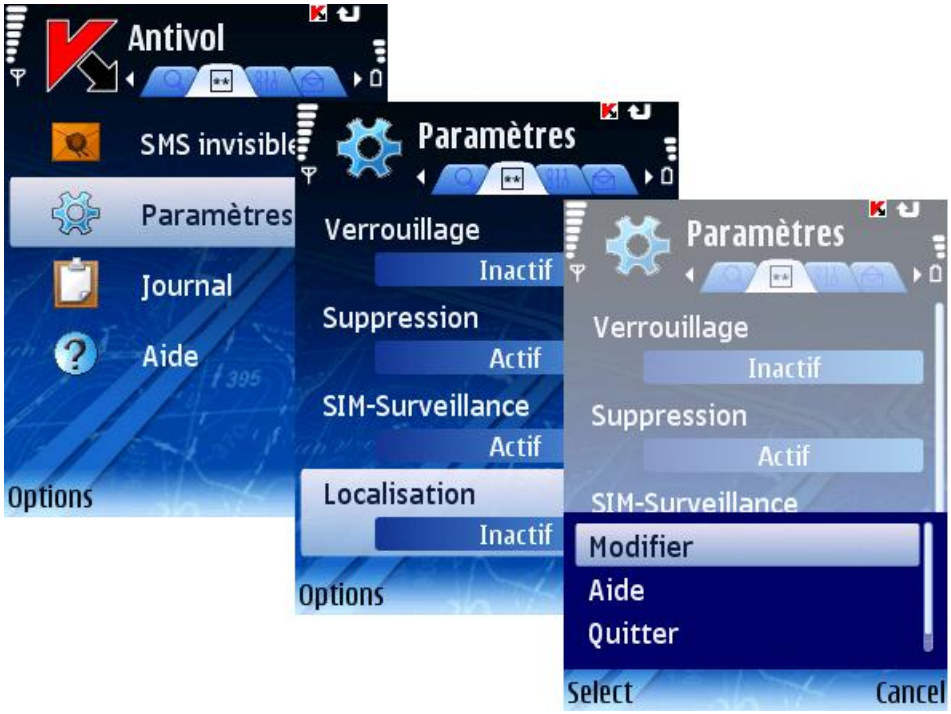

Figure 53 : Configuration de la fonction Localisation

Détermination des coordonnées de l'appareil

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, vous disposez des méthodes suivantes :

- à l'aide de la fonction SMS invisible sur un autre appareil avec Kaspersky Mobile Security préinstallé ;
- à l'aide des fonctions standards de messagerie SMS de votre téléphone.

Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Sélectionnez **Localisation** et appuyez sur **Suivant**.
3. Tapez le numéro de téléphone de l'appareil dont vous souhaitez supprimer les données. Cliquez sur **Suivant**.

4. Entrez le code secret défini sur l'appareil destinataire du message et appuyez sur **Envoi**.

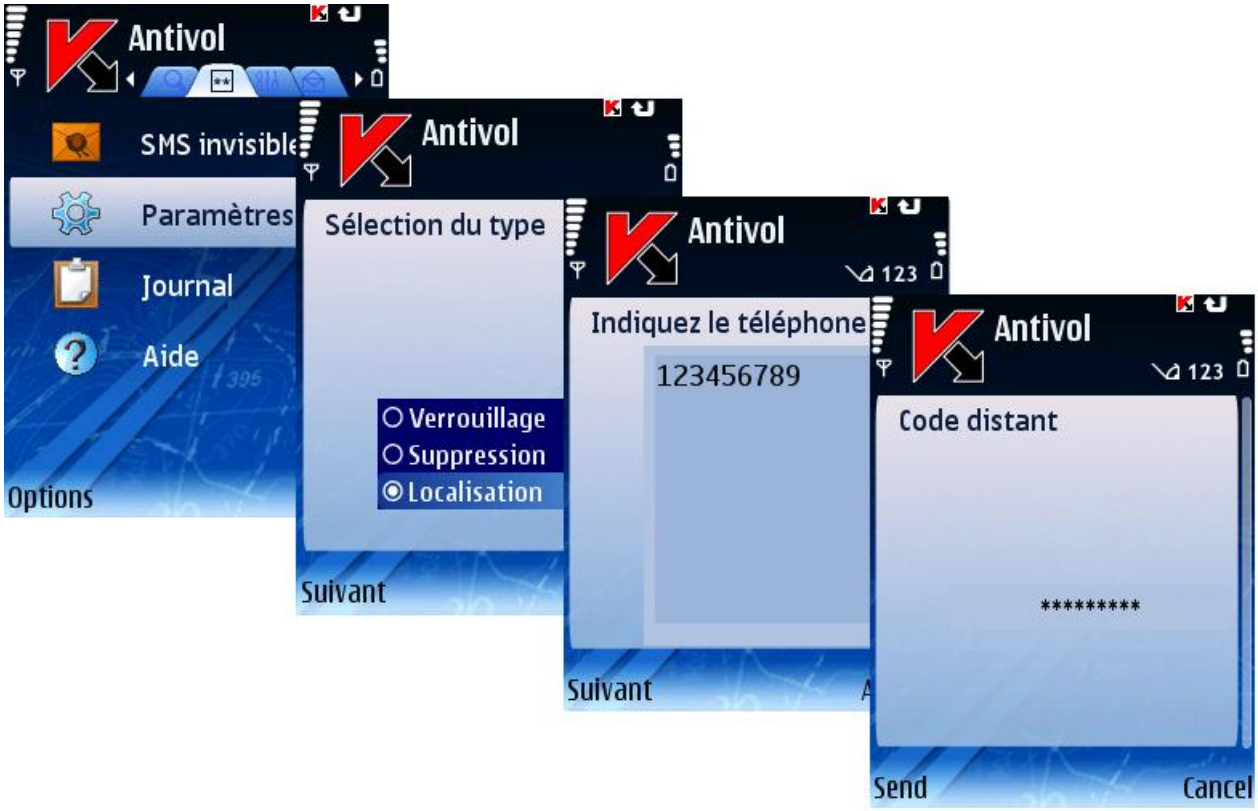

Figure 54: Détermination des coordonnées de l'appareil

➧ *Pour créer un message SMS avec les fonctions standards de votre téléphone :*

envoyez à l'appareil un message SMS contenant le texte find:<code> (où <code> est le code secret défini sur l'appareil récepteur. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Un message SMS contenant les coordonnées de l'appareil sera envoyé au numéro du téléphone ayant demandé les coordonnées, ainsi qu'à l'adresse de messagerie, si celle-ci a été spécifiée dans la configuration (voir section « Fonction Localisation » à la page 63).

Fonction SMS Invisible

La fonction **SMS invisible** permet de créer un message SMS spécial pour verrouiller l'appareil perdu, supprimer les données personnelles et déterminer ses coordonnées géographiques.

➧ *Pour créer un SMS invisible, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Sélectionnez la fonction souhaitée :
   - **Verrouillage** (voir section « Fonction Verrouillage » à la page 59).
   - **Suppression** (voir section « Fonction Suppression » à la page 60).
   - **Localisation** (voir section « Fonction Localisation » à la page 63).

Il faut que la fonction à utiliser soit activée sur l'appareil récepteur.

Cliquez sur **Suivant**.

3. Tapez le numéro de l'appareil destinataire du message. Cliquez sur **Suivant**.

4. Entrez le code secret spécifié sur l'appareil destinataire du SMS et appuyez sur **Envoi**.

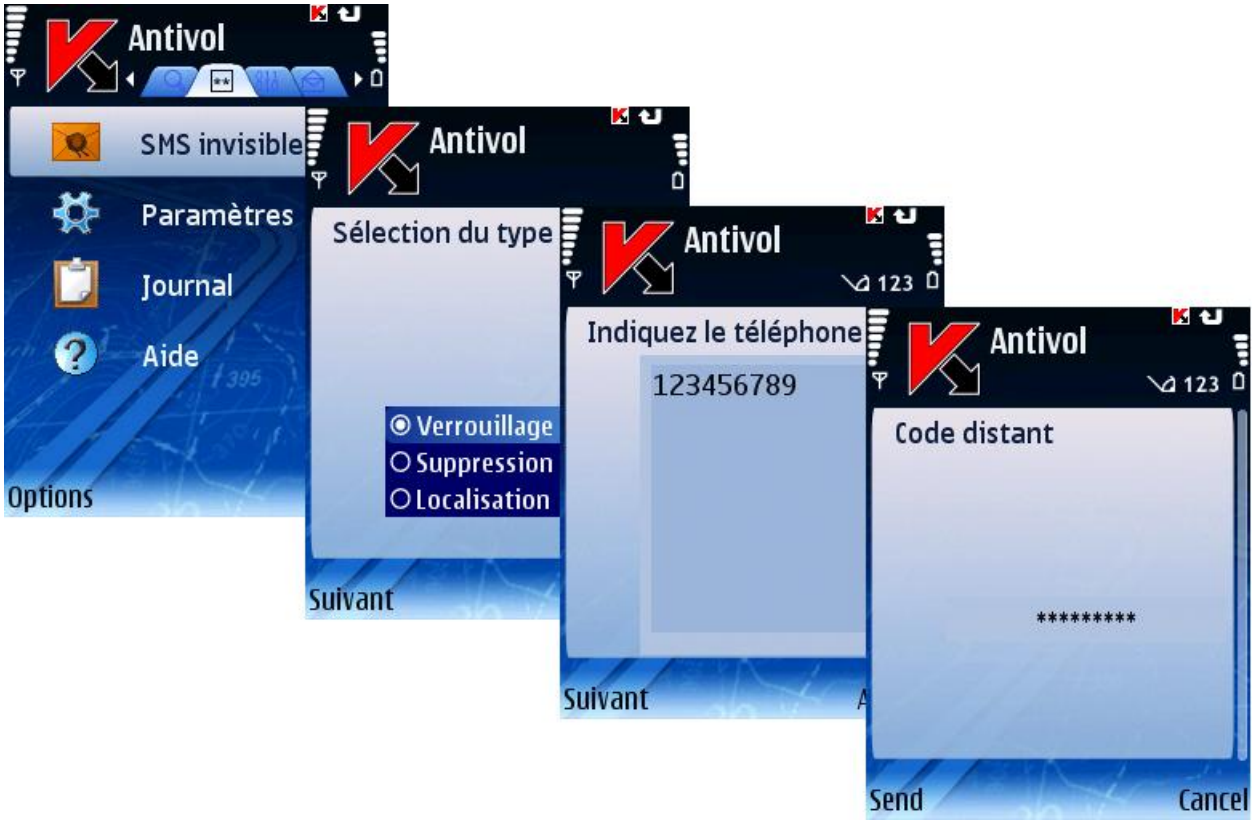

Figure 55 : Configuration de la fonction SMS invisible

Pare-feu

Cette section décrit le composant Pare-feu chargé de la surveillance de l'activité réseau de l'appareil et de sa protection sur le réseau.

Dans cette section

À propos du Pare-feu 66

Sélection du niveau de sécurité du Pare-feu 67

Notifications sur les tentatives de connexion 68

À propos du Pare-feu

Le composant Pare-feu permet à l'utilisateur de spécifier quelles connexions réseau doivent être autorisées ou interdites.

Des informations sur l'activité du Pare-feu sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Sélection du niveau de sécurité du Pare-feu

Le fonctionnement du composant Pare-feu repose sur la configuration de niveaux de sécurité. Le niveau de sécurité permet de spécifier quels protocoles réseau sont autorisés, ou au contraire interdits, pour le transfert de données.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil 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 les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour sélectionner le niveau de sécurité du Pare-feu, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Pare-feu**.
2. Sélectionnez **Pare-feu**. Dans la fenêtre ouverte, sélectionnez le niveau de sécurité requis :
   - **Haut** : toute l'activité réseau est interdite sauf la mise à jour des bases et le renouvellement de la licence.
   - **Moyen** : toutes les connexions entrantes sont interdites, les connexions sortantes ne sont autorisées qu'à travers les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
   - **Bas** : interdit uniquement les connexions entrantes.
   - **Inactif** : autorise toute l'activité réseau.
3. Sélectionnez **Précédent** pour enregistrer les modifications et revenir à la fenêtre **Paramètres**.

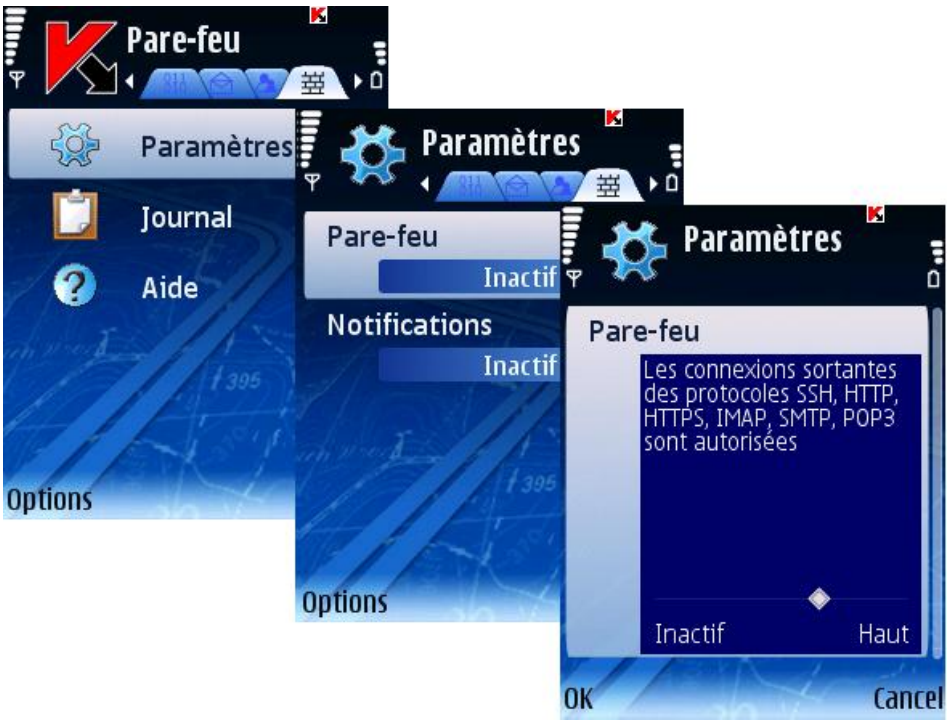

Figure 56 : Configuration du niveau de sécurité du Pare-feu

Notifications sur les tentatives de connexion

- *Il est possible de contrôler l'affichage de notifications sur les tentatives de connexion bloquées en fonction du niveau de sécurité du Pare-feu ;*

1. Sélectionnez **Paramètres** dans l'onglet **Pare-feu**.
2. Choisissez la valeur **Actif** dans le paramètre **Notifications**.

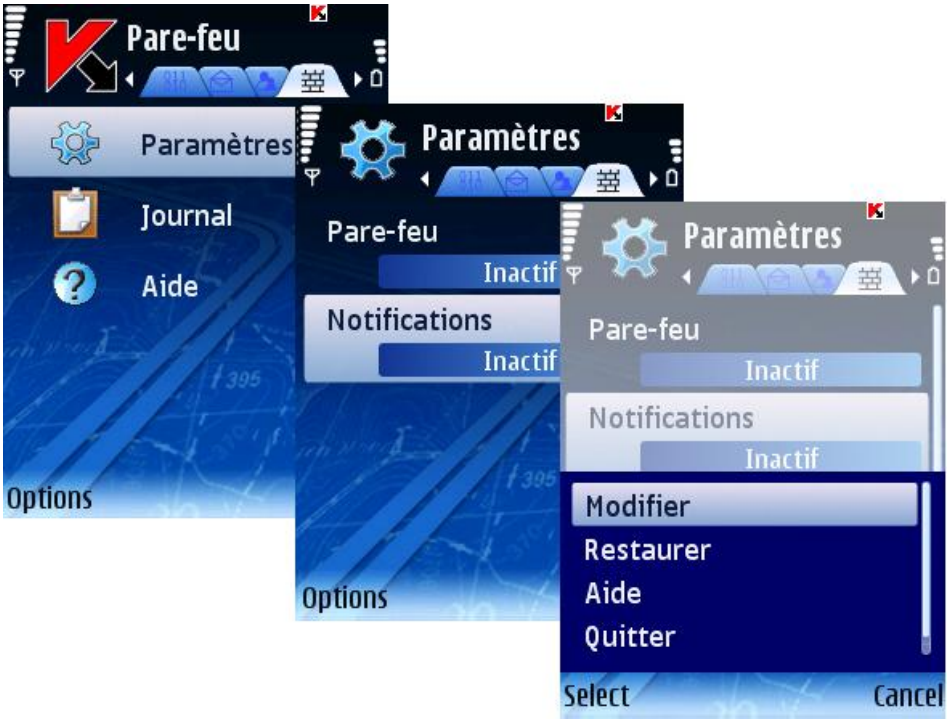

Figure 57 : Notifications sur les tentatives de connexion

Chiffrement

Cette section décrit le composant de protection chargé de chiffrer les données dans l'appareil.

Dans cette section

À propos du chiffrement 68

Chiffrement des données 69

Déchiffrement de données 70

Informations sur les données chiffrées 70

Interdiction d'accès aux données chiffrées 71

À propos du chiffrement

Le chiffrement est destiné à protéger le contenu d'un certain dossier contre l'examen de personnes non autorisées, même si celles-ci ont accès à l'appareil.

La première fois que vous accédez au chiffrement, vous devez définir un code secret (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé à la fonction de chiffrement et aux données chiffrées. Le code permet également d'accéder aux paramètres de l'Antivol et du Contrôle parental.

Le contenu du dossier est chiffré dès l'exécution de la commande **Chiffrer** après quoi les données sont chiffrées ou déchiffrées « au vol » au fur et à mesure que des données sont ajoutées, extraites ou consultées dans le dossier.

Des informations sur l'activité du composant sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 77).

Chiffrement des données

Le composant Chiffrement permet de chiffrer n'importe quel dossier (sauf les dossiers système) dans la mémoire de l'appareil ou dans une carte d'extension mémoire.

Pour protéger par chiffrement un dossier de l'appareil, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Chiffrer** dans l'onglet **Chiffrement**.

2. Dans la fenêtre ouverte, sélectionnez le dossier que vous souhaitez chiffrer.

   Pour vous déplacer dans le système de fichiers, utilisez le stylo ou les boutons du joystick de votre appareil : **Haut**, **Bas** – pour vous déplacer à l'intérieur du dossier sélectionné ; **Gauche**, **Droit** – pour monter ou descendre de niveau par rapport au dossier courant.

   Pour lancer le chiffrement du dossier sélectionné, utilisez **Chiffrer** dans le menu **Options**.

Figure 58 : Chiffrement des données

Le contenu du dossier est chiffré dès l'exécution de la commande après quoi les données sont chiffrées ou déchiffrées « au vol » au fur et à mesure que des données sont ajoutées, extraites ou consultées.

Vous ne pouvez chiffrer qu'un seul dossier au moyen de la fonction **Chiffrement**. Si vous souhaitez chiffrer un autre dossier, vous devez d'abord déchiffrer le dossier le dossier déjà protégé. Après l'opération de chiffrement, la commande **Chiffrer** change à **Déchiffrer**, ce qui vous permet de déchiffrer les données (voir section « Déchiffrement des données » à la page 70).

Déchiffrement de données

Il est possible de déchiffrer complètement les données préalablement protégées (voir section « Chiffrement de données » à la page 69).

- *Pour déchiffrer complètement le dossier préalablement chiffré,*

  Sélectionnez **Déchiffrer** dans l'onglet **Chiffrement** (voir figure suivante).

Figure 59 : Déchiffrement des données

Après l'opération, la commande **Déchiffrer** change à **Chiffrer** ce qui vous permet de chiffrer de nouveau les données (voir section « Chiffrement de données » à la page 69).

Informations sur les données chiffrées

Si la fonction de chiffrement est activée, vous pouvez vérifier quel est le dossier actuellement chiffré.

- *Pour afficher le chemin du dossier actuellement chiffré, procédez de la manière suivante (voir figure suivante) :*

  1. Ouvrez l'onglet **Chiffrement**.
  2. Sélectionnez **Informations**. Le chemin du dossier chiffré est affiché.

Figure 60 : Informations sur les données chiffrées

Interdiction d'accès aux données chiffrées

Vous pouvez interdire l'accès aux données chiffrées soit immédiatement, soit après un délai. Après quoi vous devrez saisir le code secret avant de pouvoir consulter les données chiffrées.

Pour s'assurer que les données sont protégées dès que l'appareil bascule en mode veille, il est possible de configurer le verrouillage automatique des données.

Le paramètre **Interdire l'accès** définit le délai d'inactivité après la désactivation du rétro éclairage et le passage en mode veille de l'appareil, après lequel il est nécessaire de saisir le code secret permettant de consulter les données chiffrées.

Par défaut, l'accès est interdit immédiatement après la désactivation du rétro éclairage (la valeur **Sans délai** est sélectionnée).

Pour activer le verrouillage par inactivité, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Chiffrement**.
2. Sélectionnez **Interdire l'accès** dans la fenêtre ouverte.
3. Définissez le délai souhaité : **1 minute**, **5 minutes**, **15 minutes** ou **1 heure**.

4. Appuyez sur **OK** pour enregistrer les modifications.

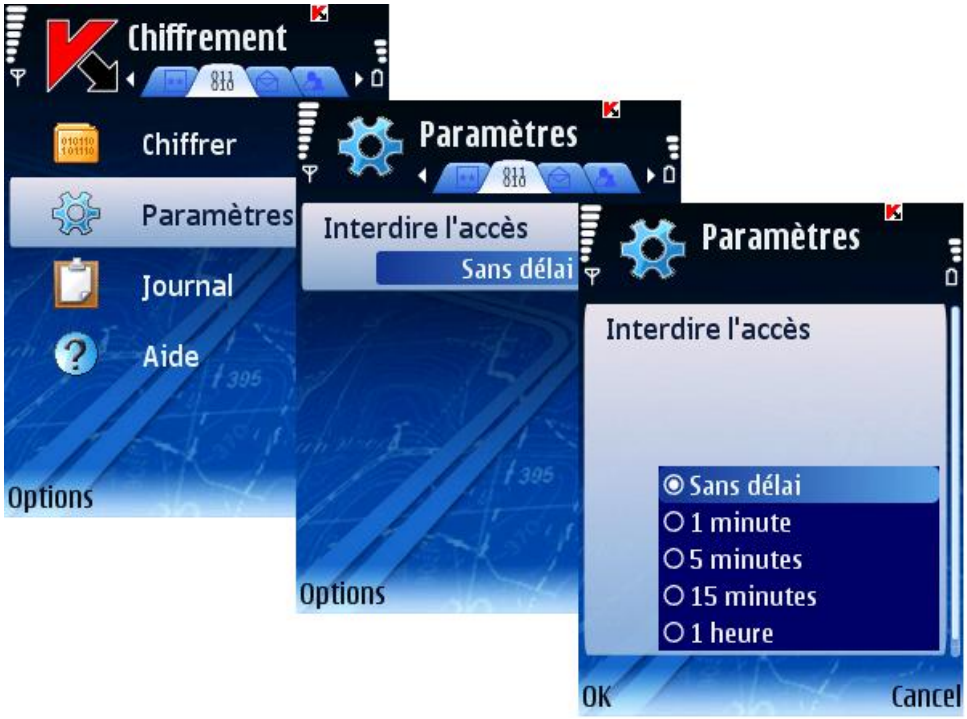

Figure 61 : Interdiction d'accès aux données chiffrées

Vous pouvez également interdire l'accès aux données chiffrées immédiatement et demander la saisie du code secret.

- *Pour un verrouillage immédiat ,*

  Appuyez sur les buttons 0 et 1 en même temps.

Mise à jour des bases du programme

Cette section décrit le composant de mise à jour. La mise à jour régulière des bases de données est nécessaire pour garantir un fonctionnement optimum de Kaspersky Mobile Security.

Dans cette section

À propos de la mise à jour des bases 73

Affichage d'informations sur les bases 73

Mise à jour manuelle 73

Mise à jour planifiée 74

Mise à jour en itinérance 75

Configuration de la connexion 76

À propos de la mise à jour des bases

La recherche de logiciels malveillants fait appel au contenu de bases de données logicielles, contenant la description et les procédés de réparation de tous les logiciels malveillants connus jusqu'à ce jour, ainsi que la description d'autres objets indésirables. 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 par Internet depuis les serveurs de Kaspersky Lab, ce qui exige une connexion Internet.

Pour afficher le détail des bases en cour d'usage, sélectionnez **Infos des bases** dans l'onglet **Informations**.

Des informations sur les mises à jour des bases de données sont consignées dans le journal du logiciel (voir section « Journaux du logiciel» à la page 77).

Affichage d'informations sur les bases

- *Pour afficher les informations sur les bases installées (voir figure suivante),*

  Sélectionnez **Infos des bases** dans l'onglet **Informations**.

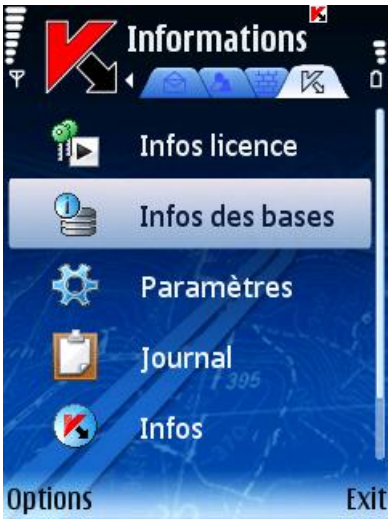

*Figure 62 : L'onglet **Informations***

Mise à jour manuelle

Vous pouvez lancer la mise à jour manuellement à n'importe quel moment approprié.

Pour lancer la mise à jour manuelle des bases antivirus,

Sélectionnez **Mise à jour** dans l'onglet **Anti-Virus** (voir figure suivante). Le programme lance la mise à jour des bases depuis le serveur à traves la connexion sélectionnée au moment de l'activation du logiciel. Si nécessaire, vous pouvez modifier le point d'accès dans la configuration des mises à jour (voir section « Paramètres de connexion » à la page 76).

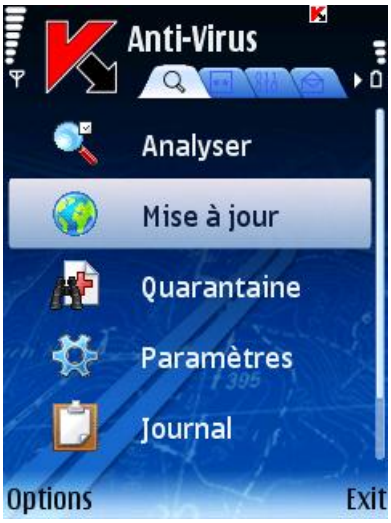

Figure 63 : Mise à jour manuelle

Mise à jour planifiée

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Selon votre critère, vous pouvez configurer la mise à jour automatique des bases à n'importe quel moment approprié.

Pour configurer la mise à jour automatique des bases du logiciel, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.

2. Dans la fenêtre ouverte sélectionnez **Planification des mises à jour** et configurez les paramètres de **Mise à jour auto**.

   - **Inactif** : ne réalise pas de mises à jour planifiées.

   - **Chaque jour** : exécute la mise à jour tous les jours. Spécifiez l'heure de mise à jour dans le champ correspondant.

   - **Chaque semaine** : exécute la mise à jour une fois par semaine. Spécifiez la date et l'heure de mise à jour dans les champs correspondants.

3. Sélectionnez **Précédent** pour enregistrer les modifications et revenir à la fenêtre **Paramètres**.

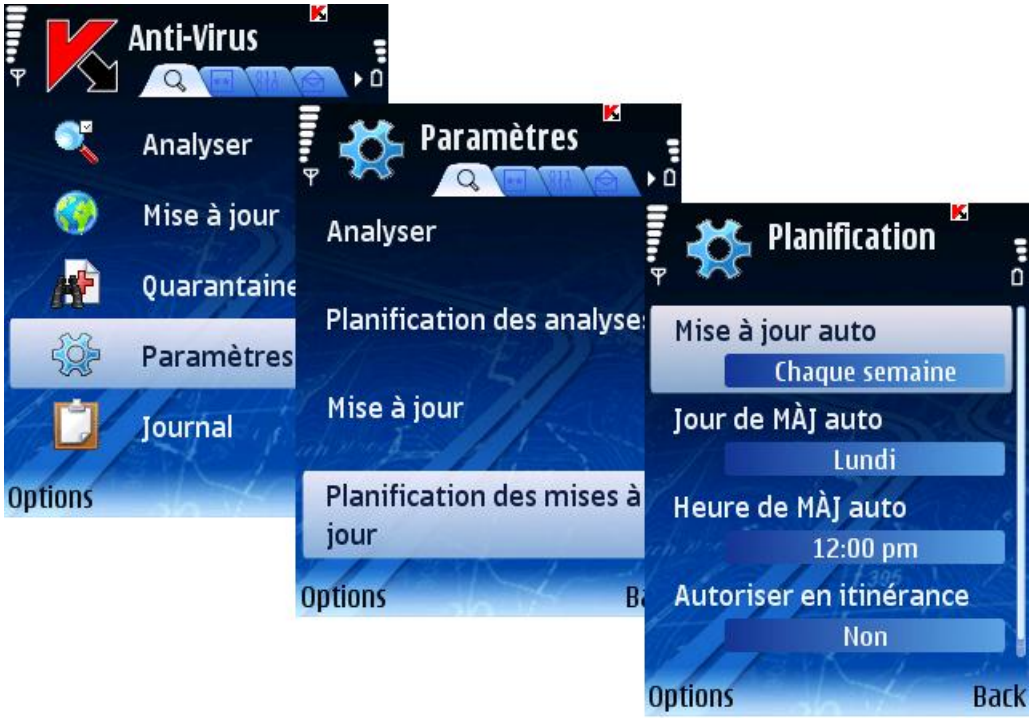

Figure 64 : Configuration de mises à jour planifiées

Vous pouvez également contrôler l'exécution de mises à jour automatiques si votre téléphone se trouve à l'étranger (voir section « Mise à jour en itinérance » à la page 75).

Mise à jour en itinérance

Vous pouvez configurer la désactivation automatique des mises à jour planifiées si votre téléphone se trouve en itinérance. La mise à jour manuelle reste disponible dans le mode normal.

➧ *Pour désactiver automatiquement les mises à jour planifiées lorsque votre téléphone se trouve en itinérance, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Planification des mises à jour** dans la fenêtre ouverte.
3. Choisissez la valeur **Non** dans le paramètre **Autoriser en itinérance**.
4. Sélectionnez **Précédent** pour enregistrer les modifications et revenir à la fenêtre **Paramètres**.

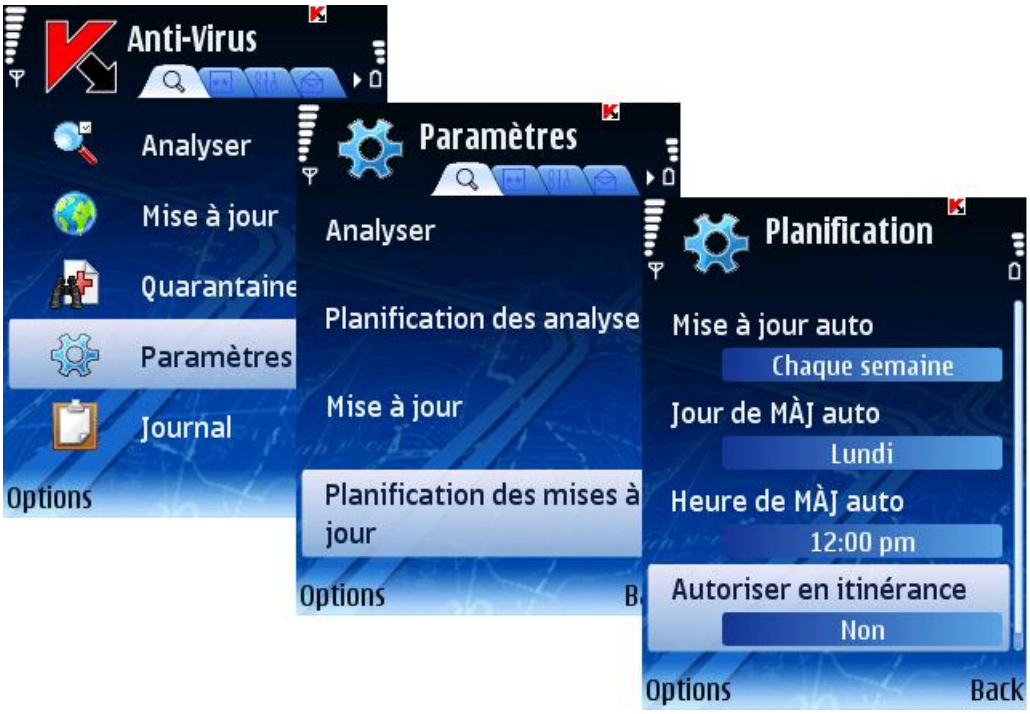

Figure 65 : Configuration des mises en jour en itinérance

Configuration de la connexion

➡ *Pour configurer les paramètres de connexion, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Mise à jour** dans la fenêtre ouverte.
3. Sélectionnez le point d'accès (paramètre **Point d'accès**) utilisé pour vous connecter au serveur de mise à jour.

   La configuration du point d'accès doit se faire conformément aux informations de votre fournisseur de services.

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

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

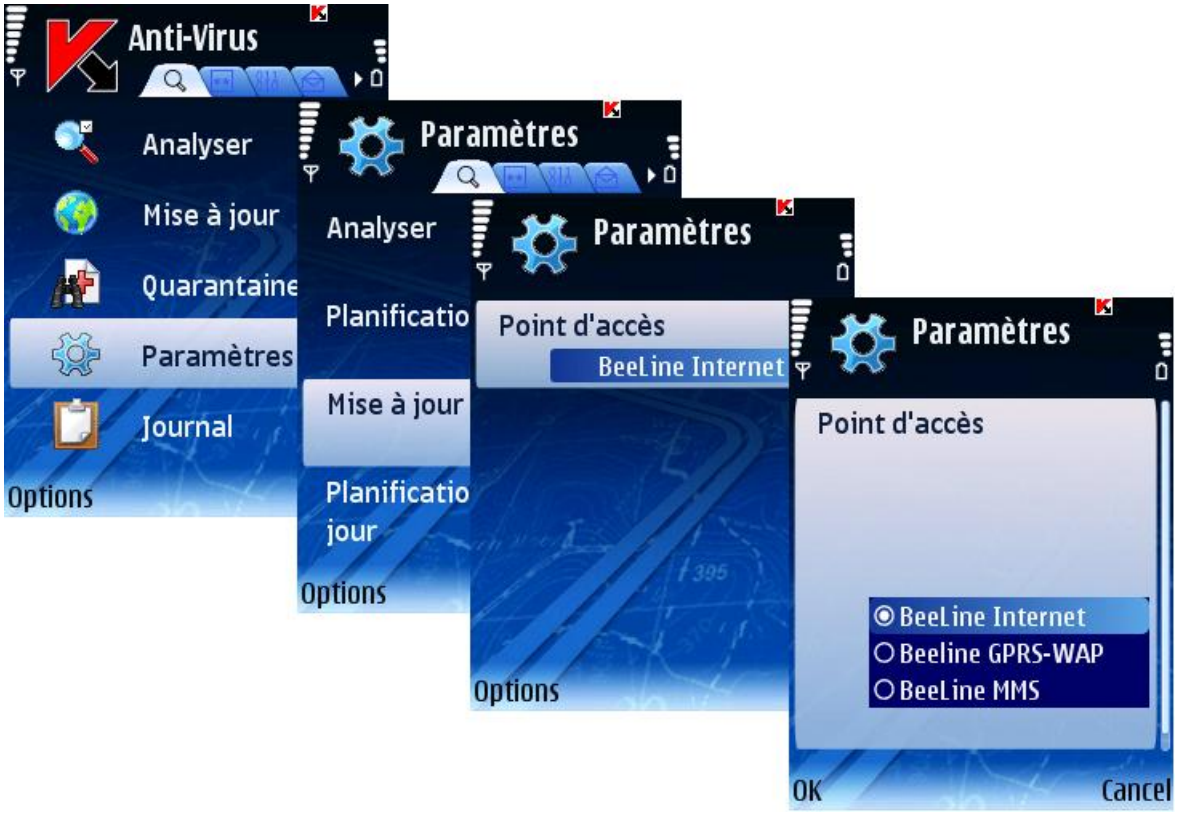

Figure 66 : Configuration de la connexion

Une fois la mise à jour terminée, la connexion établie pour cette opération est automatiquement interrompue. Si la connexion était déjà établie avant la mise, elle reste alors disponible pour d'autres opérations.

Journaux du logiciel

Cette section décrit les journaux de l'application et la gestion des informations qu'ils contiennent.

Dans cette section

À propos des journaux....77

Affichage des événements du journal....78

Suppression d'événements dans les journaux....78

À propos des journaux

Dans les journaux sont consignés les événements qui se produisent au cours des opérations de Kaspersky Mobile Security, classés par heure de consignation, à commencer par les entrées les plus récentes.

Affichage des événements du journal

- *Pour afficher tous les événements consignés dans le journal, procédez de la manière suivante :*

  1. Sélectionnez la commande dans le menu **Journal** du composant dont vous voulez afficher les informations (for exemple, commande **Journal** dans l'onglet **Anti-Virus**).

  2. Utilisez les boutons du joystick pour vous déplacer dans le journal. **Haut**, **Bas** – pour vous déplacer à travers des messages du composant sélectionné ; **Gauche**, **Droit** – pour passer aux messages des autres composants.

- *Pour afficher le détail d'un événement consigné dans le journal,*

  Sélectionnez un message et utilisez **Détails** dans le menu **Options**.

Suppression d'événements dans les journaux

- *Pour supprimer tous les messages du journal :*

  1. Sélectionnez **Journal** dans le menu de n'importe quel composant (for exemple, commande **Journal** dans l'onglet **Anti-Virus**).

  2. Sélectionnez **Effacer le journal** dans le menu **Options**. Tous les événements du journal de chaque composant seront supprimés.

Affichage de la fenêtre d'état

Vous pouvez activer ou désactiver l'affichage de la fenêtre d'état au démarrage de l'application.

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

- *Pour configurer l'affichage de la fenêtre d'état, procédez de la manière suivante (voir figure suivante) :*

  1. Sélectionnez **Paramètres** dans l'onglet **Informations**.

  2. Sélectionnez la valeur requise pour le paramètre **Afficher l'écran d'état** dans la fenêtre ouverte :

     - Pour afficher la fenêtre d'état au démarrage du programme, choisissez **Oui**.

     - Si vous ne souhaitez pas afficher la fenêtre d'état, choisissez **Non**.

  3. Appuyez sur **Précédent** pour enregistrer les modifications.

Figure 67 : Configuration de l'affichage de la fenêtre d'état

Notifications sonores

Vous pouvez configurer l'utilisation du son dans les notifications émises pour certains événements (détection d'objets infectés, message concernant l'état du programme, etc.). Par défaut, l'utilisation du son en cas de détection d'un virus dépend du profil de l'appareil (valeur **Dépendant du profil**).

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

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab. Si vous souhaitez restaurer les valeurs recommandées après leur modification, ouvrez la fenêtre **Paramètres** et sélectionnez **Restaurer** dans le menu **Options**.

Pour configurer des notifications sonores, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Informations**.
2. Sélectionnez **Son** dans la fenêtre ouverte.
3. Choisissez la valeur souhaitée :
   - Pour que la notification sonore soit activée sans tenir compte du profil sélectionné dans l'appareil, choisissez la valeur **Activé**.
   - Pour que la reproduction d'un signal sonore en cas de détection d'un virus soit dépendante du profil de l'appareil, choisissez la valeur **Dépendant du profil**.
   - Pour désactiver les notifications sonores, sélectionnez la valeur **Désactivé**.
4. Sélectionnez **OK** pour enregistrer les modifications.

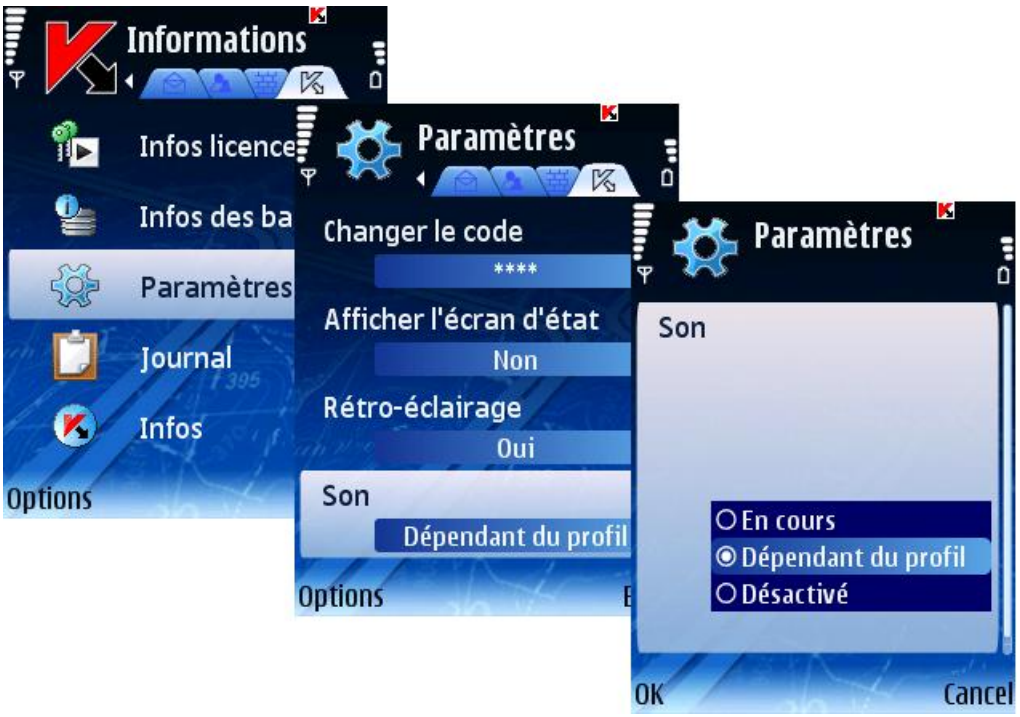

Figure 68 : Contrôle des notifications sonores

Gestion de la licence

Kaspersky Mobile Security permet d'afficher les informations de la licence actuelle et de la renouveler si nécessaire.

Dans cette section

Affichage des informations de licence 80

Renouvellement de la licence 81

Affichage des informations de licence

➧ *Pour afficher les informations sur la licence, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Infos licence** dans l'onglet **Informations**.

2. Sélectionnez **Licence** dans la fenêtre ouverte.

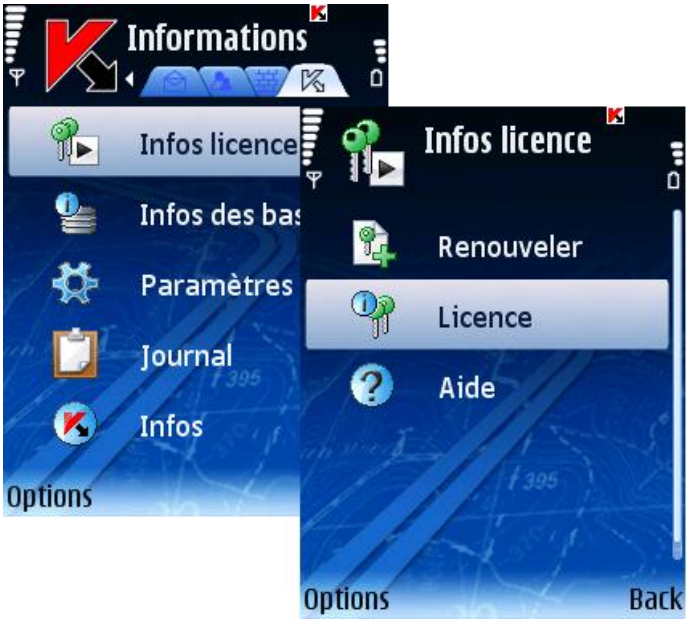

Figure 69 : Affichage des informations de licence

Renouvellement de la licence

➡ *Pour renouveler votre licence, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Infos licence** dans l'onglet **Informations**.

2. Sélectionnez **Renouveler** dans la fenêtre ouverte.

   La fenêtre de saisie du code s'affiche sur l'écran du smartphone.

3. Saisissez le code dans les 4 champs contigus. Le code d'activation est composé de lettres en alphabet latin et de chiffres, et n'est pas sensible à la casse. Après avoir saisi le code d'activation, sélectionnez **Activer** dans le menu **Options**.

4. Au moment de spécifier un point d'accès, sélectionnez le type de connexion utilisé pour la connexion au serveur.

Le programme envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe le fichier clé.

Figure 70 : Renouvellement de la licence

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

Si l'installation de la clé réussit, les informations de licence sont affichées à l'écran. Pour commencer à utiliser le programme, appuyez sur **OK**.

Désinstallation du programme

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

1. Assurez-vous qu'il n'existe pas de données chiffrées (voir section « Chiffrement de données » à la page 69).
2. Fermez Kaspersky Mobile Security. Pour ce faire :
   a. Maintenez appuyé le bouton **Menu**.
   b. Sélectionnez **KMS 8.0** dans la liste des programmes en exécution.

c. Sélectionnez **Quitter** dans le menu **Options** (voir figure suivante).

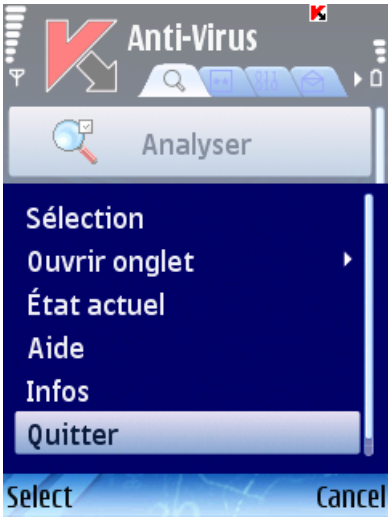

Figure 71 : Quitter le logiciel.

3. Désinstallation de Kaspersky Mobile Security

a. Ouvrez le menu principal de l'appareil.

b. Ouvrez le menu **Outils** et sélectionnez **App. mgr.** (voir figure suivante).

Figure 72 : Démarrage du Gestionnaire d'applications

c. Sélectionnez **KMS 8.0** dans la liste des programmes et appuyez sur **Options** (voir figure suivante).

Figure 73 : Sélection de l'application

d. Sélectionnez **Supprimer** dans le menu (voir figure suivante).

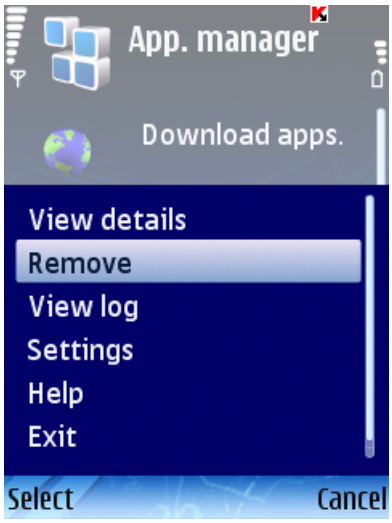

Figure 74 : Désinstallation de l'application

e. Cliquez sur **Oui** dans la fenêtre de confirmation de suppression du programme.

f. En réponse au programme, saisissez le code secret si nécessaire.

g. Pour sauvegarder la configuration du programme, les objets en quarantaine ou les listes du composant Anti-Spam, cochez les cases des paramètres correspondants (voir figure suivante).

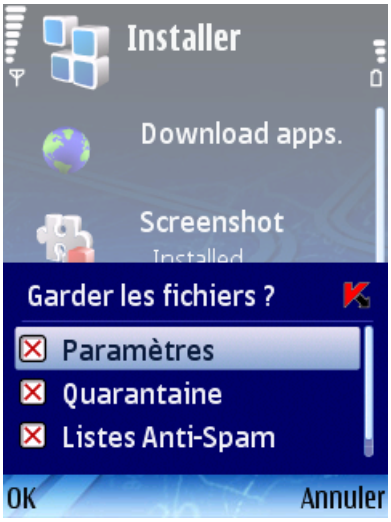

Figure 75 : La liste des paramètres à sauvegarder

h. Redémarrez le téléphone pour compléter la désinstallation du programme.

KASPERSKY MOBILE SECURITY POUR MICROSOFT WINDOWS MOBILE

Cette section décrit le fonctionnement de Kaspersky Mobile Security sur des Smartphone équipés de l'OS Microsoft Windows mobile 5.0, 6.0, 6.1.

Dans cette section

Installation de Kaspersky Mobile Security 86

Premiers pas 87

Protection en temps réel 92

Analyse à la demande 95

Quarantaine 102

Anti-Spam 105

Contrôle parental 117

Antivol 125

Pare-feu 134

Chiffrement 136

Mise à jour des bases du programme 141

Journaux du logiciel 144

Gestion de la licence 146

Désinstallation du programme 148

Installation de Kaspersky Mobile Security

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

1. Copiez le fichier CAB contenant la distribution du programme dans votre appareil mobile. Pour ce faire, appliquez l'une des méthodes suivantes :
   - depuis la page de téléchargement du site de Kaspersky Lab ;
   - avec l'application Microsoft ActiveSync ;
   - avec une carte d'extension mémoire.
2. Exécutez l'installation (ouvrez le fichier CAB de la distribution dans l'appareil mobile).

3. Lisez le contrat de licence (figure suivante). Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Kaspersky Mobile Security sera installé dans l'appareil. En cas de désaccord avec les conditions du contrat de licence, choisissez **Annuler**.

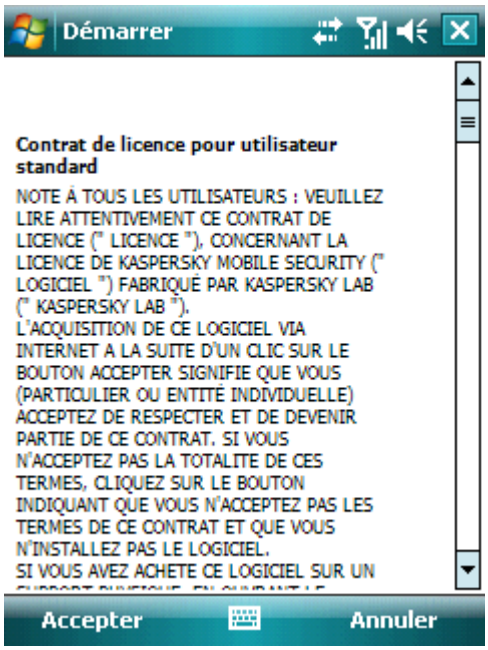

Figure 76 : Contrat de licence

4. Choisissez la langue de l'interface de Kaspersky Mobile Security (figure suivante) et cliquez sur **OK**.

Figure 77: Sélection de la langue de l'interface du programme

5. Après l'installation, un message s'affiche recommandant de redémarrer l'appareil. Pour redémarrer l'appareil, appuyez sur **Redémarrer** ou, pour le faire plus tard, appuyez sur **Annuler**.

Premiers pas

Cette section décrit le démarrage du programme, les pré requis de son activation, l'utilisation de son interface et la définition du code secret.

Dans cette section

Activation du logiciel 88

Démarrage du logiciel 89

Interface graphique utilisateur 90

Code secret 91

Informations sur le programme 92

Activation du logiciel

Avant de démarrer. il faut d'abord activer Kaspersky Mobile Security. La procédure d'activation suppose de saisir le code d'activation puis de recevoir une clé que le logiciel utilise pour déterminer vos droits et la durée d'utilisation du programme.

Le code d'activation est disponible à l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html chez un distributeur Kaspersky Lab.

Pour activer Kaspersky Mobile Security, votre smartphone doit disposer d'une connexion Internet.

Avant de lancer l'activation, assurez-vous que la date et l'heure système de l'appareil sont correctes.

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

1. Sélectionnez **Programmes** dans le menu **Démarrer**.
2. Sélectionnez **KMS8** et démarrer le programme avec le stylo ou le bouton central du joystick.
3. Sélectionnez **Saisissez le code** dans la fenêtre ouverte.

La fenêtre d'activation de Kaspersky Mobile Security s'affiche à l'écran (voir figure suivante).

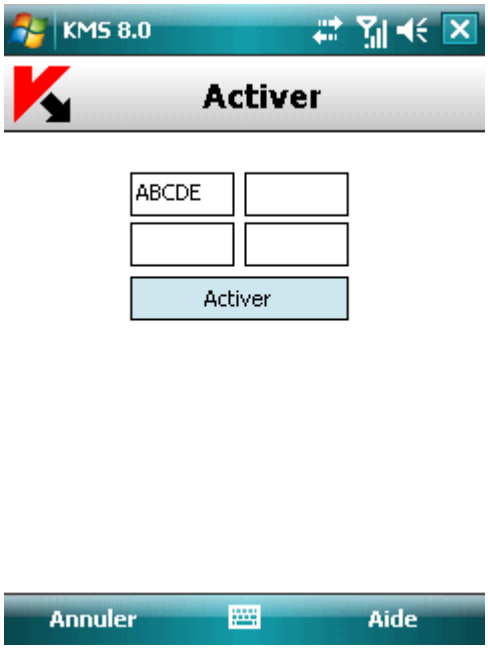

Figure 78 : Saisie du code

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

5. Le programme envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe le fichier clé.

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

Si l'installation de la clé réussit, un message d'information sur l'installation de la clé et sur la licence s'affiche à l'écran. Pour commencer à utiliser le programme, appuyez sur **OK**.

Démarrage du logiciel

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

1. Sélectionnez **Programmes** dans le menu **Démarrer**.

2. Sélectionnez **KMS8** et démarrer le programme avec le stylo ou le bouton central du joystick.

Après son démarrage, les principaux composants Kaspersky Mobile Security sont présentés dans une fenêtre (voir figure suivante) affichée à l'écran.

- **Prot. en temps réel** – État de la protection en temps réel.
- **Dernière analyse** – date et heure de la dernière analyse anti-virus de l'appareil.
- **Mise à jour des bases** – date de publication des bases installées dans l'appareil.
- **Pare-feu** – niveau de protection de l'appareil contre des activités réseau indésirables.

- **Anti-Spam** – état de la protection contre des messages entrants indésirables.

Figure 79 : La fenêtre d'état des composants du programme

Vous pouvez lancer une analyse complète de l'appareil à la recherche d'objets malveillants à l'aide du bouton **Analyser** ou ouvrir l'onglet avec **Menu**.

Interface graphique utilisateur

Les composants logiciels sont organisés par groupes, et leurs paramètres sont disponibles sur sept onglets :

- L'onglet **Anti-Virus** contient les paramètres de protection en temps réel, d'analyse à la demande, de mise à jour des bases logicielles et de la quarantaine ainsi que les paramètres de planification des tâches d'analyse et de mise à jour.
- L'onglet **Antivol** contient les paramètres nécessaires pour verrouiller l'appareil et effacer les données en cas de perte ou de vol.
- L'onglet **Chiffrement** contient les paramètres de chiffrement permettant de protéger les informations présentes dans l'appareil.
- L'onglet **Anti-Spam** contient les paramètres permettant de filtrer les appels et messages entrants indésirables.
- L'onglet **Contrôle parental** contient les paramètres utilisés pour interdire les appels et messages sortants indésirables.
- L'onglet **Pare-feu** contient tous les paramètres de protection de l'activité réseau de l'appareil.
- L'onglet **Informations** contient les paramètres généraux de fonctionnement ainsi que des informations sur le programme et sur les bases utilisées. L'onglet comprend également des informations sur la licence installée et la disponibilité de son renouvellement.

Pour vous déplacer dans les onglets, appuyez sur **Menu** et sélectionnez l'onglet souhaité (voir figure suivante).

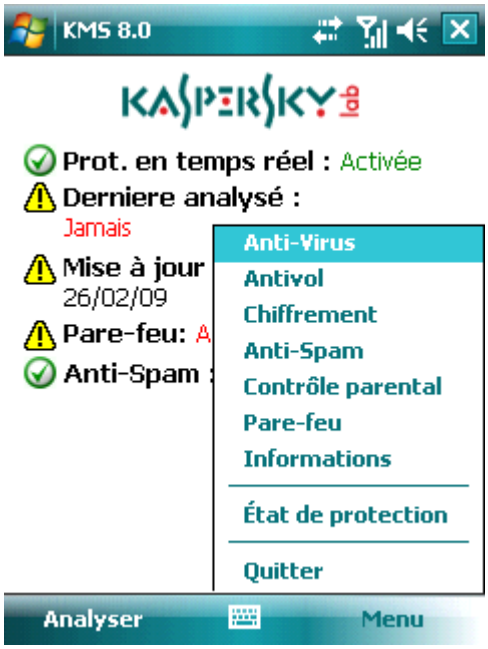

Figure 80 : Menu du programme

- *Pour revenir à la fenêtre d'état des composants logiciels,*

  sélectionnez **État de la protection**.

- *Pour quitter le programme,*

  choisissez **Quitter**.

Code secret

Le code secret est utilisé pour empêcher l'accès non autorisé aux paramètres des composants Antivol, Contrôle parental et Chiffrement ainsi que pour la création d'un SMS invisible, la désinstallation du logiciel et l'accès aux données chiffrées.

Pour définir le code secret, appliquez l'une des méthodes suivantes :

- Lors de la configuration des composants suivants :
  - Antivol (à la page 125).
  - Contrôle parental (à la page 117).
  - Chiffrement (à la page136).
- Avec la commande **Changer le code** dans l'onglet **Informations**.

Nous recommandons d'utiliser un code secret composé d'au moins 7 chiffres.

- *Pour définir le code secret dans l'onglet **Informations**, procédez comme suit :*

  1. Sélectionnez **Changer le code** dans l'onglet **Informations**.
  2. Dans la zone **Saisissez le nouveau code**, tapez les chiffres de votre code, appuyez sur **OK**. Tapez de nouveau ce code dans la zone **Confirmer**.

En outre, si le code n'est pas encore défini, vous pourrez le faire lors de votre accès aux paramètres des composants Antivol, Chiffrement ou Contrôle parental. En outre, les zones **Saisissez le nouveau code** et **Confirmation du code** seront affichées.

Pour changer le code secret, procédez comme suit :

1. Sélectionnez l'onglet **Informations**.
2. Dans l'onglet, sélectionnez **Paramètres**, puis **Changer le code.**
3. Tapez le code actuel dans la zone **Saisissez le code**. Tapez le nouveau code dans la zone **Saisissez le nouveau code** puis de nouveau dans la zone **Confirmer** pour le confirmer.

En cas d'oubli du code secret, vous ne pourrez ni utiliser les fonctions de Kaspersky Mobile Security ni désinstaller le logiciel.

Informations sur le programme

Vous pouvez afficher des informations générales sur le logiciel, ainsi que les détails de version et de copyright.

Pour afficher les informations sur le logiciel,

Sélectionnez **Infos logiciel** dans l'onglet **Informations** (voir figure suivante).

*Figure 81 : L'onglet **Informations***

Protection en temps réel

Cette section décrit la protection en temps réel de votre appareil, comment l'activer et configurer ses paramètres.

Dans cette section

À propos de la protection en temps réel 93

Activation et désactivation de la protection en temps réel 93

Sélection des actions à appliquer sur des objets 94

À propos de la protection en temps réel

La protection en temps réel se charge en même temps que le système d'exploitation et s'exécute dans la mémoire de l'appareil, pour analyser tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte toutes les tentatives d'accès aux fichiers de la part de l'utilisateur ou d'un autre programme.

2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés en les comparant aux bases de données du logiciel. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Après l'analyse, Kaspersky Mobile Security peut appliquer les actions suivantes :

   - Si du code malveillant est détecté dans un fichier, Kaspersky Mobile Security bloque le fichier et exécute l'action prévue dans la configuration.

   - Si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Des informations sur les résultats de l'analyse sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Voir aussi

Journaux du logiciel 144

Activation et désactivation de la protection en temps réel

Le programme permet de contrôler l'état de protection en temps réel de l'appareil contre les objets malveillants.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

➡ *Pour activer la protection en temps réel, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.

2. Sélectionnez **Paramètres de protection** dans la fenêtre ouverte.

3. Cochez la case **Activer la protection** associée au **Etat de la prot. en temps réel** dans l'écran qui s'affiche.

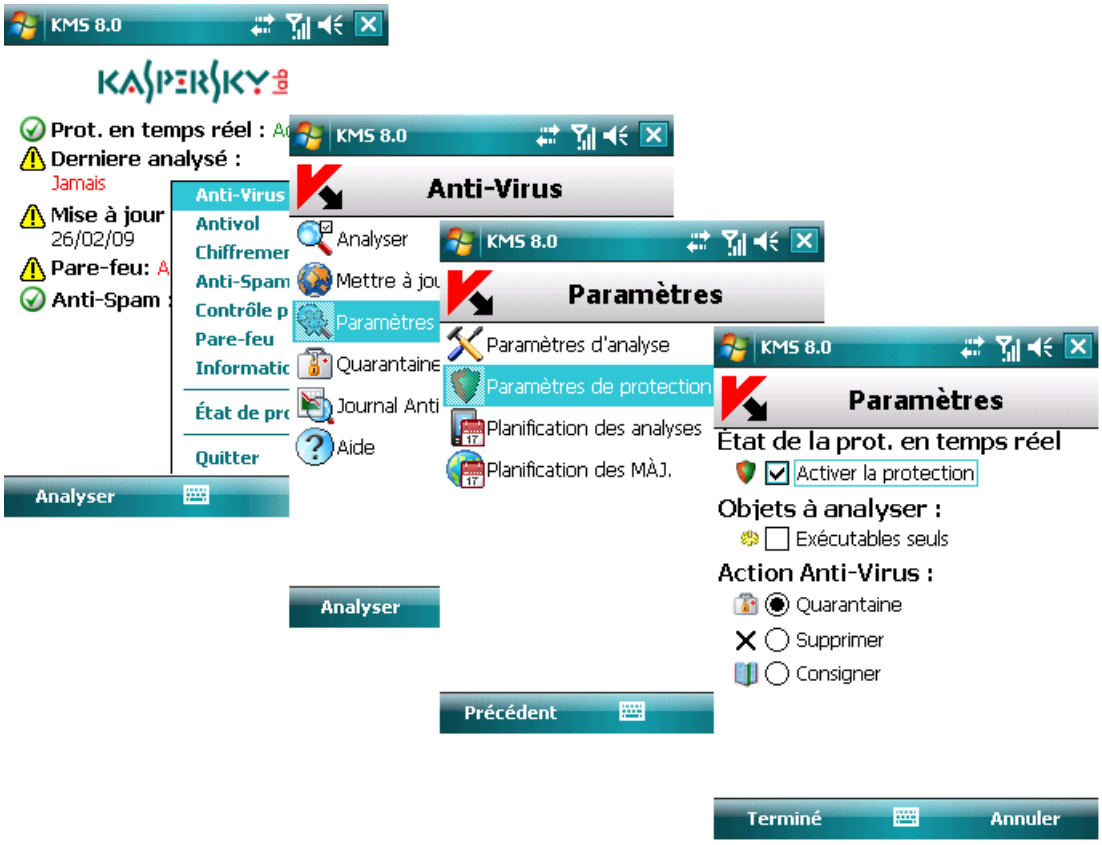

Figure 82 : Activation de la protection en temps réel

➡ *Pour désactiver la protection en temps réel, procédez de la manière suivante :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Paramètres de protection** dans la fenêtre ouverte.
3. Décochez la case **Activer la protection** associée au **Etat de la prot. en temps réel** dans l'écran qui s'affiche.

Les spécialises de Kaspersky Lab recommandent vivement de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

Sélection des actions à appliquer sur des objets

Vous pouvez configurer les actions appliquées par le programme quand il détecte un objet malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

➡ *Pour configurer la réponse du programme en présence d'un objet malveillant, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Paramètres de protection** dans la fenêtre ouverte.

3. Sélectionnez la réponse du programme quand il détecte un objet infecté dans le paramètre **Action antivirus**.

   - **Quarantaine :** place en quarantaine les objets malveillants.
   - **Supprimer :** supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Consigner** : ignore l'objet malveillant, consigne des informations sur sa détection dans le journal du programme.

4. Cliquez sur **Terminé** pour enregistrer les modifications.

Figure 83 : Sélection de l'action appliquée à un objet

Analyse à la demande

Cette section décrit le composant **Analyser**, comment exécuter dans votre appareil une analyse antivirus de l'appareil, configurer les paramètres d'analyse et planifier l'exécution automatique des analyses.

Dans cette section

À propos de l'analyse à la demande 96

Exécution manuelle d'une analyse 96

Configuration d'analyses planifiées 99

Sélection des objets à analyser 99

Sélection des actions à appliquer sur des objets 101

À propos de l'analyse à la demande

Kaspersky Mobile Security permet de faire une analyse complète ou partielle de la mémoire de l'appareil et de la mémoire système à la recherche d'objets malveillants.

Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés en les comparant aux bases de données utilisées par le logiciel. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour. Si du code malveillant est détecté dans un fichier, Kaspersky Mobile Security bloque le fichier et exécute l'action prévue dans la configuration.

L'exécution de l'analyse peut se faire manuellement ou de manière planifiée.

Des informations sur les résultats de l'analyse à la demande sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Exécution manuelle d'une analyse

Une analyse à la demande peut être lancée manuellement à tout moment approprié, par exemple, quand l'appareil n'est pas occupé par d'autres tâches.

Pour lancer une analyse antivirus, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.
2. Dans l'écran affiché, sélectionnez la couverture d'analyse :
   - **Analyse complète** – analyse toute la mémoire de l'appareil et des cartes d'extension.
   - **Analyse de mémoire** – analyse des processus exécutés dans la mémoire du système et des fichiers correspondants.
   - **Analyser dossier** – sélection et analyse d'un certain dossier dans le système de fichiers ou dans les cartes d'extension de mémoire connectées à l'appareil.

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

Figure 84 : Exécution manuelle d'une analyse

Après le démarrage de l'analyse, une fenêtre (voir figure suivante) affiche la progression de la tâche : nombre d'objets analysés, chemin de l'objet en cours d'analyse.

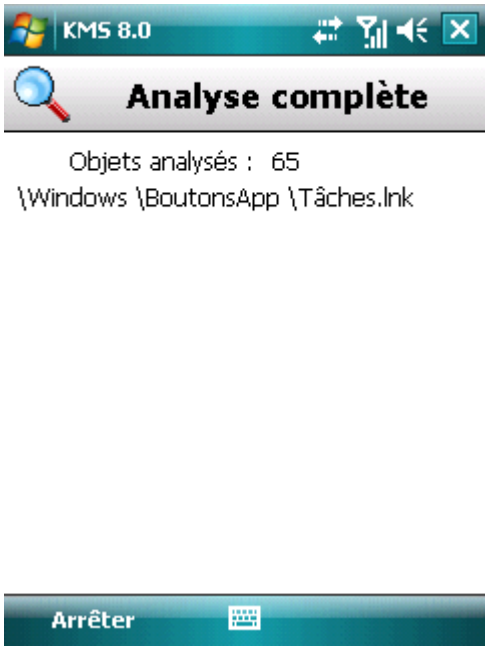

*Figure 85 : La fenêtre **Analyser***

Quand un objet infecté est détecté (voir figure suivante), une action est appliquée conformément à la configuration de l'analyse (voir section « Sélection de l'action appliquée à un objet » à la page 101).

Le logiciel ne demandera l'action à réaliser sur l'objet (voir figure suivante) que si la valeur **Demander confirmation** est sélectionnée pour le paramètre **Action**.

Figure 86 : Notification de détection de virus

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

Configuration d'analyses planifiées

Kaspersky Mobile Security permet de planifier des analyses de l'appareil qui s'exécuteront automatiquement à des heures programmées à l'avance. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, le logiciel applique l'action sélectionnée dans la configuration de l'analyse (voir section « Sélection de l'action appliquée à un objet » à la page 101).

Par défaut, la planification est désactivée.

Pour configurer l'affichage de l'icône indicateur de l'état de protection, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Planification des analyses** dans la fenêtre ouverte.
3. Dans l'écran ouvert, planifiez le lancement d'une analyse :
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Spécifiez l'**Heure** dans le champ de saisie.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Spécifiez le **Jour** et l'**Heure**.
   - **Inactif** : désactive le démarrage de l'analyse planifiée.
4. Cliquez sur **Terminé** pour enregistrer les modifications.

Figure 87 : Planification des analyses automatiques

Sélection des objets à analyser

Le programme permet de spécifier le type des objets analysés à la recherche de code malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

Pour sélectionner les objets à analyser, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Paramètres d'analyse** dans la fenêtre ouverte.
3. Configurez le paramètre **Objets à analyser** :

Si vous cochez la case...	**Pendant l'analyse, le programme exécutera les actions suivantes...**
Archives	extraction et analyse du contenu complet de l'archive ; analyse de tous les types de fichiers
Exécutables seuls	analyse uniquement les fichiers exécutables (par exemple : *.exe, *.mdl, *.app) ; pas d'extraction d'archives
Archives et **Exécutables seuls**	analyse les fichiers exécutables (par exemple : *.exe, *.mdl, *.app) ; extraction et analyse des fichiers exécutables présents dans les archives ;

Extraction des types suivants d'archives : *.zip, *.sis et *.cab.

4. Cliquez sur **Terminé** pour enregistrer les modifications.

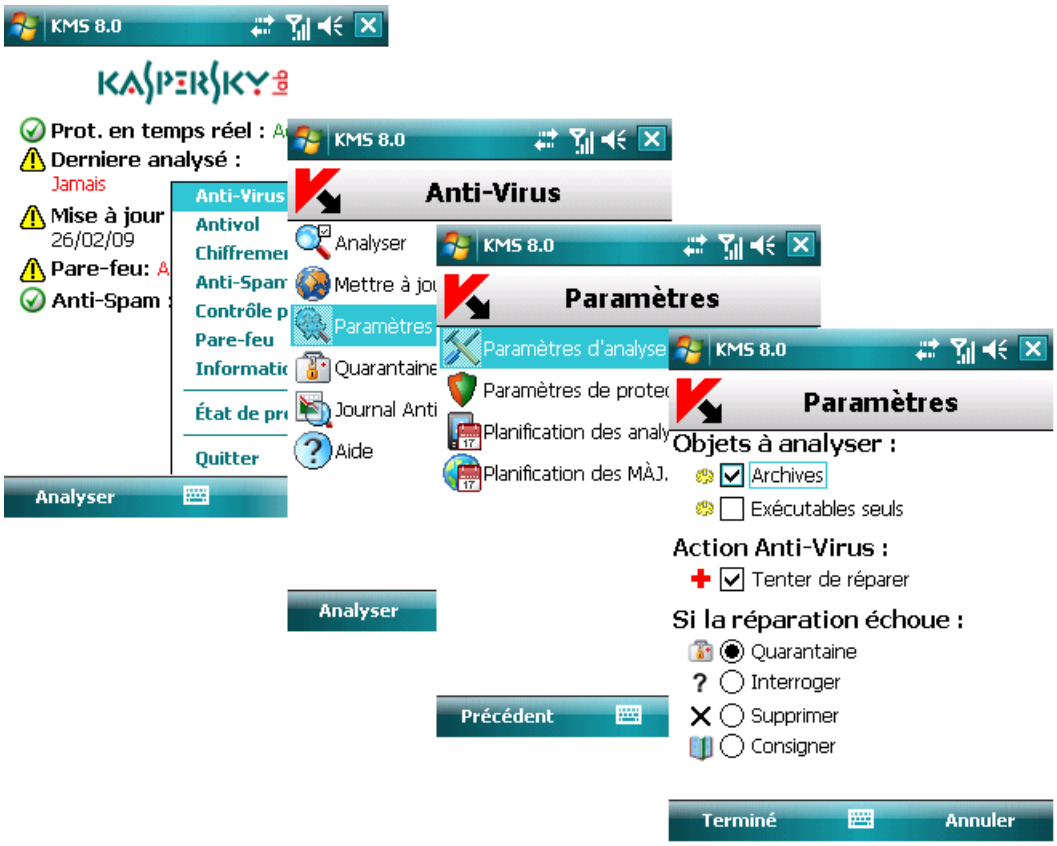

Figure 88 : Sélection d'objets à analyser

Sélection des actions à appliquer sur des objets

Vous pouvez configurer les actions appliquées par le programme quand il détecte un objet malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

Pour configurer la réponse du programme en présence d'un objet malveillant, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Paramètres d'analyse** dans la fenêtre ouverte.
3. Pour faire en sorte que le programme tente de réparer les objets infectés, cochez la case **Tenter de réparer** associée à **Action Anti-Virus**.
4. Configurez la réponse du programme aux objets malveillants dans le paramètre **Action** (si la case **Tenter de réparer** est cochée, le paramètre est libellé **Si la réparation échoue** et détermine l'action à appliquer si le programme ne peut désinfecter l'objet) :
   - **Quarantaine** : place en quarantaine des objets.
   - **Interroger** : demande à l'utilisateur de choisir une action quand un objet infecté est détecté.
   - **Supprimer :** supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Consigner** : ignore l'objet malveillant, consigne des informations sur sa détection dans le journal du programme.

5. Cliquez sur **Terminé** pour enregistrer les modifications.

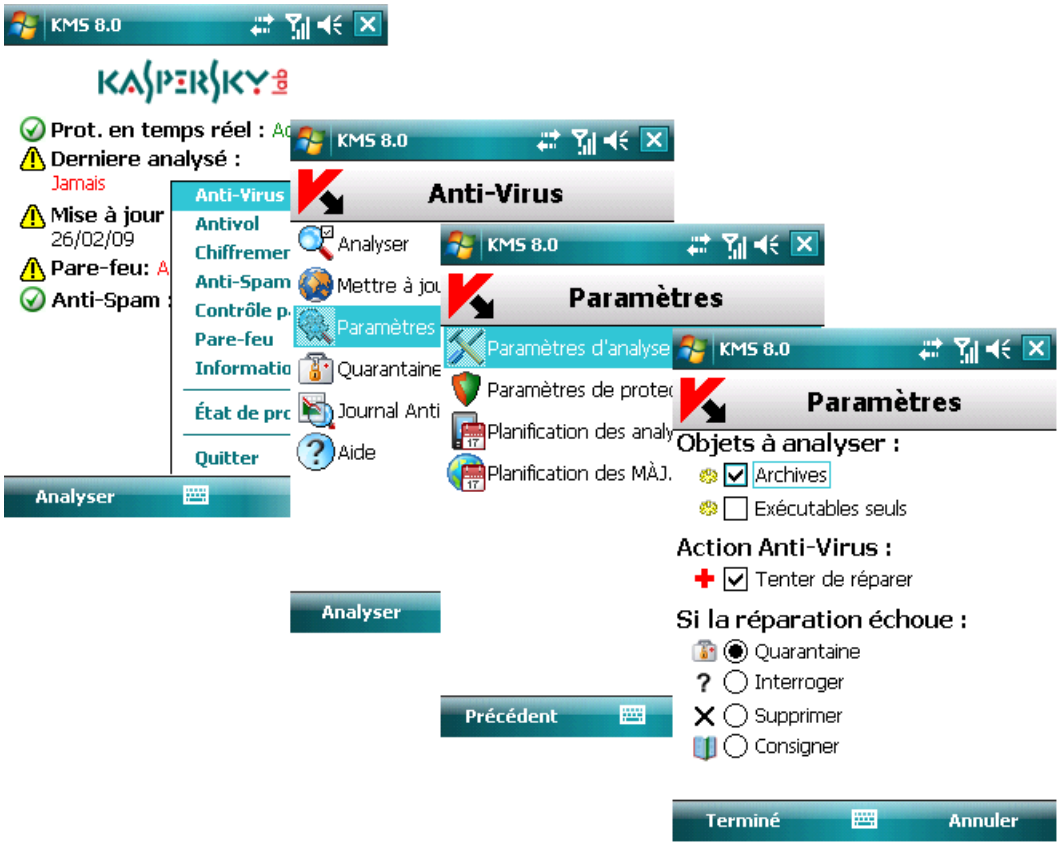

Figure 89 : Sélection de l'action appliquée à un objet

Quarantaine

Cette section décrit la quarantaine et la gestion des objets infectés placés en quarantaine.

Dans cette section

À propos de la quarantaine 102

Affichage des objets en quarantaine 103

Restauration d'objets de la quarantaine 103

Suppression d'objets de la quarantaine 104

À propos de la quarantaine

La quarantaine est une zone de stockage spécialisée dans laquelle Kaspersky Mobile Security place les objets suspectés d'être malveillants, lors d'une analyse ou par la protection en temps réel.

Les objets placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil. Les objets peuvent par la suite être supprimés ou restaurés par l'utilisateur.

Affichage des objets en quarantaine

Pour afficher la liste des objets en quarantaine,

Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**. La fenêtre **Quarantaine** ouverte contient une liste d'objets conservés dans la quarantaine (voir figure suivante).

Figure 90 : Affichage des objets en quarantaine

Voir aussi

À propos de la quarantaine 102

Restauration d'objets de la quarantaine 103

Suppression d'objets de la quarantaine 104

Restauration d'objets de la quarantaine

Pour restaurer des objets de la quarantaine, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.
2. Dans l'écran **Quarantaine** ouvert, sélectionnez l'objet que vous souhaitez restaurer.

3. Appuyez sur **Menu** et sélectionnez **Restaurer**. L'objet sélectionné dans la quarantaine est restauré dans son dossier d'origine.

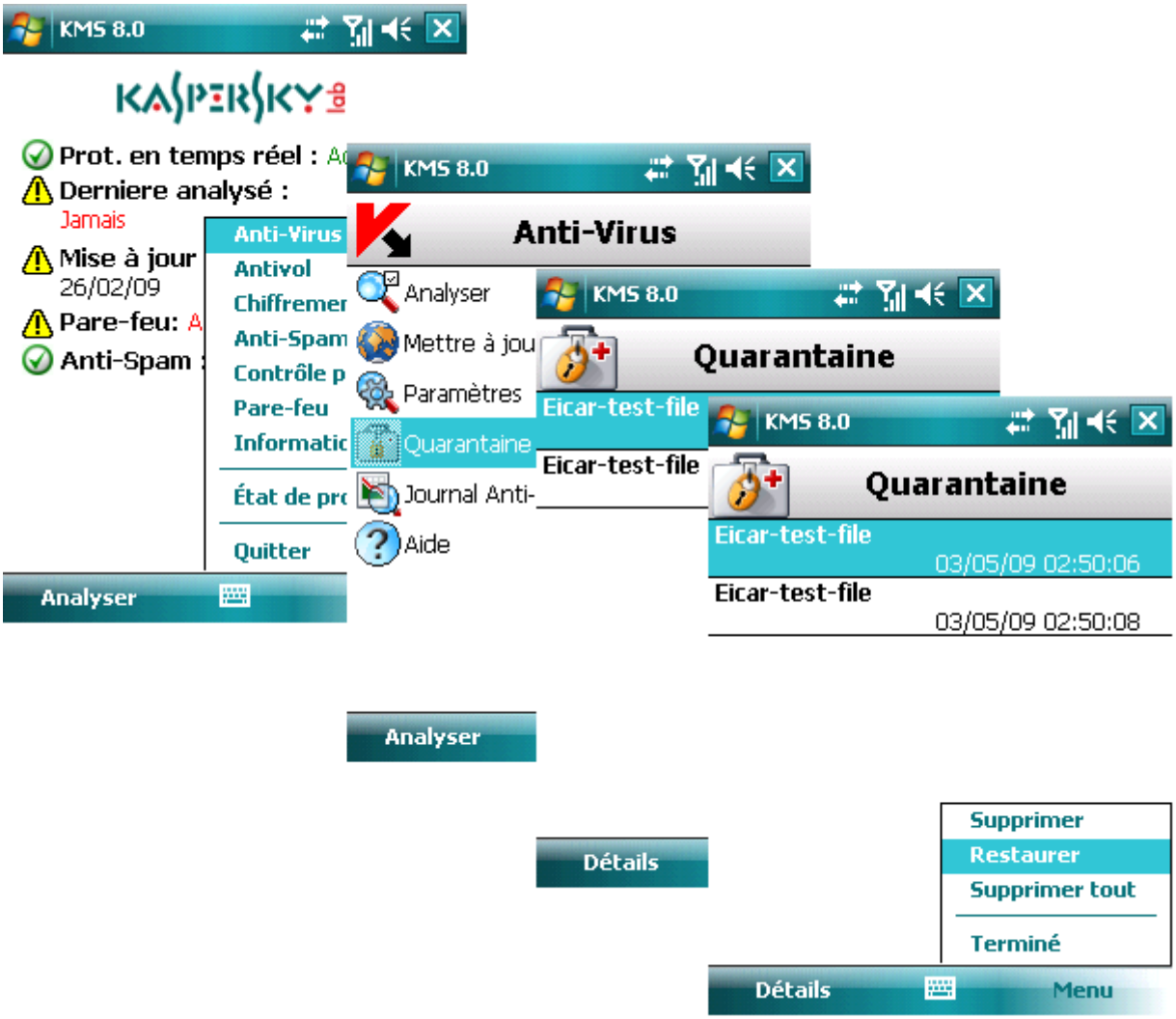

Figure 91 : Restauration d'objets depuis la quarantaine

Suppression d'objets de la quarantaine

➡ *Pour supprimer des objets dans la quarantaine, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

2. Dans l'écran **Quarantaine** ouvert, sélectionnez l'objet que vous souhaitez restaurer.

3. Appuyez sur **Menu** et sélectionnez **Supprimer**. L'objet sélectionné est supprimé de la quarantaine.

Figure 92 : Suppression d'un objet de la quarantaine

➡ *Pour supprimer tous les objets de la quarantaine, procédez de la manière suivante :*

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

2. Appuyez sur **Menu** et sélectionnez **Supprimer tout** dans l'écran **Quarantaine**. Tous les objets en quarantaine seront éliminés.

Anti-Spam

Cette section décrit le composant Anti-Spam et la méthode à suivre pour composer les listes noire et blanche, configurer les modes de fonctionnement et d'autres paramètres du composant Anti-Spam.

Dans cette section

À propos du composant Anti-Spam 106

Modes du composant Anti-Spam 106

Création d'une liste noire 107

Création d'une liste blanche 110

Réponse aux messages et appels présents dans l'annuaire téléphonique 113

Réponse aux messages d'expéditeurs non numériques 114

Sélection de l'action à appliquer sur des messages entrants 116

Sélection de l'action à appliquer sur des appels entrants 117

À propos du composant Anti-Spam

Le composant Anti-Spam permet de protéger l'appareil contre la réception de messages et d'appels indésirables. Cette protection s'appuie sur le filtrage des messages SMS et des appels entrants au moyen d'une liste noire et d'une liste blanche. Ces listes contiennent des numéros de téléphone ou des échantillons de phrases typiques de messages SMS indésirables ou normaux, respectivement.

Si une correspondance au moins est détectée avec un numéro de téléphone ou une phrase de la liste blanche, aucune vérification supplémentaire n'est réalisée et l'appel ou le message est transmis à l'appareil. Un message SMS ou un appel provenant d'un numéro de téléphone présent dans la liste noire ou un message SMS contenant du texte présent dans la liste noire sont interdits.

Modes du composant Anti-Spam

Un mode de fonctionnement Anti-Spam est un ensemble de paramètres qui déterminent la protection de votre appareil contre les messages indésirables et les appels non sollicités.

Les modes de fonctionnement Anti-Spam disponibles :

- **Autoriser tout** – aucun filtrage de messages SMS ou d'appels n'est réalisé.
- **Liste blanche** – autorisation des messages SMS et des appels présents dans la liste blanche. Tous les autres messages SMS et appels sont interdits.
- **Liste noire** – interdiction des messages SMS et des appels présents dans la liste noire. Tous les autres messages SMS et appels sont autorisés.
- **Les deux listes** – filtrage des messages SMS et des appels entrants au moyen des listes noire et blanche. Quand un message SMS ou un appel provient d'un numéro qui ne figure dans aucune de ces listes, le module Anti-Spam affiche un message proposant de l'interdire ou de l'autoriser et d'ajouter ce numéro de téléphone à la liste blanche ou noire. Ce mode est sélectionné par défaut.

Pour sélectionner un mode de fonctionnement du composant Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Spam**.

2. Dans la fenêtre ouverte, sélectionnez le mode souhaité et appuyez sur **Terminé** pour enregistrer les modifications.

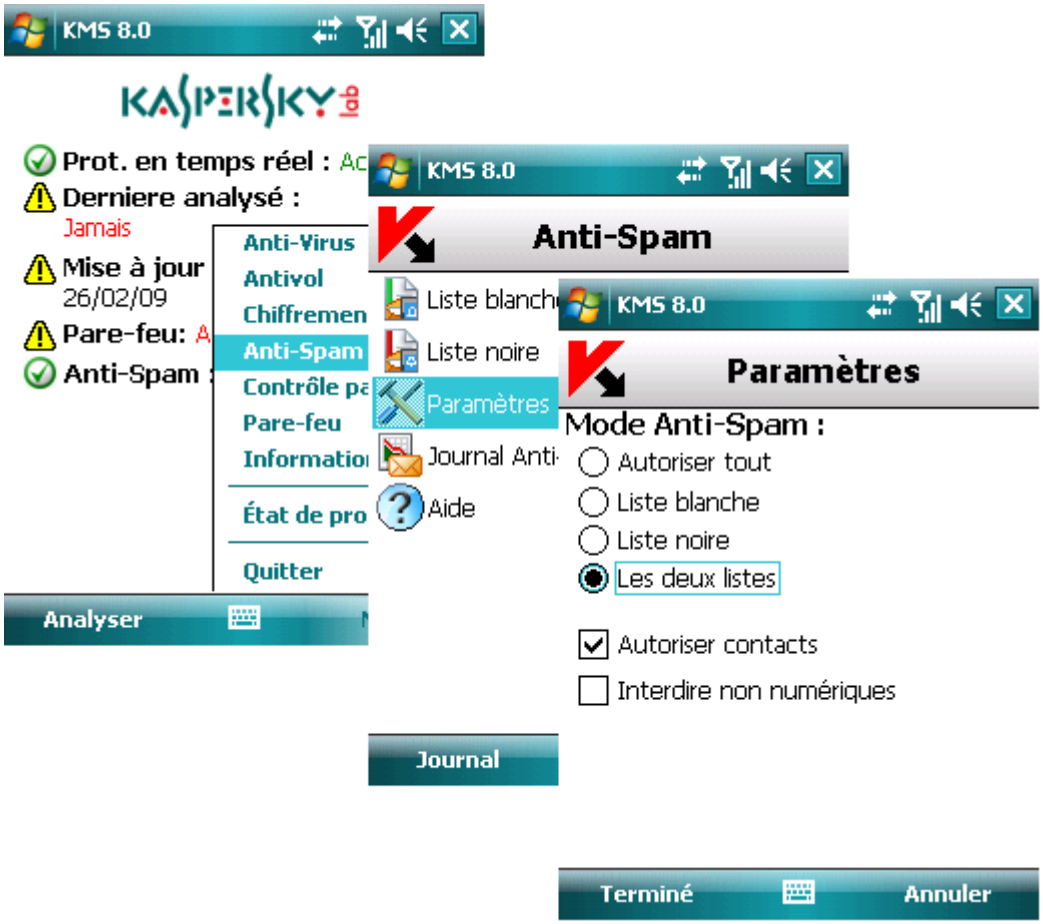

Figure 93 : Sélection du mode de fonctionnement

Création d'une liste noire

Les enregistrements de cette liste contiennent les numéros de téléphone des SMS et des appels entrants interdits par le composant Anti-Spam, ainsi que les échantillons de texte qui, s'ils figurent dans un message SMS reçu, entraînent l'interdiction de celui-ci.

Des informations sur les messages SMS et les appels interdits sont enregistrés dans le journal (voir section « Journaux du logiciel» à la page 144).

Dans cette section

Ajout d'une nouvelle entrée 107

Modification d'une entrée existante 108

Suppression d'une entrée 109

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste noire Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

2. Appuyez sur **Menu** et sélectionnez **Ajouter entrée**.

3. Définissez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est interdite. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Fonction** – action à appliquer sur un message ou un appel :

     - **Bloquer tout** : interdit les appels et les messages SMS entrants.

     - **Bloquer les appels** : interdit les appels entrants uniquement.

     - **Bloquer les messages** : interdit les messages SMS entrants uniquement.

   - **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, permet d'en interdire la réception. Ce paramètre est disponible quand la valeur **Bloquer les messages** est sélectionnée pour le paramètre **Action**.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 94 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

➡ *Pour modifier une entrée dans la liste noire Anti-Spam, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

2. Sélectionnez l'entrée à modifier dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Modifier entrée**.

4. Modifiez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est interdite. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Action** – action à appliquer sur un message ou un appel :

     - **Bloquer tout** : interdit les appels et les messages SMS entrants uniquement.

     - **Bloquer les appels** : interdit les appels entrants uniquement.

     - **Bloquer les messages** : interdit les messages SMS entrants uniquement.

   - **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, permet d'en interdire la réception. Ce paramètre est disponible quand la valeur **Bloquer les messages** est sélectionnée pour le paramètre **Action**.

5. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 95 : Modification d'une entrée existante

Suppression d'une entrée

➡ *Pour supprimer une entrée dans la liste noire Anti-Spam, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

2. Sélectionnez une entrée à supprimer dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Supprimer entrée**.

Figure 96 : Suppression d'une entrée

Création d'une liste blanche

Les enregistrements de la Liste blanche contiennent les numéros de téléphone des SMS et des appels entrants autorisés par le composant Anti-Spam, ainsi que les échantillons de texte qui, s'il leur présence est détectée dans le message SMS reçu, permet de l'autoriser.

Dans cette section

Ajout d'une nouvelle entrée 110

Modification d'une entrée existante 111

Suppression d'une entrée 112

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste blanche Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

2. Appuyez sur **Menu** et sélectionnez **Ajouter entrée**.

3. Définissez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Action** – action à appliquer sur un message ou un appel :

     - **Autoriser tout** : autorise les appels et les messages SMS entrants uniquement.

     - **Autoriser les appels** : autorise les appels entrants uniquement.

     - **Autoriser les messages** : interdit les messages SMS entrants uniquement.

   - **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, en autorise la réception. Ce paramètre est disponible quand la valeur **Autoriser les messages** est sélectionnée pour le paramètre **Action**.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 97 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier une entrée dans la liste blanche Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

2. Sélectionnez l'entrée à modifier dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Modifier entrée**.

4. Modifiez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone depuis lequel la réception de messages SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et ne peut contenir que des caractères alphanumériques. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Action** – action à appliquer sur un message ou un appel :

     - **Autoriser tout** : autorise les appels et les messages SMS entrants uniquement.

     - **Autoriser les appels** : autorise les appels entrants uniquement.

     - **Autoriser les messages** – interdit les messages SMS entrants uniquement.

   - **Texte** – texte qui, lorsqu'il est détecté dans le message SMS, en autorise la réception. Ce paramètre est disponible quand la valeur **Autoriser les messages** est sélectionnée pour le paramètre **Action**.

5. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 98 : Modification d'une entrée existante

Suppression d'une entrée

Pour supprimer une entrée de la liste blanche Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

2. Sélectionnez une entrée à supprimer dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Supprimer entrée**.

Figure 99 : Suppression d'une entrée

Réponse aux messages et appels présents dans l'annuaire téléphonique

Vous pouvez configurer la réponse du composant Anti-Spam aux messages SMS ou appels provenant de numéros présents dans l'annuaire téléphonique, sans prendre en compte les listes noire et blanche.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

➡ *Pour configurer la réponse Anti-Spam, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Spam**.
2. Dans la fenêtre ouverte, configurez le paramètre **Autoriser contacts** :
   - Si vous souhaitez que le composant Anti-Spam autorise la réception de messages SMS ou d'appels provenant de numéros présents dans l'annuaire téléphonique, cochez la case **Autoriser contacts**.
   - Si vous souhaitez que le composant Anti-Spam assure le filtrage d'un numéro de téléphone en fonction de sa présence dans l'une des listes blanche ou noire, décochez la case **Autoriser contacts**.

3. Appuyez sur **Terminé** pour enregistrer les modifications.

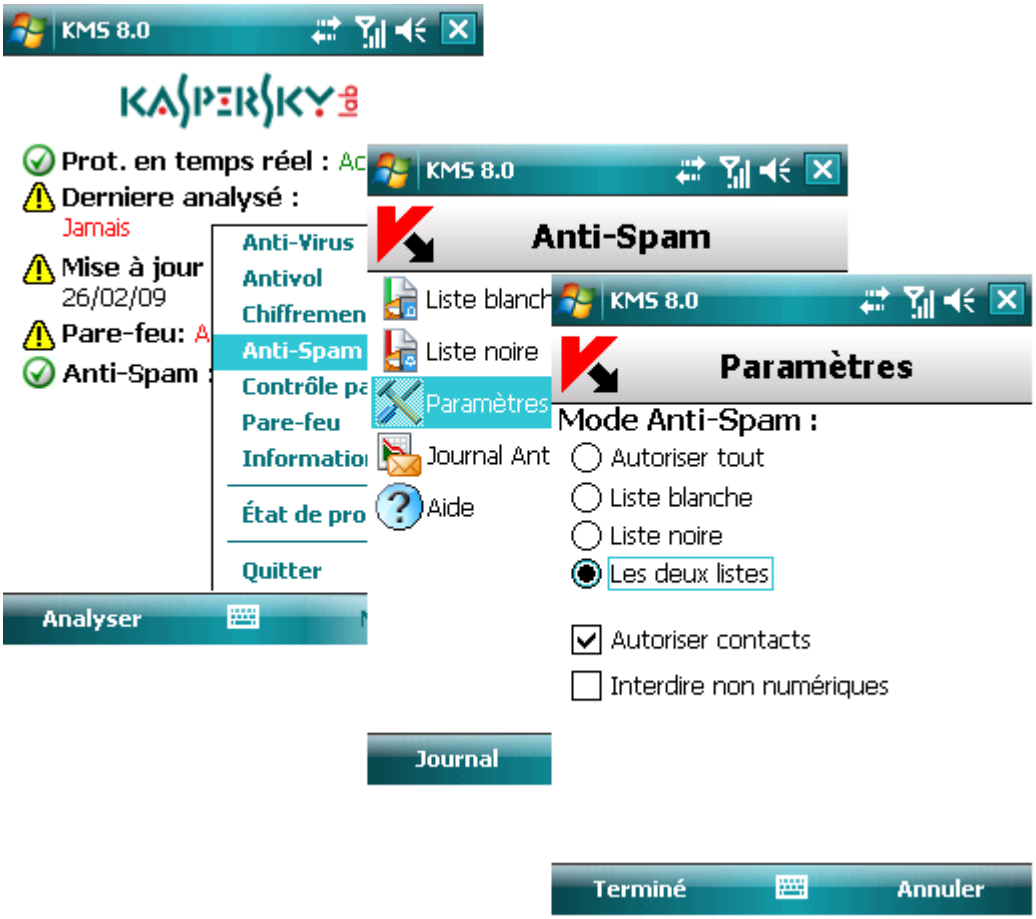

Figure 100 : Autorisation des contacts présents dans l'annuaire téléphonique

Réponse aux messages d'expéditeurs non numériques

Il est possible de configurer la réponse du programme lorsque des messages SMS proviennent d'expéditeurs non numériques (ne comprenant que des lettres).

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

Pour configurer la réponse Anti-Spam, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Spam**.
2. Configurez le paramètre **Interdire non numériques** dans la fenêtre ouverte :
   - Pour activer la suppression automatique des messages d'expéditeurs non numériques, cochez la case **Interdire non numériques**.
   - Si vous souhaitez que le composant Anti-Spam réagisse au numéro de téléphone en fonction de sa présence dans l'une des listes blanche ou noire, décochez la case **Interdire non numériques**.

3. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 101 : Interdiction des expéditeurs non numériques

Sélection de l'action à appliquer sur des messages entrants

Le composant Anti-Spam suggère de configurer la réponse aux messages SMS dont le numéro de téléphone ne figure dans aucune des listes noire ou blanche. Ce type de message sera intercepté par le composant Anti-Spam si le mode **Les deux listes** (voir section « Anti-Spam modes » à la page 106) est sélectionné, et une notification est affichée sur l'écran de l'appareil (voir figure suivante).

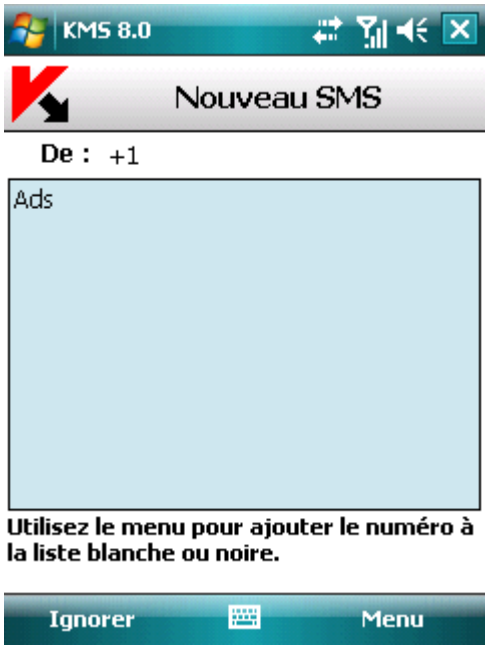

Figure 102 : Sélection de l'action à appliquer sur un message entrant

Dans le **Menu**, choisissez l'une des actions suivantes à appliquer sur le message :

- **Ajouter à la liste blanche** : autorise la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste blanche.
- **Ajouter à la liste noire** : interdit la réception du message et ajoute le numéro de téléphone de l'expéditeur à la liste noire.
- **Ignorer** : autorise la réception du message. Dans ce cas, le numéro de téléphone de l'expéditeur ne sera ajouté à aucune des listes.

Des informations sur les messages interdits sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Sélection de l'action à appliquer sur des appels entrants

Le composant Anti-Spam suggère de configurer la réponse aux messages SMS dont le numéro de téléphone ne figure dans aucune des listes noire ou blanche. À la fin de l'appel, une notification est affichée sur l'écran de l'appareil (voir figure suivante).

Figure 103 : Sélection de l'action à appliquer sur un appel entrant

Utilisez le **Menu** pour choisir l'une des actions suivantes à appliquer au numéro de téléphone de l'appelant :

- **Ajouter à la liste blanche** : ajoute le numéro de téléphone de l'appelant à la liste blanche.
- **Ajouter à la liste noire** : ajoute le numéro de téléphone de l'appelant à la liste noire.
- **Ignorer** : le numéro de l'appelant n'est pas ajouté à l'une ou l'autre des listes.

Des informations sur les appels interdits sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Contrôle parental

Cette section décrit le composant Contrôle parental et la méthode à suivre pour composer les listes noire et blanche, configurer les modes de fonctionnement et d'autres paramètres du composant Contrôle parental.

Dans cette section

À propos du contrôle parental 118

Modes du contrôle parental 118

Création d'une liste noire 119

Création d'une liste blanche 122

À propos du contrôle parental

Le fonctionnement du composant Contrôle parental s'appuie sur le filtrage des messages SMS et des appels sortants au moyen d'une liste noire et d'une liste blanche.

Si une correspondance est détectée, l'analyse est interrompue. Les messages SMS et appels qui correspondent à n'importe quelle entrée de la liste noire sont interdits, tandis que ceux qui correspondent à une entrée de la Liste blanche sont autorisés.

Le Contrôle parental bloque les messages SMS envoyés uniquement à l'aide des outils standards de l'appareil.

La première fois que vous accédez au contrôle parental, vous devez définir un code secret (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé aux Paramètres du Contrôle parental. Le code permet également d'accéder à la configuration du chiffrement et de l'Antivol.

Des informations sur l'activité du composant sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Modes du contrôle parental

Un mode de fonctionnement du contrôle parental est un ensemble de paramètres qui déterminent la protection de votre appareil contre les messages indésirables et les appels non sollicités.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Tout est autorisé** : Le contrôle parental est désactivé. Aucun filtrage de messages SMS ou d'appels n'est réalisé.
- **Liste blanche uniquement** : autorisation des messages SMS et des appels dont seuls les numéros sont présents dans la liste blanche. Tous les autres appels et messages sont interdits.
- **Liste noire uniquement** : interdiction des messages SMS et des appels dont seuls les numéros sont présents dans la liste noire. Tous les autres appels et messages sont autorisés.

Pour sélectionner le mode de fonctionnement du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Contrôle parental**.

2. Dans la fenêtre ouverte, sélectionnez le mode souhaité et appuyez sur **Terminé** pour enregistrer les modifications.

Figure 104 : Sélection du mode de fonctionnement du contrôle parental

Création d'une liste noire

Les entrées de la liste noire contiennent les numéros de téléphone des SMS ou des appels qui seront interdits par le contrôle parental.

Des informations sur les messages SMS et les appels interdits sont enregistrés dans le journal (voir section « Journaux du logiciel » à la page 144).

Dans cette section

Ajout d'une nouvelle entrée 119

Modification d'une entrée existante 120

Suppression d'une entrée 121

Ajout d'une nouvelle entrée

➡ *Pour ajouter une entrée dans la liste noire du Contrôle parental, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.

2. Appuyez sur **Menu** et sélectionnez **Ajouter entrée**.

3. Définissez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et doit contenir des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Action** – action à appliquer sur un message ou un appel :

     - **Bloquer tout** : interdiction des appels et messages SMS sortants.

     - **Bloquer les appels** : interdiction des appels sortants uniquement.

     - **Bloquer les messages** : interdit les messages SMS sortants uniquement.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 105 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier une entrée dans la liste noire du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.

2. Sélectionnez l'entrée à modifier dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Modifier entrée**.

4. Modifiez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et doit contenir des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

   - **Action** – action à appliquer sur un message ou un appel :

     - **Bloquer tout** : interdit les appels et messages SMS sortants.

     - **Bloquer les appels** : interdit les appels sortants uniquement

     - **Bloquer les messages** : interdit les messages SMS sortants uniquement.

5. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 106 : Modification d'une entrée existante

Suppression d'une entrée

Pour supprimer une entrée dans la liste noire du Contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle parental**.

2. Sélectionnez une entrée à supprimer dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Supprimer entrée**.

Figure 107 : Suppression d'une entrée

Création d'une liste blanche

Les enregistrements de la Liste blanche contiennent les numéros de téléphone des SMS et des appels autorisés par le contrôle parental.

Dans cette section

Ajout d'une nouvelle entrée 122

Modification d'une entrée existante 123

Suppression d'une entrée 124

Ajout d'une nouvelle entrée

Pour ajouter une entrée dans la liste blanche du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.
2. Appuyez sur **Menu** et sélectionnez **Ajouter entrée**.
3. Définissez les paramètres suivants dans la fenêtre ouverte :

- **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels est autorisé. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et doit contenir des chiffres. En outre, pour indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

- **Action** – action à appliquer sur un message ou un appel :

  - **Autoriser tout** : interdit les appels et messages SMS sortants.

  - **Autoriser les appels** : interdit les appels sortants uniquement.

  - **Autoriser les messages** : interdit les messages SMS sortants uniquement.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 108 : Ajout d'une nouvelle entrée

Modification d'une entrée existante

Pour modifier une entrée dans la liste blanche du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.

2. Sélectionnez l'entrée à modifier dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Modifier entrée**.

4. Modifiez les paramètres suivants dans la fenêtre ouverte :

   - **Numéro de téléphone** – vers lequel l'envoi de messages SMS ou d'appels est autorisé. Le numéro peut commencer par un chiffre, par une lettre ou par le signe « + » et doit contenir des chiffres. En outre, pour

indiquer un numéro, vous pouvez utiliser les caractères génériques « ? » et « * ». (où « * » représente une suite de caractères quelconques et « ? » un seul caractère).

- **Action** – action à appliquer sur un message ou un appel :
  - **Autoriser tout** : interdit les appels et messages SMS sortants.
  - **Autoriser les appels** : interdit les appels sortants uniquement.
  - **Autoriser les messages** : interdit les messages SMS sortants uniquement.

5. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 109 : Modification d'une entrée

Suppression d'une entrée

Pour supprimer une entrée dans la liste blanche du contrôle parental, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle parental**.
2. Sélectionnez une entrée à supprimer dans la liste.

3. Appuyez sur **Menu** et sélectionnez **Supprimer entrée**.

Figure 110 : Suppression d'une entrée

Antivol

Cette section décrit le fonctionnement du composant Antivol, conçu pour protéger les informations en cas de vol de l'appareil.

Dans cette section

À propos du composant Antivol 126

Fonction Verrouillage 126

Verrouillage de l'appareil 127

Fonction Suppression 128

Suppression de données personnelles 129

Fonction SIM-Surveillance 130

Fonction Localisation 131

Détermination des coordonnées de l'appareil 132

Fonction SMS Invisible 133

À propos du composant Antivol

Le composant Antivol est conçu pour protéger les données de l'appareil contre tout accès non autorisé en cas de perte ou de vol.

Ce composant dispose des fonctions suivantes :

- **Verrouillage** – verrouillage l'appareil à la demande de l'utilisateur.
- **Suppression** – suppression ces informations personnelles (tous les contacts, messages, galerie, calendrier, journal, paramètres de connexion réseau), les données des cartes d'extension et les fichiers du dossier Mes documents.
- **SIM-Surveillance** – permet, en cas de remplacement ou de mise en marche de l'appareil sans la carte SIM, de récupérer le nouveau téléphone au numéro ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil volé.
- **Localisation** – permet de récupérer les coordonnées géographiques de l'appareil volé par message SMS sur un autre appareil ou dans une adresse de messagerie spécifiée. Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré.
- **SMS invisible** – permet de créer un message SMS spécial pour verrouiller l'appareil, supprimer les données personnelles et déterminer ses coordonnées géographiques.

La première fois que vous accédez au composant Antivol, vous devez définir un code secret (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé aux paramètres Antivol. Ce code permet également d'accéder à la configuration du chiffrement et du contrôle parental ainsi qu'à la création d'un SMS invisible.

Des informations sur l'activité du composant sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Fonction Verrouillage

La fonction **Verrouillage** permet de verrouiller l'appareil si nécessaire. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Pour activer la fonction Verrouillage, procédez de la manière suivante (voir figure suivante) :

1. Ouvrez l'onglet **Antivol**
2. Sélectionnez **Verrouillage** dans la fenêtre ouverte.
3. Choisissez **Activée** avec le stylo ou le bouton central du joystick.

Figure 111 : Activation de la fonction

Verrouillage de l'appareil

Pour verrouiller un appareil perdu, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- l'envoi d'un SMS invisible depuis un autre appareil équipé de Kaspersky Mobile Security ;
- avec les fonctions standards de messagerie SMS de votre téléphone.

Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Configurez les paramètres du message :
   - Tapez le numéro de téléphone de l'appareil à verrouiller dans la zone **Numéro de téléphone**.
   - Dans le paramètre **Fonction**, sélectionnez **Verrouillage** (il faut que la fonction à utiliser soit activée sur l'appareil récepteur du message).
   - Entrez le code secret spécifié sur l'appareil destinataire du SMS dans la zone **Code distant**.

3. Appuyez sur **Terminé** pour envoyer le message.

Figure 112 : Verrouillage de l'appareil

Pour créer un message SMS avec les fonctions standards de votre téléphone :

envoyez à l'appareil un message SMS contenant le texte block:<code> (où <code> est le code secret défini sur l'appareil à verrouiller). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Fonction Suppression

La fonction **Suppression** permet de supprimer les informations personnelles (tous les contacts, messages, galerie, calendrier, journal, paramètres de connexion réseau), les données des cartes d'extension et les fichiers du dossier Mes documents dès que l'appareil reçoit un message SMS spécial.

Pour configurer la fonction Suppression, procédez de la manière suivante (voir figure suivante) :

1. Ouvrez l'onglet **Antivol**
2. Sélectionnez **Suppression** dans la fenêtre ouverte.
3. Dans l'écran suivant (voir figure suivante) sélectionnez les données qui seront supprimés dès la réception du message SMS spécial par l'appareil.
   - Pour supprimer uniquement vos données personnelles, cochez la case **Données personnelles**.

Les contacts seront éliminés sur l'annuaire téléphonique et sur la carte SIM de l'appareil.

- Si vous souhaitez supprimer vos fichiers personnels (données du dossier Mes documents), cochez la case **Mes documents**.

- Pour supprimer les données de toutes les cartes mémoire installées, cochez la case **Fichiers des cartes mémoire**.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 113 : Activation de la fonction

Suppression de données personnelles

Pour supprimer les données personnelles de l'appareil, si la fonction Suppression est activée, vous disposez des méthodes suivantes :

- l'envoi d'un SMS invisible depuis un autre appareil équipé de Kaspersky Mobile Security ;

- avec les fonctions standards de messagerie SMS de votre téléphone.

➡ *Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).*

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.

2. Configurez les paramètres du message :

   - Tapez le numéro de téléphone de l'appareil dont vous souhaitez supprimer les données dans la zone **Numéro de téléphone**.

- Dans le paramètre **Fonction**, sélectionnez **Suppression** (il faut que la fonction à utiliser soit activée sur l'appareil récepteur du message).
- Entrez le code secret spécifié sur l'appareil destinataire du SMS dans la zone **Code distant**.

3. Appuyez sur **Terminé** pour envoyer le message.

Figure 114 : Suppression de données personnelles

➡ *Pour créer un message SMS avec les fonctions standards de votre téléphone :*

envoyez à l'appareil un message SMS contenant le texte clean:<code> (où <code> est le code secret défini sur l'appareil récepteur. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Fonction SIM-Surveillance

SIM-Surveillance permet, en cas de remplacement de la carte SIM, de récupérer le nouveau téléphone au numéro ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil volé.

Par défaut la fonction SIM-Surveillance est désactivée.

➡ *Pour configurer la fonction SIM-Surveillance, procédez de la manière suivante (voir figure suivante) :*

1. Ouvrez l'onglet **Antivol**
2. Sélectionnez **SIM-Surveillance** dans la fenêtre ouverte.

3. Dans le menu qui s'affiche, configurez les paramètres de surveillance en cas de remplacement de la carte SIM de l'appareil.

   - Dans la zone **Numéro de téléphone**, tapez le numéro de téléphone destinataire du message contenant le nouveau numéro de téléphone en cas de remplacement de la carte SIM de votre appareil. Ces numéros peuvent commencer par un chiffre ou par le signe « + » et ne peuvent contenir que des chiffres.

   - Dans la zone **Indiquez le courriel**, précisez l'adresse de messagerie destinataire du message contenant le nouveau numéro de téléphone.

   - Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, cochez la case **Bloquer**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret. Par défaut, le verrouillage de l'appareil est désactivé.

4. Appuyez sur **Terminé** pour enregistrer les modifications apportées.

Figure 115 : Activation de la fonction

Fonction Localisation

La fonction Localisation permet de récupérer les coordonnées géographiques de l'appareil volé par message SMS sur un autre appareil ou dans une adresse de messagerie spécifiée.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. Si nécessaire, le récepteur sera activé automatiquement.

Vous ne pouvez recevoir les coordonnées que si l'appareil se trouve dans une zone couverte par satellite. Si aucun satellite n'est disponible au moment de la requête, des tentatives de localisation régulières sont répétées jusqu'au redémarrage de l'appareil.

Pour configurer le fonctionnement de la fonction SIM-Surveillance, procédez de la manière suivante (voir figure suivante) :

1. Ouvrez l'onglet **Antivol** et choisissez **Localisation** (il faut que la fonction à utiliser soit activée sur l'appareil récepteur du message).

2. Dans l'écran affiché, précisez l'adresse de messagerie (paramètre **Indiquez le courriel**) destinataire des coordonnées de l'appareil, en plus du message SMS, et appuyez sur **Terminé**.

3. Sélectionnez **Terminé** dans la fenêtre ouverte.

Figure 116 : Activation de la fonction

Détermination des coordonnées de l'appareil

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, vous disposez des méthodes suivantes :

- l'envoi d'un SMS invisible depuis un autre appareil équipé de Kaspersky Mobile Security ;
- avec les fonctions standards de messagerie SMS de votre téléphone.

Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.

2. Configurez les paramètres du message :

- Tapez le numéro de téléphone de l'appareil dont vous souhaitez récupérer les coordonnées dans la zone **Numéro de téléphone**.
- Choisissez la valeur **Localisation** dans le paramètre **Fonction**.
- Entrez le code secret spécifié sur l'appareil destinataire du SMS dans la zone **Code distant**.

3. Appuyez sur **Terminé** pour envoyer le message.

Figure 117 : Détermination des coordonnées de l'appareil

➡ *Pour créer un message SMS avec les fonctions standards de votre téléphone :*

envoyez à l'appareil un message SMS contenant le texte find:<code> (où <code> est le code secret défini sur l'appareil récepteur. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Fonction SMS invisible

La fonction SMS invisible permet de créer un message SMS spécial pour verrouiller l'appareil perdu, supprimer les données personnelles et déterminer ses coordonnées géographiques.

➡ *Pour créer un message SMS avec la fonction SMS invisible, procédez de la manière suivante (voir figure suivante).*

1. Sélectionnez **SMS invisible** dans l'onglet **Antivol**.
2. Configurez les paramètres du message :

- Tapez le numéro de téléphone de l'appareil auquel vous souhaitez envoyer un message dans la zone **Numéro de téléphone**.
- Choisissez la valeur du paramètre **Fonction**:
  - **Verrouillage** (voir section « Fonction Verrouillage » à la page 126).
  - **Suppression** (voir section « Fonction Verrouillage » à la page 128).
  - **Localisation** (voir section « Fonction Verrouillage » à la page 130).

  Il faut que la fonction à utiliser soit activée sur l'appareil récepteur du message.
- Entrez le code secret spécifié sur l'appareil destinataire du SMS dans la zone **Code distant**.

3. Appuyez sur **Terminé** pour envoyer le message.

Figure 118 : Verrouillage de l'appareil

Pare-feu

Cette section décrit le composant Pare-feu chargé de la surveillance de l'activité réseau de l'appareil et de sa protection sur le réseau.

Dans cette section

À propos du Pare-feu 135

Sélection du niveau de sécurité du Pare-feu 135

À propos du Pare-feu

Le composant Pare-feu permet à l'utilisateur de spécifier quelles connexions réseau doivent être autorisées ou interdites.

Des informations sur le fonctionnement du Pare-feu sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Sélection du niveau de sécurité du Pare-feu

Le fonctionnement du composant Pare-feu repose sur la configuration de niveaux de sécurité. Le niveau de sécurité permet de spécifier quels protocoles réseau sont autorisés, ou au contraire interdits, pour le transfert de données.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Par défaut, le programme utilise la configuration recommandée par les spécialistes de Kaspersky Lab.

Pour sélectionner le niveau de sécurité du Pare-feu, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Pare-feu**.
2. Dans la fenêtre ouverte, sélectionnez le niveau de sécurité requis :
   - **Bloquer tout** – toute l'activité réseau est interdite sauf la mise à jour des bases et le renouvellement de la licence.
   - **Sécurité maximum** – toutes les connexions entrantes sont interdites, les connexions sortantes ne sont autorisées qu'à travers les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
   - **Protection minimum** – interdit uniquement les connexions entrantes.
   - **Autoriser tout** – autorise toute l'activité réseau.

3. Appuyez sur **Terminé** pour enregistrer les modifications.

Figure 119 : Sélection du niveau de protection

Chiffrement

Cette section décrit le composant de protection chargé de chiffrer les données dans l'appareil.

Dans cette section

À propos du chiffrement 136

Chiffrement des données 137

Déchiffrement des données 138

Interdiction d'accès aux données chiffrées 139

À propos du chiffrement

Le chiffrement est destiné à protéger le contenu d'un certain dossier contre l'examen de personnes non autorisées, même si celles-ci ont accès à l'appareil.

La première fois que vous accédez au chiffrement, vous devez définir un code secret (s'il n'est pas déjà défini). Le code secret est utilisé pour empêcher l'accès non autorisé à la fonction de chiffrement et aux données chiffrées. Le code secret permet également d'accéder aux paramètres de l'Antivol et du Contrôle parental.

Le contenu du dossier est chiffré dès l'exécution de la commande **Chiffre** après quoi les données sont chiffrées ou déchiffrées « au vol » au fur et à mesure que des données sont ajoutées, extraites ou consultées dans le dossier.

Le lancement des fichiers EXE exécutables depuis le dossier codé n'est pas supporté.

Des informations sur l'activité du composant seront consignées dans le journal de l'application.

Voir aussi

Code secret 91

Journaux du logiciel 144

Chiffrement des données

Le composant Chiffrement permet de chiffrer n'importe quel dossier (sauf les dossiers système) dans la mémoire de l'appareil ou dans une carte d'extension mémoire.

Pour protéger par chiffrement un dossier de l'appareil, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Chiffrer** dans l'onglet **Chiffrement**.
2. Dans l'écran affiché, sélectionnez le dossier que vous souhaitez chiffrer.

   Pour vous déplacer dans le système de fichiers, utilisez le stylo ou les boutons du joystick de votre appareil : **Haut**, **Bas** – pour vous déplacer à l'intérieur du dossier sélectionné ; **Gauche**, **Droit** – pour monter ou descendre de niveau par rapport au dossier courant.
3. Appuyez sur **Chiffrer** pour lancer le processus de chiffrement.

Le contenu du dossier est chiffré dès l'exécution de la commande après quoi les données sont chiffrées ou déchiffrées « au vol » au fur et à mesure que des données sont ajoutées, extraites ou consultées.

Figure 120 : Sélection des données à chiffrer

Vous ne pouvez chiffrer qu'un seul dossier au moyen de la fonction **Chiffrement**. Si vous souhaitez chiffrer un autre dossier, vous devez d'abord déchiffrer le dossier le dossier déjà protégé. Après l'opération de chiffrement, la commande **Chiffrer** change à **Déchiffrer**, ce qui vous permet de déchiffrer les données (voir section « Déchiffrement des données » à la page 138).

Déchiffrement des données

Il est possible de déchiffrer complètement les données préalablement protégées (voir section « Chiffrement de données » à la page 137).

Pour déchiffrer complètement le dossier préalablement chiffré,

Sélectionnez **Déchiffrer** dans l'onglet **Chiffrement** (voir figure suivante).

Figure 121 : Déchiffrement des données

Après l'opération, la commande **Déchiffrer** change à **Chiffrer** ce qui vous permet de chiffrer de nouveau les données (voir section « Chiffrement de données » à la page 137).

Interdiction d'accès aux données chiffrées

Pour s'assurer que les données sont protégées dès que l'appareil bascule en mode veille, il est possible d'activer le verrouillage par code secret.

Vous pouvez configurer un délai ou la demande immédiate du code secret.

Délai d'inactivité – définit le délai d'inactivité après la désactivation du rétro éclairage et le passage en mode veille de l'appareil, après lequel il est nécessaire de saisir le code secret pour consulter les données chiffrées.

Par défaut, le délai d'inactivité est désactivé (valeur **Non**), par conséquent, immédiatement après la désactivation du rétro éclairage, vous devrez saisir le code pour pouvoir accéder aux données chiffrées.

Pour activer le délai d'inactivité, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Chiffrement**.

2. Dans l'écran affiché, définissez le délai souhaité **1, 5, 15 minutes ou 1 heure** dans le paramètre **Intedire l'accés**.

3. Appuyez sur **Terminé** pour enregistrer les modifications..

Figure 122 : Interdiction d'accès aux données chiffrées

Vous pouvez également verrouiller momentanément l'accès aux données chiffrées et demander la saisie du code secret.

- *Pour une demande immédiate du code secret,*

  Appuyez sur l'icône Kaspersky Mobile Security dans la barre système de l'appareil et sélectionnez **Verrouiller les données** (voir figure suivante).

Figure 123 : Menu contextuel de l'icône

Mise à jour des bases du programme

Cette section décrit le composant de mise à jour. La mise à jour régulière des bases de données est nécessaire pour garantir un fonctionnement optimum de Kaspersky Mobile Security.

Dans cette section

À propos de la mise à jour des bases....141

Affichage d'informations sur les bases....142

Mise à jour manuelle....142

Planification des mises à jour....143

À propos de la mise à jour des bases

La recherche de logiciels malveillants fait appel au contenu de bases de données logicielles, contenant la description et les procédés de réparation de tous les logiciels malveillants connus jusqu'à ce jour, ainsi que la description d'autres objets indésirables. 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 par Internet depuis les serveurs de Kaspersky Lab ; ce qui exige une connexion Internet.

Pour afficher le détail des bases en cour d'usage, sélectionnez **Infos des bases** dans l'onglet **Informations**.

Des informations sur les mises à jour des bases de données sont consignées dans le journal du logiciel (voir section « Journaux du logiciel » à la page 144).

Affichage d'informations sur les bases

- *Pour afficher les informations sur les bases installées (voir figure suivante),*

  Sélectionnez **Infos des bases** dans l'onglet **Informations**.

*Figure 124 : L'onglet **Informations***

Mise à jour manuelle

Vous pouvez lancer la mise à jour manuellement à n'importe quel moment approprié.

Pour lancer la mise à jour manuelle des bases antivirus,

Sélectionnez **Mettre à jour** dans l'onglet **Anti-Virus** (voir figure suivante). Le programme lance la mise à jour des bases depuis le serveur.

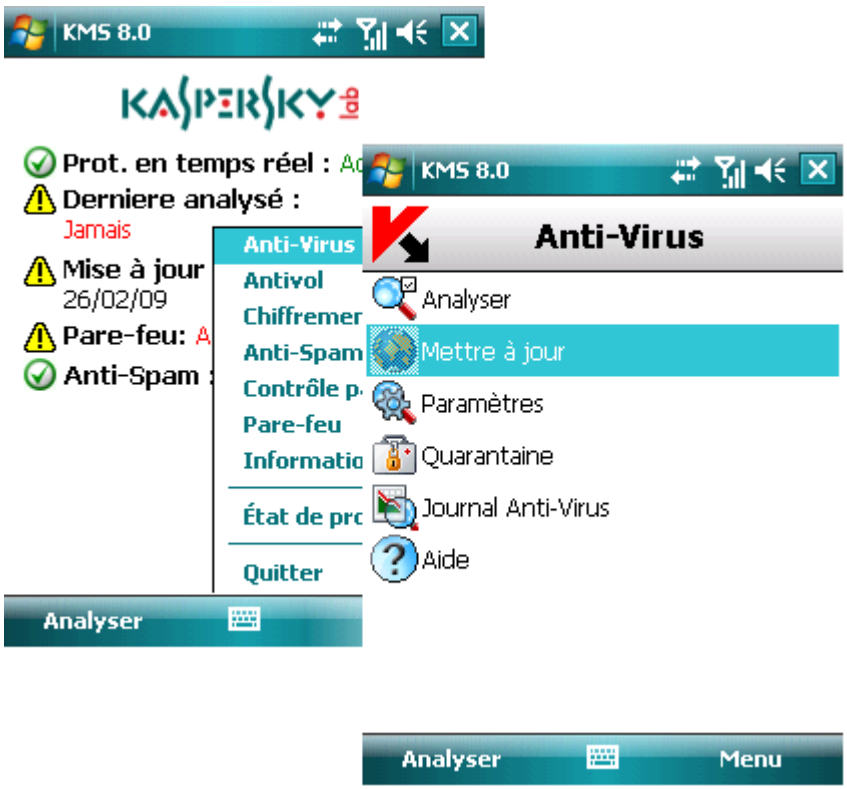

Figure 125 : Mise à jour manuelle

Planification des mises à jour

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Selon votre critère, vous pouvez configurer la mise à jour automatique des bases à n'importe quel moment approprié.

Pour configurer la mise à jour automatique des bases du logiciel, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Paramètres** dans l'onglet **Anti-Virus**.
2. Sélectionnez **Planification des MAJ**.
3. Spécifiez la fréquence dans le paramètre **Mise à jour auto :**
   - **Chaque jour** : la mise à jour s'exécute tous les jours. Le cas échéant, spécifiez l'**Heure** de la mise à jour.
   - **Chaque semaine** : la mise à jour s'effectuera une fois par semaine. Le cas échéant, spécifiez le **Jour de la semaine** et l'**Heure** de mise à jour.
   - **Inactif** : la mise à jour est lancée manuellement par l'utilisateur.

4. Cliquez sur **Terminé** pour enregistrer les modifications.

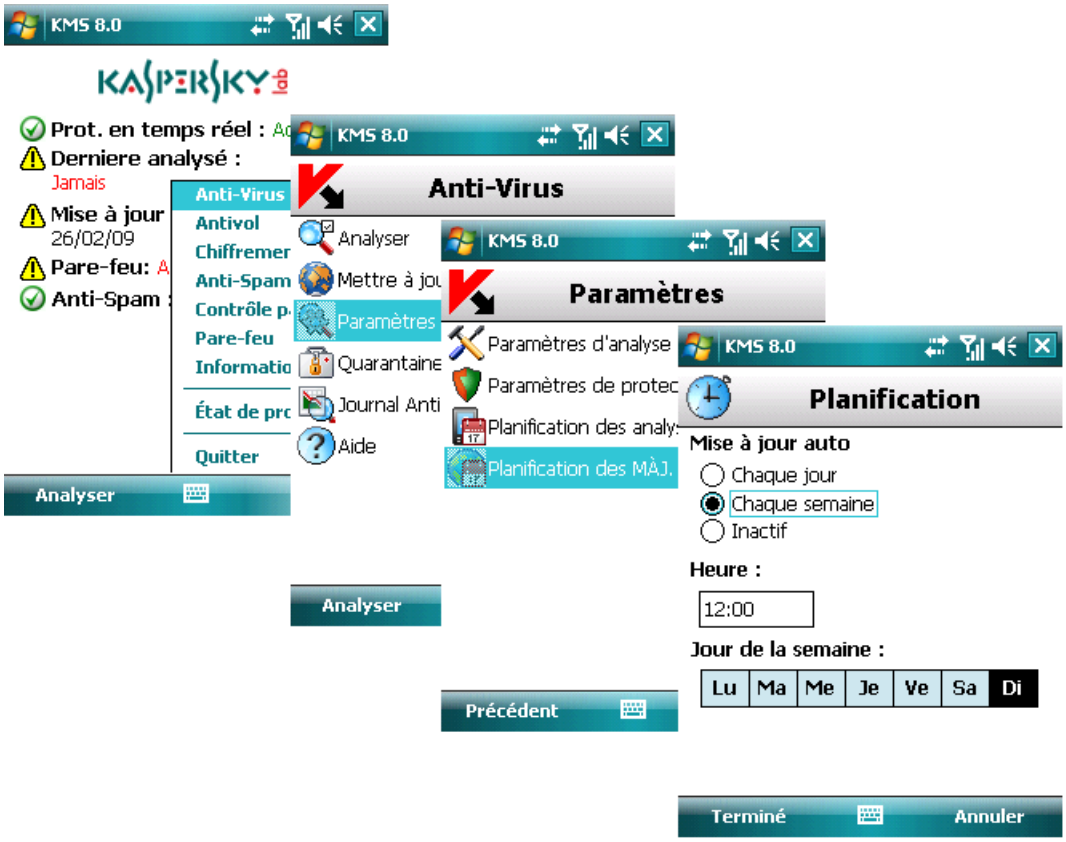

Figure 126 : Planification de la mise à jour

Journaux du logiciel

Cette section décrit les journaux de l'application et la gestion des informations qu'ils contiennent.

Dans cette section

À propos des journaux.....144

Affichage des événements du journal.....144

Suppression d'événements dans les journaux 145

À propos des journaux

Dans les journaux sont consignés les événements qui se produisent au cours des opérations de Kaspersky Mobile Security, classés par heure de consignation, à commencer par les entrées les plus récentes.

Affichage des événements du journal

➡ *Pour afficher tous les événements consignés dans le journal, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Journaux** dans l'onglet **Informations**.

2. Sélectionnez le journal du composant que vous souhaitez ouvrir.

Figure 127 : Affichage d'événements dans les journaux

➡ *Pour afficher le détail d'un événement consigné dans le journal*

Sélectionnez l'événement et appuyez sur **Détails**.

Suppression d'événements dans les journaux

➡ *Pour supprimer tous les événements du journal, procédez de la manière suivante (voir figure suivante) :*

1. Sélectionnez **Journaux** dans l'onglet **Informations**.

2. Ouvrez le journal de n'importe quel composant.

3. Appuyez sur **Menu** et sélectionnez **Supprimer tout**. Tous les événements du journal de chaque composant seront supprimés.

Figure 128 : Suppression d'enregistrement

Gestion de la licence

Kaspersky Mobile Security permet d'afficher les informations de la licence actuelle et de la renouveler si nécessaire.

Dans cette section

Affichage des informations de licence 147

Renouvellement de la licence 147

Affichage des informations de licence

Pour afficher les informations de licence :

Sélectionnez **Infos licence** dans l'onglet **Informations** (voir figure suivante).

Figure 129 : Affichage des informations de licence

Renouvellement de la licence

Pour renouveler votre licence, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Infos licence** dans l'onglet **Informations**.
2. Dans la fenêtre ouverte, sélectionnez **Activer** dans le menu **Menu**.

   La fenêtre de saisie du code d'activation s'affiche sur l'écran du smartphone.

3. Saisissez le code d'activation dans les 4 champs contigus. Le code d'activation est composé de lettres en alphabet latin et de chiffres, et n'est pas sensible à la casse. Après avoir saisi le code d'activation, appuyez sur **Continuer**. Le programme envoie une requête HTTP au serveur d'activation de Kaspersky Lab puis télécharge et installe le fichier clé.

Figure 130 : Renouvellement de la licence

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

Si l'installation de la clé réussit, les informations de licence sont affichées à l'écran. Pour continuer à utiliser l'application, appuyez sur **Terminer**.

Désinstallation du programme

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

1. Assurez-vous qu'il n'existe pas de données chiffrées (voir section « Chiffrement de données » à la page 137).

2. Fermez Kaspersky Mobile Security. Pour ce faire, appuyez sur **Menu** et sélectionnez **Quitter** (voir figure suivante).

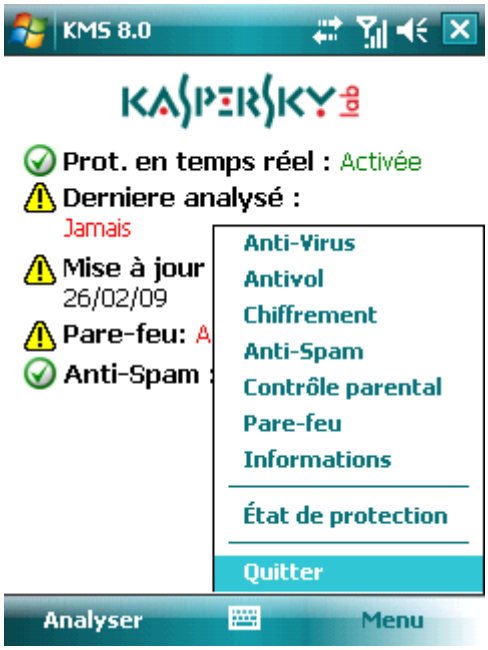

Figure 131 : Fin du travail du programme

3. Désinstallation du logiciel. Pour ce faire :

   a. Appuyez sur **Démarrer** et sélectionnez **Paramètres**.

   b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système** (voir figure suivante).

*Figure 132 : Onglet **Système***

c. Sélectionnez **Kaspersky Mobile Security** dans la liste des programmes installés et appuyez sur **Supprimer** (voir figure suivante).

Figure 133 : Sélection du programme

d. Appuyez sur **Oui** pour confirmer la désinstallation du programme.

e. Tapez le code secret à la demande du programme. Appuyez sur **OK**.

f. Pour sauvegarder la configuration du programme ou les objets en quarantaine, appuyez sur **Conserver** (voir figure suivante). Appuyez sur **Supprimer** pour désinstaller complètement le logiciel.

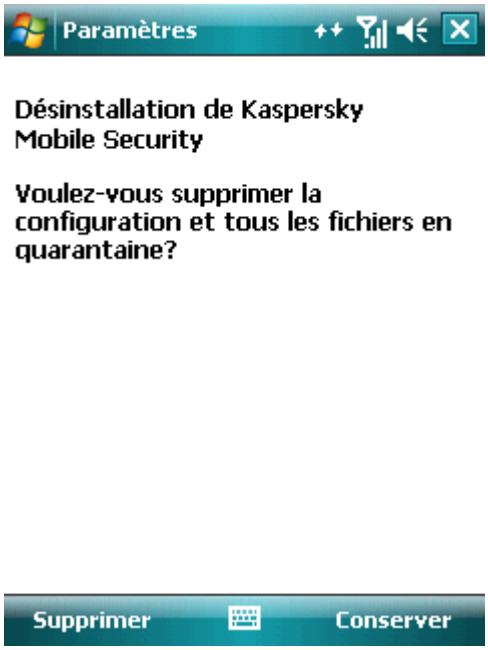

Figure 134 : Désinstallation du programme

4. Redémarrez l'appareil pour terminer la désinstallation.

Glossaire

A

Activation du logiciel

La procédure d'activation suppose de saisir le code d'activation puis de recevoir une clé que le logiciel utilise pour déterminer vos droits et la durée de licence.

Analyse à la demande

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

Archive

Fichier « conteneur » d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

Bases

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît. Pour améliorer la qualité de la détection des menaces, nous recommandons de télécharger régulièrement les mises à jour des bases de données depuis les serveurs de Kaspersky Lab.

Blocage d'un objet

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

D

Désinfection ou réparation d'objets

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

Durée de licence

Période de temps pendant laquelle il est possible d'exploiter toutes les caractéristiques d'une application Kaspersky Lab. Normalement, la durée de validité d'une licence est d'une année calendaire, à compter de son installation. Après l'expiration de la licence, le fonctionnement du programme est limité : vous ne pouvez plus mettre à jour la base de données.

L

Liste blanche

Les entrées de cette liste contiennent :

- *les numéros de téléphone*, depuis lesquels les appels et les messages SMS entrants sont autorisés par l'Anti-Spam, *et les numéros de téléphone* sur lesquels les appels et les messages SMS sortants sont autorisés par le Contrôle parental.
- *le texte*, dont la détection permet d'autoriser un message SMS entrant.

Liste noire

Les entrées de cette liste contiennent :

- *les numéros de téléphone*, depuis lesquels les appels et les messages SMS entrants sont refusé par l'Anti-Spam, *et les numéros de téléphone* sur lesquels les appels et les messages SMS sortants sont refusé par le Contrôle parental.

- *le texte*, dont la détection permet d'autoriser un message SMS entrant.

L

Masque de fichiers

Représentation du nom et de l'extension d'un fichier moyennant des caractères génériques. Les deux caractères génériques de base utilisés dans les masques de fichier sont « * » et « ? » (où « * » représente une suite de caractères quelconques et « ? » un seul caractère). Grâce à ces caractères génériques, il est possible de désigner n'importe quel fichier. Notez que le nom et l'extension du fichier sont toujours séparés par un point.

Mises à jour

Procédé de remplacement ou d'ajout de nouveaux fichiers (bases de données ou composants logiciels), téléchargés depuis les serveurs de mise à jour de Kaspersky Lab.

N

Non-numériques

Numéro de téléphone contenant des lettres ou composé intégralement de lettres.

P

Objet infecté

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible carune section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l' appareil.

P

Placer des objets en quarantaine

Méthode permettant de traiter des objets probablement infectés, en interdisant leur accès et en les déplaçant de leur position d'origine vers le dossier de quarantaine, où l'objet est enregistré sous une forme chiffrée qui annule toute menace d'infection.

Protection en temps réel

Mode de fonctionnement du programme dans lequel les objets sont analysés à la recherche de code malveillant en temps réel.

Le programme intercepte toutes les tentatives d'accès à n'importe quel objet en lecture, en écriture ou en exécution, et analyse la présence de menaces dans l'objet. Les objets non infectés sont délivrés à l'utilisateur ; les objets contenant des menaces ou suspects d'en contenir, sont traités conformément à la configuration des tâches (désinfection, suppression, quarantaine, etc.).

Q

Quarantaine

Dossier spécial dans lequel sont placés tous les objets probablement infectés, détectés pendant l'analyse de l' appareil ou par la protection en temps réel.

R

Restauration

Restitution de l'objet en quarantaine ou sauvegardé dans le dossier d'origine où il se trouvait avant d'être placé en quarantaine ou réparé, ou bien encore, dans un autre dossier choisi par l'utilisateur.

S

Suppression d'un message SMS

Méthode de traitement d'un message SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des messages SMS clairement indésirables.

Suppression d'un objet

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme (disque fixe, dossier, ressource réseau). Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

Kaspersky Lab

La société Kaspersky Lab a été fondée en 1997. Elle compte aujourd'hui parmi les premiers développeurs de bon nombre de produits de sécurité informatique performants, comprenant des systèmes antivirus, antispam et anti-piratage.

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 (Californie), dans les pays du Benelux, en Chine, en Pologne et en Roumanie. Un nouveau service de la compagnie, le centre européen de recherches antivirus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises dans le monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 400 professionnels, tous spécialistes des technologies antivirus. Neuf d'entre eux possèdent un M.B.A et 15 autres un doctorat. Les analystes senior de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. 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 premiers fabricants de logiciels antivirus. 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 systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. 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. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus® dans leurs produits : Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Allemagne), Deerfield (USA), Alt-N (USA), 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. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. 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.

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

Site officiel de Kaspersky Lab :	http://www.kaspersky.com/fr
Encyclopédie de virus :	http://www.viruslist.com/fr/
Laboratoire antivirus :	http://newvirus.kaspersky.fr
Forum de Kaspersky Lab :	http://forum.kaspersky.com

Crypto Ex Ltd.

Pour la création et vérification de signatures numériques, Kaspersky Anti-Virus utilise la bibliothèque Crypto C de sécurité informatique de Crypto Ex Ltd. La licence de CryptoEx Ltd est fournie par la Federal Agency for Government Communications and Informations (Federal Security Service de la Fédération Russe) pour le développement de la bibliothèque Crypto C de protection de données et d'authentification.

Site corporatif de CryptoEx Ltd : http://www.cryptoex.ru

Index

A

ACTIONS
- ANALYSE À LA DEMANDE 27, 101
- PROTECTION EN TEMPS RÉEL 20, 94

ACTIVER
- ANTI-SPAM 36, 106
- CHIFFREMENT 69, 137
- CONTRÔLE PARENTAL 49, 118
- FIREWALL 67, 135
- PROTECTION EN TEMPS RÉEL 18, 93

ACTIVER LE LOGICIEL 13, 88

AFFICHER
- ICÔNE DE PROTECTION 21
- RÉTRO-ÉCLAIRAGE 31

AJOUTER
- LISTE BLANCHE ANTI-SPAM 41, 110
- LISTE BLANCHE DU CONTRÔLE PARENTAL 54, 122
- LISTE NOIRE ANTI-SPAM 37, 107
- LISTE NOIRE DU CONTRÔLE PARENTAL 50, 119

ANALYSE À LA DEMANDE
- ACTIONS À APPLIQUER SUR LES OBJETS 27, 101
- EXÉCUTION MANUELLE 23, 96
- EXECUTION PLANIFIEE 25, 99
- OBJETS À ANALYSER 26, 99

ANTI-SPAM
- ACTION À APPLIQUER SUR UN APPEL 48, 117
- ACTION À APPLIQUER SUR UN MESSAGE 47, 116
- LISTE BLANCHE 41, 110
- LISTE NOIRE 37, 107
- MODES 36, 106
- NON-NUMÉRIQUES 45, 114

ARCHIVES
- ANALYSE À LA DEMANDE 30, 99

AUTORISER
- APPELS ENTRANTS 41, 110
- APPELS SORTANTS 54, 122
- CONNEXIONS RÉSEAU 67, 135
- MESSAGES SMS ENTRANTS 41, 110
- MESSAGES SMS SORTANTS 54, 122

C

CODE
- CODE D'ACTIVATION 13, 88
- CODE SECRET 16, 91

CONTRÔLE PARENTAL
- LISTE BLANCHE 54, 122
- LISTE NOIRE 50, 119
- MODES 49, 118

COORDONNÉES DE L'APPAREIL 64, 132

D

DÉSACTIVER
- ANTI-SPAM 36, 106
- CHIFFREMENT 70, 138
- CONTRÔLE PARENTAL 49, 118
- FIREWALL 67, 135

PROTECTION EN TEMPS RÉEL 18, 93

DÉSINSTALLER
PROGRAMME 82, 148

DONNÉES
CHIFFREMENT 69, 137
DÉCHIFFREMENT 70, 138
SUPPRESSION 61, 129
VERROUILLAGE AVEC UN CODE 71, 139

E

ENTRÉE
LISTE BLANCHE ANTI-SPAM 41, 110
LISTE BLANCHE DU CONTRÔLE PARENTAL 54, 122
LISTE NOIRE ANTI-SPAM 37, 107

ÉTAT DU PROGRAMME 78

EXÉCUTER
ANALYSE À LA DEMANDE 23, 96
MISE À JOUR 73, 142
PROGRAMME 14, 89

F

FIREWALL
NIVEAU DE SÉCURITÉ 67, 135

FONCTIONNEMENT DU CODE SECRET 71, 139

I

ICÔNE DE PROTECTION 21

INTERDIRE
APPELS ENTRANTS 37, 107, 119
APPELS SORTANTS 50, 119
CONNEXIONS RÉSEAU 67, 135
DONNÉES CHIFFRÉES 71, 139
MESSAGES SMS ENTRANTS 37, 107, 119
MESSAGES SMS SORTANTS 50, 119

INTERDIRE L'ACCÈS AUX DONNÉES 71, 139

J

JOURNAUX
AFFICHAGE DES ÉVÉNEMENTS 78, 144
SUPPRESSION D'ÉVÉNEMENTS 78, 145

K

KASPERSKY LAB 8

L

LICENCE
ACTIVATION DU LOGICIEL 13, 88
INFORMATIONS 80, 147
RENOUVELLEMENT 81, 147

LISTE BLANCHE
ANTI-SPAM 41, 110
CONTRÔLE PARENTAL 54, 122

LISTE NOIRE
ANTI-SPAM 107
CONTRÔLE PARENTAL 50, 119

LISTE NOIRE ANTI-SPAM 37

LOCALISATION 63, 131

M

METTRE À JOUR
EXÉCUTION MANUELLE ... 73, 142
EXÉCUTION PLANIFIÉE ... 74, 143
ITINÉRANCE ... 75
MODES
ANTI-SPAM ... 36, 106
CONTRÔLE PARENTAL ... 49, 118

O

OBJET INFECTÉ ... 152

P

PLANIFIER
ANALYSE A LA DEMANDE ... 25, 99
MISE À JOUR ... 74, 143
PROTECTION EN TEMPS RÉEL
ACTIONS À APPLIQUER SUR LES OBJETS ... 20, 94
ACTIVATION ... 18, 93
DÉSACTIVATION ... 18, 93
OBJETS À ANALYSER ... 19

Q

QUARANTAINE
AFFICHAGE DES OBJETS ... 33, 103
RESTAURATION D'UN OBJET ... 34, 103
SUPPRESSION D'UN OBJET ... 34, 104

R

RENOUVELER LA LICENCE ... 81, 147
RÉSEAU
CONNEXION ... 76
RESTAURATION ... 152
RÉTRO-ÉCLAIRAGE ... 31

S

SIM-SURVEILLANCE ... 62, 130
SMS INVISIBLE ... 65, 133
SMS-CLEAN ... 60
SON ... 79
SUPPRESSION ... 128
SUPPRIMER
DONNÉES PERSONNELLES ... 61, 129
ÉVÉNEMENTS DES JOURNAUX ... 78, 145
LISTE BLANCHE ANTI-SPAM ... 43, 112
LISTE BLANCHE DU CONTRÔLE PARENTAL ... 56, 124
LISTE NOIRE ANTI-SPAM ... 39, 109
LISTE NOIRE DU CONTRÔLE PARENTAL ... 52, 121
OBJET DE LA QUARANTAINE ... 34, 104

V

VERROUILLAGE ... 59, 126
VERROUILLER
APPAREIL ... 59, 127