Kaspersky Endpoint Security 8 for Smartphone

pour Symbian OS

Guide de l'utilisateur

VERSION DE L'APPLICATION : 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.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, Kaspersky Lab) et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois de la France.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et ses illustrations ne peuvent être utilisés qu'à des fins d'information à usage non-commercial ou personnel.

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.

Kaspersky Lab décline toute responsabilité en rapport au contenu, à la qualité, à la pertinence ou à la précision de matériels, utilisés dans ce document, dont les droits sont la propriété de tiers, ou aux dommages potentiels associés à l'utilisation de ce type de documents.

Ce document fait référence à des marques enregistrées et à des marques de services qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 27.05.2011

© Kaspersky Lab ZAO, 1997–2011

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

TABLE DES MATIERES

A PROPOS DE CE MANUEL

Le présent document est un Guide d'installation, de configuration et d'utilisation de l'application Kaspersky Endpoint Security 8 for Smartphone. Ce document est destiné au grand public.

Buts du document :

- aider l'utilisateur à installer l'application sur l'appareil mobile par ses propres soins, à l'activer et à configurer l'application d'une manière équilibrée en fonction des tâches utilisateur ;
- à assurer une recherche d'information rapide pour résoudre des problèmes liés à l'application ;
- à informer sur les autres sources d'information concernant l'application, ainsi que sur les possibilités d'obtenir l'assistance technique.

SOURCES D'INFORMATIONS COMPLEMENTAIRES

Pour toute question sur l'installation ou l'utilisation de Kaspersky Endpoint Security 8 for Smartphone, vous pouvez rapidement trouver des réponses en utilisant plusieurs sources d'information. Vous pouvez sélectionner celle qui vous convient le mieux en fonction de l'importance et de l'urgence du problème.

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

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

Page sur le site Web de Kaspersky Lab

http://www.kaspersky.com/fr/endpoint-security-smartphone

Utilisez cette page pour obtenir des informations générales sur Kaspersky Endpoint Security 8 for Smartphone, ses possibilités et ses caractéristiques de fonctionnement.

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

http://support.kaspersky.com/fr/kes8m

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

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Endpoint Security 8 for Smartphone. Ces articles sont regroupés par sujet, par exemple «Utilisation des fichiers de licence», «Mise à jour des bases» ou «Elimination des échecs». Les articles répondent non seulement à des questions sur Kaspersky Endpoint Security 8 for Smartphone, 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 problème concernant un écran ou un onglet spécifiques de Kaspersky Endpoint Security 8 for Smartphone, vous disposez de l'aide contextuelle.

Pour accéder à l'aide contextuelle, ouvrez l'écran en question et cliquez sur **Aide** ou sélectionnez **Menu** → **Aide**.

Documentation

Le kit de distribution de Kaspersky Endpoint Security 8 for Smartphone comprend le **Guide de l'utilisateur** (format PDF). Ce document décrit les procédures d'installation, de suppression, d'administration des paramètres de l'application, ainsi que celles de premier lancement de l'application et de configuration de ses composants. Le

document décrit l'interface de l'application, propose des solutions pour des tâches type de l'utilisateur lors de l'utilisation de l'application.

PUBLIER DES MESSAGES DANS LE FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.com.

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.

CONTACTER L'EQUIPE DE REDACTION DE LA DOCUMENTATION

Si vous avez des questions concernant la documentation, ou vous y avez trouvé une erreur, ou vous voulez laisser un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs. Pour contacter l'Équipe de rédaction de la documentation, envoyez un message à docfeedback@kaspersky.com. Dans le champ d'objet mettez «Kaspersky Help Feedback : Kaspersky Endpoint Security 8 for Smartphone».

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protège les données stockées sur les appareils mobiles tournant sous Symbian OS. L'application protège les données de l'appareil contre l'infection par des menaces connues, refuse les SMS et les appels non sollicités, contrôle les connexions de réseau de l'appareil, chiffre les données, masque les informations pour les contacts confidentiels et protège les données confidentielles en cas de perte ou de vol de l'appareil. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier. L'installation et la configuration de l'application sont effectuées par l'administrateur via les systèmes d'administration distante.

Kaspersky Endpoint Security 8 for Smartphone reprend les composants de protection suivants :

- **Anti-Virus**. Protège le système de fichiers de l'appareil mobile contre les virus et autres programmes malveillants. Antivirus permet d'identifier et de neutraliser les objets malveillants sur votre appareil, ainsi que de mettre à jour les bases antivirus de l'application.
- **Anti-Spam**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant permet de configurer en souplesse la fonction de blocage des SMS et des appels considérés comme indésirables.
- **Antivol** Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol tout en facilitant sa recherche. Antivol permet de verrouiller l'appareil à distance à l'aide des SMS, de supprimer les données qu'il contient et de déterminer ses coordonnées géographiques (si l'appareil mobile est doté d'un récepteur GPS). De plus, Antivol permet également de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.
- **Contacts personnels**. Masque les informations liées aux numéros confidentiels de la Liste des contacts que vous avez créée. Les Contacts personnels masquent les entrées des Contacts, les SMS, les entrées dans le journal des appels, les SMS reçus et les appels entrants pour ce type de numéros.
- **Pare-feu**. Contrôle les connexions de réseau de votre appareil mobile. Le Pare-feu permet de définir les connexions qui seront autorisées ou interdites.
- **Chiffrement**. Stocke les données en mode crypté. Le composant Chiffrement permet de crypter un nombre quelconque de dossiers qui ne sont pas définis par le système et enregistrés aussi bien dans la mémoire de l'appareil que sur les cartes mémoire. L'accès aux fichiers depuis les dossiers chiffrés est offert uniquement après avoir saisi le code secret de l'application.

Outre cela, l'application propose diverses fonctions de service permettant de maintenir l'application dans un état actuel, élargir les possibilités d'utilisation de l'application, et ceux qui aide l'utilisateur à travailler :

- État de la protection. Les états des composants de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection des données stockées sur l'appareil.
- La mise à jour des bases antivirus de l'application. Cette fonction permet de maintenir les bases antivirus de Kaspersky Endpoint Security 8 for Smartphone à jour.
- Journal des événements. Les informations sur le fonctionnement de chacun des composants (par exemple, rapport d'analyse, mise à jour des bases antivirus, détails sur un fichier bloqué) sont consignées dans un journal des événements spécifique. Les rapports sur le fonctionnement des composants sont envoyés et stockés dans le système d'administration distante.

Kaspersky Endpoint Security 8 for Smartphone ne réalise pas de copies de sauvegarde des données en vue d'une restauration ultérieure.

DANS CETTE SECTION

NOUVEAUTES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Voici une présentation détaillée des nouveautés de Kaspersky Endpoint Security 8 for Smartphone.

Nouveautés au niveau de la protection :

- L'accès au programme est régi par un mot de passe.
- La liste des fichiers exécutables, analysés par Protection et Analyse (dans le cas de limitation du type des fichiers exécutables), est élargie. L'application analyse uniquement les fichiers exécutables des applications aux formats suivants : EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS. La liste des archives analysées est également élargie. L'application analyse les archives des formats suivants : ZIP, JAR, JAD, SIS и SISX.
- Pour les contacts confidentiels, le composant Contacts personnels permet de masquer les informations suivantes : entrées dans les Contacts, correspondance SMS, journal des appels, SMS reçus et appels entrants. Les informations confidentielles sont accessibles si la fonction de dissimulation est désactivée.
- Le composant Chiffrement permet de chiffrer les dossiers enregistrés dans la mémoire de l'appareil ou sur une carte de mémoire. Le composant stocke les informations confidentielles en mode crypté et ne permet d'accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application.
- La version actualisée de l'Antivol propose la fonction de Géolocalisation qui permet de recevoir les coordonnées géographiques de l'appareil au numéro de téléphone ou à l'adresse de la messagerie électronique définie en cas de perte ou de vol. De plus, Antivol propose une version actualisée de la fonction de Suppression qui permet de supprimer à distance non seulement les données personnelles de l'utilisateur, stockées dans la mémoire de l'appareil ou sur la carte mémoire, mais aussi les fichiers de la liste des dossiers à supprimer que vous avez créée.
- Pour réduire le trafic, l'application propose une nouvelle fonctionnalité qui permet de désactiver automatiquement la mise à jour des bases de l'application en itinérance.
- L'application propose également une nouvelle fonction de service Affichage des astuces : Kaspersky Endpoint Security 8 for Smartphone affiche une brève description du composant avant la configuration de ses paramètres.

CONFIGURATION LOGICIELLE ET MATERIELLE

Kaspersky Endpoint Security 8 for Smartphone peut être installé sur des appareils mobiles avec des systèmes d'exploitation Symbian OS 9.1, 9.2, 9.3 et 9.4 Series 60® UI.

INSTALLATION DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

L'installation de Kaspersky Endpoint Security 8 for Smartphone est effectuée par l'administrateur avec des outils d'administration distante. En fonction de l'outil d'administration utilisé par l'administrateur, l'installation peut être effectuée automatiquement ou peut nécessiter une intervention de l'utilisateur.

Si l'installation de l'application nécessite une intervention de l'utilisateur, il faut recourir à une des procédures suivantes :

- L'utilitaire d'installation homonyme de l'application Kaspersky Endpoint Security 8 for Smartphone s'installe sur votre poste de travail. Il vous permet d'installer Kaspersky Endpoint Security 8 for Smartphone sur votre appareil mobile.
- Vous recevez par courrier électronique un message d'administrateur contenant la distribution de l'application ou l'instruction sur le téléchargement de la distribution. Procédez à l'installation de Kaspersky Endpoint Security 8 for Smartphone sur l'appareil mobile en vous référant aux instructions du message.

Cette section détaille les démarches qui précèdent l'installation de Kaspersky Endpoint Security 8 for Smartphone, décrit les types d'installation de l'application sur l'appareil mobile et les actions de l'utilisateur pour chacun d'eux.

DANS CETTE SECTION

INSTALLATION AUTOMATIQUE DE L'APPLICATION

L'administrateur lance l'installation de l'application sur l'appareil avec des outils d'administration distante.

L'appareil mobile reçoit la distribution de Kaspersky Endpoint Security 8 for Smartphone et exécute l'installation automatique.

Ensuite, vous serez invité à intervenir pour assurer l'installation de l'application.

Pour installer l'application, procédez comme suit :

1. Pour confirmer l'installation de l'application, cliquez sur **Oui**.
2. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.

   Si la langue du système d'exploitation ne correspond pas à la langue de Kaspersky Endpoint Security 8 for Smartphone, un message s'affiche. Pour continuer l'installation de l'application dans la langue actuelle, cliquez sur **OK**.
3. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. L'installation de Kaspersky Endpoint Security 8 for Smartphone est lancée. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue. Une nouvelle tentative d'installation sera faite pendant la synchronisation suivante de l'appareil avec le système d'administration distante.
4. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade en cliquant sur **OK**.

L'application sera installée sur l'appareil.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

A PROPOS DE L'INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

Si l'administrateur a installé l'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone sur votre poste de travail, vous pouvez installer Kaspersky Endpoint Security 8 for Smartphone sur les appareils mobiles connectés à cet ordinateur. L'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone contient le distributif de l'application et le transmet sur l'appareil. Après l'installation de l'utilitaire sur le poste de travail, l'utilitaire est activé automatiquement et contrôle la connexion des appareils mobiles à l'ordinateur. A chaque connexion de l'appareil mobile au poste de travail, l'utilitaire contrôle si l'appareil est conforme aux spécifications système de Kaspersky Endpoint Security 8 for Smartphone et propose de l'installer l'application.

Pour une installation réussie, l'application Nokia Ovi Suite ou Nokia® Ovi® Suite ou Nokia PC Suite doit être installée sur le poste de travail.

INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

Si l'utilitaire de transmission Kaspersky Endpoint Security 8 for Smartphone est installé sur votre poste de travail, alors à chaque connexion des appareils, satisfaisant les exigences de système, l'installation de Kaspersky Endpoint Security 8 for Smartphone vous sera proposée.

Vous pouvez interdire l'installation de Kaspersky Endpoint Security 8 for Smartphone lors des connexions suivantes des appareils à l'ordinateur.

Pour installer l'application sur l'appareil mobile, procédez comme suit :

1. Connectez l'appareil mobile à l'ordinateur avec Nokia Ovi Suite ou Nokia PC Suite.

   Si l'appareil est conforme aux spécifications système d'installation de l'application, la fenêtre **KES 8** avec les informations sur l'utilitaire s'ouvrira (cf. ill. ci-après).

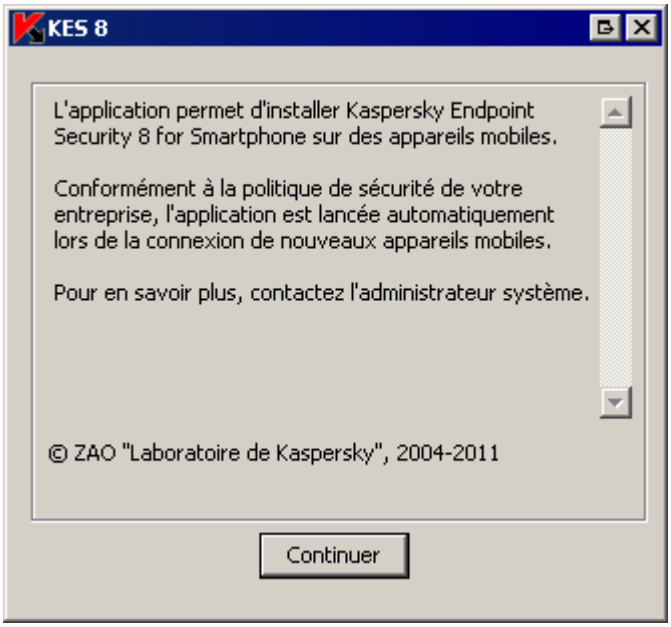

Figure 1: programme d'installation de Kaspersky Endpoint Security 8 for Smartphone

2. Cliquez sur le bouton **Continuer**.

   La fenêtre **KES 8** avec la liste des appareils connectés découverts s'ouvrira.

   Si plusieurs appareils conformes aux spécifications système sont connectés au poste de travail, ils seront affichés sur la liste des appareils connectés dans la fenêtre **KES 8**.

3. Sélectionnez un ou plusieurs appareils dans la liste des appareils connectés pour installer l'application. Pour ce faire, cochez les cases à côté des appareils (cf. ill. ci-après).

Figure 2: sélection des appareils pour installer Kaspersky Endpoint Security 8 for Smartphone

4. Cliquez sur **Installer**.

   L'utilitaire transmet la distribution de l'application vers les appareils sélectionnés. L'état de la transmission sera affiché dans la fenêtre **KES 8.0** du poste de travail.

   Après la transmission de la distribution, l'installation de l'application sur les appareils mobiles sélectionnés sera lancée automatiquement.

5. Pour confirmer l'installation de l'application, cliquez sur **Oui**.

6. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.

   Si la langue du système d'exploitation ne correspond pas à celle de Kaspersky Endpoint Security 8 for Smartphone, un message s'affiche. Pour continuer l'installation de l'application dans la langue actuelle, cliquez sur **OK**.

7. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. L'installation de Kaspersky Endpoint Security 8 for Smartphone est lancée. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.

8. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade en cliquant sur **OK**.

   L'application sera installée sur l'appareil.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

- *Vous pouvez interdire l'installation de Kaspersky Endpoint Security 8 for Smartphone lors des connexions suivantes des appareils à l'ordinateur,*

  dans la fenêtre **KES 8**, cochez la case **Interrompre le lancement automatique de l'application pour l'installation de Kaspersky Endpoint Security 8 for Smartphone**.

A PROPOS DE L'INSTALLATION DE L'APPLICATION APRES LA RECEPTION D'UN MESSAGE ELECTRONIQUE

Vous recevez par courrier électronique un message d'administrateur contenant la distribution de l'application ou l'instruction sur le téléchargement de la distribution.

Le message contient les informations suivantes :

- la distribution de l'application jointe au message ou un lien pour la télécharger ;
- les détails sur les paramètres de connexion de l'application au système d'administration distante.

Il est déconseillé de supprimer ce message avant que Kaspersky Endpoint Security 8 for Smartphone soit installé sur l'appareil.

INSTALLATION DE L'APPLICATION APRES LA RECEPTION D'UN MESSAGE ELECTRONIQUE

Pour installer Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Ouvrez le message avec les paramètres d'installation de l'application sur l'appareil mobile ou sur le poste de travail.
2. Exécutez une des opérations suivantes :
   - Si le message contient un lien, cliquez-le et téléchargez la distribution de l'application.
   - Si la distribution est jointe au message, téléchargez la distribution de l'application.
3. Exécutez une des opérations suivantes :
   - Si vous avez téléchargé la distribution de l'application sur l'appareil mobile, l'installation de l'application sera lancée automatiquement.
   - Si vous avez téléchargé la distribution sur le poste de travail, connectez l'appareil mobile à l'ordinateur avec Nokia Ovi Suite ou Nokia PC Suite, copiez la distribution sur l'appareil. L'installation de l'application sur l'appareil sera effectuée automatiquement.
4. Pour confirmer l'installation de l'application, cliquez sur **Oui**.
5. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.

   Si la langue du système d'exploitation ne correspond pas à celle de Kaspersky Endpoint Security 8 for Smartphone, un message s'affiche. Pour continuer l'installation de l'application dans la langue actuelle, cliquez sur **OK**.
6. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. L'installation de Kaspersky Endpoint Security 8 for Smartphone est lancée. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.
7. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade en cliquant sur **OK**.

   L'application sera installée sur l'appareil mobile.

8. Lancez l'application (cf. la rubrique «Lancement de l'application» à la page 24). Pour ce faire, sélectionnez **Applications** → **Install.** → **KES 8** et lancez l'application avec le stylet ou la touche centrale du joystick

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

9. Saisissez le code secret de l'application (cf. la rubrique «Installation du code secret» à la page 24). Pour ce faire, remplissez le champ **Saisissez le nouveau code**, puis le champ **Confirmation du code** et cliquez sur **OK**.

   L'écran **Paramètres de synchr.** s'ouvrira. (voir figure suivante).

Figure 3: paramètres de synchronisation

10. Spécifiez les valeurs des paramètres de connexion au système d'administration distante, s'ils figurent dans le message de l'administrateur que vous avez reçu. Saisissez les valeurs des paramètres suivant :

    - **Serveur** ;
    - **Port** ;
    - **Groupe**.

    Si les valeurs pour les paramètres sollicités n'ont pas été spécifiées dans le message de l'administrateur que vous avez reçu, contactez l'administrateur.

11. Saisissez dans le champ **Votre adr. électr.** l'adresse électronique de votre société et cliquez sur **OK**.

    Saisissez l'adresse électronique correctement parce qu'elle sera utilisée pour enregistrer l'appareil dans le système d'administration distante.

Si vous avez constaté des erreurs pendant l'installation de l'application, contactez l'administrateur.

SUPPRESSION DE L'APPLICATION

L'application ne peut être supprimée de l'appareil qu'en mode manuel par l'utilisateur.

Les actions suivantes sont automatiquement exécutées à la suppression :

- La dissimulation des informations confidentielles se désactive.
- Les données sur l'appareil qui ont été chiffrées à l'aide de Kaspersky Endpoint Security 8 for Smartphone sont déchiffrées.

Pour supprimer Kaspersky Endpoint Security 8 for Smartphone à la main, procédez comme suit :

1. Fermez Kaspersky Endpoint Security 8 for Smartphone. Pour ce faire, choisissez **Fonctions** → **Quitter** (cf. ill. ci-après).

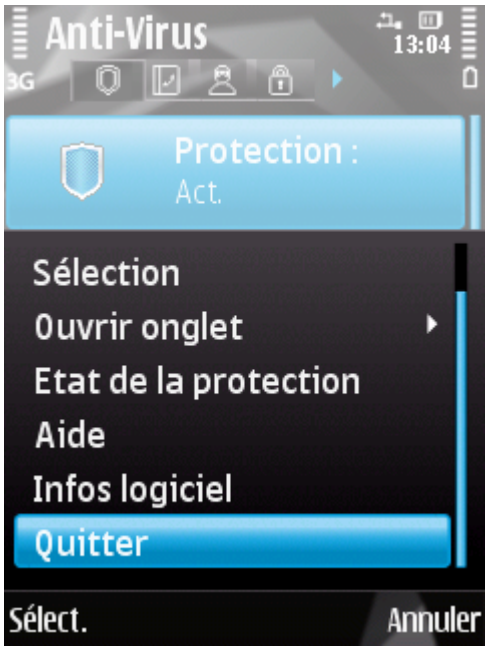

Figure 4 : Quitter le logiciel

2. Désinstallation de Kaspersky Endpoint Security 8 for Smartphone Pour ce faire, exécutez les actions suivantes :
   a. Ouvrez le menu principal de l'appareil.
   b. Sélectionnez le dossier **Applications** → **Install.** (voir figure suivante).

Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

Figure 5 : chemin d'accès aux applications installées

   c. Dans la liste des applications, sélectionnez **KES 8**, puis choisissez **Fonctions** → **Désinstaller** (cf. ill. ci-après).

Figure 6: suppression de l'application

d. Pour confirmer la suppression de l'application, cliquez sur **Oui**.

e. Saisissez le code secret puis cliquez sur **OK**.

f. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :

- Si vous souhaitez conserver les paramètres de l'application et les objets en quarantaine, cochez la case en regard des paramètres requis, puis cliquez sur **OK** (cf. ill. ci-après).
- Pour supprimer complètement une application, cliquez sur **Annuler**.

Figure 7 : liste des paramètres à sauvegarder

La suppression de l'application va commencer.

Si la dissimulation des informations confidentielles sur votre appareil est activée et / ou un ou plusieurs dossiers ont été chiffrés à l'aide de Kaspersky Endpoint Security 8 for Smartphone, l'application vous invite à désactiver la dissimulation des données confidentielles et/ou à déchiffrer tous les dossiers.

3. Redémarrez l'appareil pour terminer la suppression de l'application.

ADMINISTRATION DES PARAMETRES DE L'APPLICATION

Tous les paramètres de Kaspersky Endpoint Security 8 for Smartphone, licence comprise, sont configurés par l'administrateur via le système d'administration distante. Dans ce cas, l'administrateur peut autoriser ou interdire à l'utilisateur de modifier les valeurs de ces paramètres.

Vous pouvez modifier les paramètres de fonctionnement de l'application sur l'appareil mobile si cette modification a été autorisée par l'administrateur.

Si à gauche du paramètre de l'application s'affiche un verrou, le paramètre de l'application de l'appareil mobile ne peut pas être modifié.

Si l'administrateur a changé les paramètres de l'application, ils seront envoyés vers l'appareil via le système d'administration distante. Dans ce cas, les paramètres interdits à la modification par l'administrateur seront également modifiés. Les valeurs des paramètres que l'administrateur n'a pas interdit à la modification, restent les mêmes.

Si l'appareil n'a pas reçu les paramètres de l'application ou si vous voulez restaurer les valeurs des paramètres définies par l'administrateur, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique «Lancement de la synchronisation à la main» à la page 22).

L'utilisation de la fonction de la synchronisation n'est possible que sous la direction de l'administrateur.

GESTION DE LA LICENCE

Cette section propose des informations sur la licence, sur les modalités de son activation et la procédure de consultation des informations qui la concerne.

DANS CETTE SECTION

PRESENTATION DES LICENCES DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

La *licence* est le droit d'utilisation de Kaspersky Endpoint Security 8 for Smartphone et des services complémentaires associés offerts par Kaspersky Lab ou ses partenaires.

Pour pouvoir utiliser l'application, vous devez installer la licence.

Chaque licence se définit par sa durée de validité et son type.

La *durée de validité de la licence* désigne la période pendant laquelle vous pouvez bénéficier des services complémentaires :

- Assistance technique ;
- La mise à jour des bases antivirus de l'application.

Le volume des services proposés dépend du type de licence.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Endpoint Security 8 for Smartphone.

  Toutes les fonctions de l'application sont accessibles pendant l'action de la version d'évaluation. Une fois la licence d'évaluation expirée, Kaspersky Endpoint Security 8 for Smartphone arrête de fonctionner. Seules les fonctions suivantes sont accessibles :

  - désactiver des composants Chiffrement et Contacts personnels ;
  - l'utilisateur peut déchiffrer les dossiers qu'il a sélectionnés pour le chiffrement ;
  - désactiver de la dissimulation des informations confidentielles ;
  - consulter le système d'aide ;
  - synchronisation avec le système d'administration distante.

- *Commerciale* : licence payante avec une durée de validité définie (par exemple, un an) octroyée à l'achat de Kaspersky Endpoint Security 8 for Smartphone.

  Toutes les fonctionnalités de l'application et les services complémentaires sont accessibles pendant la période de validité de la licence commerciale.

  Une fois que la licence commerciale a expiré, les fonctionnalités de Kaspersky Endpoint Security 8 for Smartphone seront limitées. Vous pouvez toujours utiliser les composants Anti-Spam et Pare-feu, effectuer l'analyse antivirus de votre ordinateur et utiliser les composants de la protection, mais la date de mise à jour des bases antivirus sera celle de l'expiration de la licence. Uniquement les actions suivantes sont disponibles pour d'autres composants :

  - désactiver des composants Chiffrement, Antivol et Contacts personnels ;
  - déchiffrer les dossiers sélectionnés par l'utilisateur à chiffrer ;

- désactiver de la dissimulation des informations confidentielles ;
- consulter le système d'aide ;
- synchronisation avec le système d'administration distante.

INSTALLATION D'UNE LICENCE

La licence est installée via le système d'administration distante par l'administrateur.

Toutes les fonctionnalités de Kaspersky Endpoint Security 8 for Smartphone restent opérationnelles pendant trois jours qui suivent l'installation de l'application. Durant cette période, l'administrateur installe la licence via le système d'administration distante pour activer l'application.

Si la licence n'a pas été installée pendant trois jours les fonctionnalités de l'application seront limitées. Dans ce mode vous pouvez :

- désactiver tous les composants ;
- déchiffrer un ou plusieurs dossiers ;
- désactiver de la dissimulation des informations confidentielles ;
- consulter le système d'aide.

Si la licence n'a pas été installée dans les trois jours qui suivent l'installation de l'application, pour installer la licence, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique «Lancement de la synchronisation à la main» à la page 22).

AFFICHAGE DES INFORMATIONS DE LICENCE

Vous pouvez consulter les informations suivantes sur la licence : le numéro de la licence, le type, la date d'activation, la date de l'expiration, le nombre de jours restant avant l'expiration et le numéro de série de l'appareil.

➧ *Pour consulter les informations relatives à la licence,*

sous l'onglet **Avancé**, choisissez l'option **Infos licence** (cf. ill. ci-après).

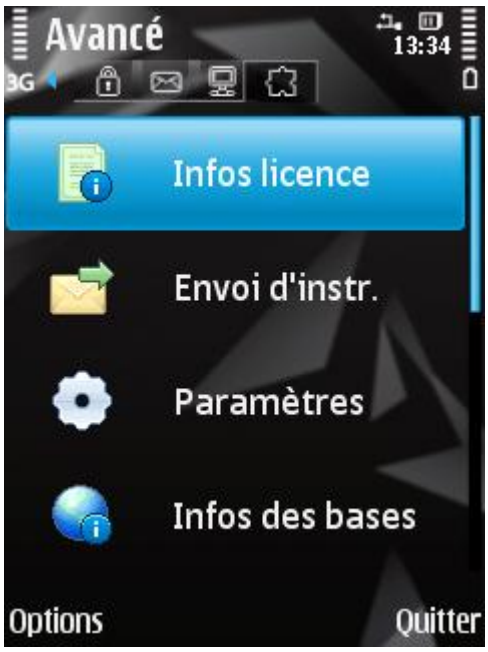

Figure 8 : Affichage des informations de licence

L'écran **Infos licence** s'ouvre.

SYNCHRONISATION AVEC LE SYSTEME D'ADMINISTRATION DISTANTE

Lors de la synchronisation, l'appareil reçois les paramètres de l'application, installés par l'administrateur. L'appareil envoie dans le système d'administration distante les rapports sur le fonctionnement des composants de l'application.

La synchronisation de l'appareil avec le système d'administration distante se fait automatiquement.

Vous pouvez toujours lancer la synchronisation à la main, si elle n'a pas été effectuée en mode automatique.

Il faut effectuer la synchronisation à la main, si dans les trois jours qui suivent l'installation de l'application la licence n'a pas été installée.

En fonction du type de système d'administration distante, sélectionné par l'administrateur pour la gestion de l'application, l'utilisateur peut être invité à saisir les paramètres de connexion au système d'administration distante pendant l'installation de l'application. Dans ce cas, les valeurs que l'utilisateur a saisi à la main peuvent être modifiées depuis l'application (cf. la rubrique «Modification des paramètres de synchronisation» à la page 23).

DANS CETTE SECTION

LANCEMENT DE LA SYNCHRONISATION A LA MAIN

- *Pour synchroniser l'appareil avec le système d'administration distante à la main,*

  sous l'onglet **Avancé**, sélectionnez **Synchronisation** (cf. ill. ci-après).

Figure 9: synchronisation à la main

Si l'utilisateur n'a pas été invité à saisir les paramètres de connexion au système d'administration distante, une fenêtre de confirmation de la synchronisation avec le système d'administration distante s'affichera sur l'écran. Autorisez la synchronisation en cliquant sur **Oui**. La connexion au système d'administration distante sera établie.

Si l'utilisateur a été invité à saisir les paramètres de connexion au système d'administration distante, le système affichera l'écran **Synchronisation**. Sélectionnez l'option **Lancement sync.**. Une fenêtre de confirmation de la synchronisation avec le système d'administration distante s'affichera sur l'écran. Autorisez la synchronisation en cliquant sur **Oui**. La connexion au système d'administration distante sera établie.

MODIFICATION DES PARAMETRES DE SYNCHRONISATION

Il est déconseillé de modifier les paramètres de connexion au système d'administration distante sans être guidé par l'administrateur.

Pour modifier les paramètres de connexion au système d'administration distante, procédez comme suit :

1. sous l'onglet **Avancé** sélectionnez l'option **Synchronisation**.

   L'écran **Synchronisation** s'ouvre.

2. Sélectionnez l'option **Param. de synchr.**.

   L'écran **Paramètres de synchr.** s'ouvrira. (voir figure suivante).

Figure 10: modification des paramètres de synchronisation

3. Modifiez les valeurs des paramètres suivants :
   - **Serveur** ;
   - **Port** ;
   - **Groupe**.
4. Appuyez sur **OK**.

PREMIERS PAS

Cette section reprend les informations sur la première utilisation de Kaspersky Endpoint Security 8 for Smartphone : la saisie du code secret de l'application, le lancement de l'application, la mise à jour des bases antivirus et l'analyse antivirus de l'appareil.

DANS CETTE SECTION

DEMARRAGE DU LOGICIEL

Pour installer Kaspersky Endpoint Security 8 for Smartphone, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KES 8**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Fonctions** → **Ouvrir**.

   L'écran **KES 8** s'ouvre.

4. Saisissez le code secret de l'application (cf. la rubrique «Saisissez le code secret» à la page 24), puis cliquez sur **OK**.

SAISIE DU CODE SECRET

Vous serez invité à saisir le code secret de l'application après son lancement. Le *code secret de l'application* permet d'éviter l'accès non autorisé aux paramètres de l'application. Vous pourrez modifier ultérieurement le code secret de l'application définit.

Kaspersky Endpoint Security 8 for Smartphone demande le code secret dans les cas suivants :

- Pour accéder à l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Géolocalisation, Contacts personnels ;
- Pour supprimer l'application.

Mémorisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Endpoint Security 8 for Smartphone, ni obtenir l'accès aux fichiers chiffrés, ni supprimer l'application.

Le code secret de l'application est composé de chiffres. Le code secret doit compter au moins quatre chiffres.

Pour saisir le code secret, procédez comme suit :

1. Après le lancement, saisissez dans le champ **Saisissez le nouveau code** les chiffres qui constituent votre code.
2. Tapez de nouveau ce code dans la zone **Confirmer**.

   La robustesse du code saisi est vérifiée automatiquement.
3. Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche et l'application demande une confirmation. Pour utiliser le code, cliquez sur **Oui**. Pour définir un nouveau code, cliquez sur **Non**.
4. Pour commencer à utiliser le programme, appuyez sur **OK**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez consulter les informations générales sur l'application Kaspersky Endpoint Security 8 for Smartphone et ses versions.

Pour consulter les informations relatives à l'application,

sur l'onglet **Avancé** sélectionnez l'option **Infos logiciel**.

INTERFACE DE L'APPLICATION

Cette section présente des informations sur les principaux composants de l'interface de Kaspersky Endpoint Security 8 for Smartphone.

DANS CETTE SECTION

ICONE DE PROTECTION

L'icône de la protection indique l'état de fonctionnement de l'application. Si l'icône est activée (en couleur), cela signifie que la protection est activée. Si l'icône est inactive (grise), cela indique que la protection est suspendue et que tous ses composants sont désactivés.

Par défaut, l'icône de la protection ne s'affiche pas à l'écran de l'appareil. Vous pouvez modifier les paramètres d'affichage de l'icône (cf. la rubrique «Affichage de la fenêtre d'état» à la page 92).

VOIR AUSSI

FENETRE D'ETAT DE LA PROTECTION

L'état des composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection.

Il existe trois états possibles pour chaque composant. Chacun d'entre eux est associé à une couleur, comme les feux de circulation. Le vert signifie que la protection de l'appareil est assurée au niveau requis. Le jaune et le rouge signalent des menaces de sécurité de nature différente. Les menaces groupent non seulement des bases antivirus dépassées, mais aussi des composants de la protection désactivés, des paramètres de base minimum de l'application etc.

La fenêtre de l'état de la protection est accessible directement après le lancement de l'application et reprend les informations suivantes :

- **Protection** : état de la protection en temps réel (cf. la rubrique «Protection en temps réel» à la page 29).

  L'icône verte de l'état indique que la protection est activée et assurée au niveau requis. Les bases antivirus de l'application sont à jour.

  L'icône jaune signale que la mise à jour des bases antivirus n'a plus eu lieu depuis quelques jours.

  L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil. Par exemple, la protection est désactivée. Il se peut que l'application n'ait pas été actualisée depuis plus de deux semaines.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. la rubrique «Filtrage de l'activité de réseau. Pare-feu» à la page 75).

  L'icône verte de l'état signifie que le composant est activé. Le niveau de protection du pare-feu a été sélectionné.

  Une icône rouge indique que le filtrage de l'activité de réseau n'a pas lieu.

- **Antivol** : état de la protection des données en cas de vol ou de perte de l'appareil (cf. la rubrique «Protection des données en cas de perte ou de vol de l'appareil» à la page 56).

L'icône verte signifie que les fonctions de l'Antivol dont le nom apparaît sous l'état du composant sont activées.

L'icône rouge indique que toutes les fonctions de l'Antivol sont désactivées.

- : état de la dissimulation des informations confidentielles (cf. la rubrique «Dissimulation des informations confidentielles» à la page 66).

  L'icône verte de l'état signifie que le composant est activé. Les données confidentielles sont masquées.

  L'icône jaune prévient l'utilisateur que le composant est désactivé. Les données personnelles sont visibles et peuvent être consultées.

- **Licence** : durée de validité de la licence (cf. la rubrique «Administration des licences» à la page 20).

  L'icône verte d'état indique que la licence est encore valide pendant plus de 14 jours.

  L'icône jaune indique que la licence est valide pour moins de 14 jours.

  L'icône rouge indique que la validité de la licence est écoulée.

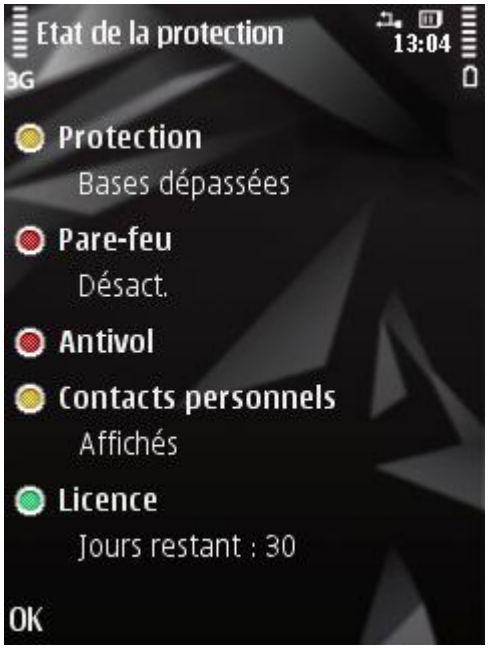

Figure 11: Fenêtre de l'état de la protection

Vous pouvez également ouvrir la fenêtre d'état de la protection en sélectionnant l'option **Fonctions → État de protection**.

Par défaut, la fenêtre de l'état de la protection s'affiche directement après le lancement de l'application. Vous pouvez modifier ses paramètres d'affichage (cf. la rubrique «Affichage de la fenêtre d'état» à la page 92).

VOIR AUSSI

ONGLETS DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et accessibles sur les onglets de l'application. Chaque onglet permet d'accéder aux paramètres du composant sélectionné et aux tâches de la protection.

Kaspersky Endpoint Security 8 for Smartphone propose les onglets suivants :

- **Anti-Virus :** protection du système de fichiers, analyse à la demande et mise à jour des bases antivirus de l'application.
- **Contacts personnels** : masque les informations confidentielles sur l'appareil.

- **Antivol** : blocage de l'appareil et suppression des informations en cas de vol ou de perte.
- **Chiffrement** : chiffre les données stockées sur l'appareil.
- **Anti-Spam** : filtrage des SMS et des appels entrants non sollicités.
- **Pare-feu** : contrôle l'activité de réseau.
- **Avancé** : paramètres généraux de l'application, lancement de la synchronisation de l'appareil avec le système d'administration distante, information sur l'application et sur la licence.

Par défaut, les onglets de l'application sont accessibles après la consultation de la fenêtre d'état de la protection (cf. la rubrique «Fenêtre d'état de la protection» à la page 26).

Vous pouvez naviguer entre les onglets d'une des manières suivantes :

- avec le joystick de l'appareil ou avec le stylet ;
- via le menu **Fonctions** → **Ouvrir onglet**.

MENU DE L'APPLICATION

Le menu de l'application permet de passer à l'exécution des principales actions. Le menu contient les options suivantes (cf. ill. ci-après) :

- **Sélection** : sélection de la fonction, de l'instruction ou du paramètre.
- **Ouvrir l'onglet** : passage à la sélection du composant de l'application.
- **Etat de protection** : ouverture de la fenêtre de l'état de la protection.
- **Aide** : affichage de l'aide contextuelle de Kaspersky Endpoint Security 8 for Smartphone.
- **Infos logiciel** : affichage de l'écran reprenant les informations sur l'application.
- **Quitter** : fin de l'utilisation de Kaspersky Endpoint Security 8 for Smartphone.

Figure 12: menu de l'application

➡ *Pour ouvrir le menu de l'application,*

sélectionnez **Fonctions**.

Pour naviguer dans le menu de l'application, utilisez le joystick de l'appareil ou le stylet.

PROTECTION DU SYSTEME DE FICHIERS

La rubrique présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. La section explique aussi comment activer / suspendre la protection et la configurer.

DANS CETTE SECTION

PRESENTATION DE LA PROTECTION

La protection est lancée en même temps que le système d'exploitation et se trouve en permanence dans la mémoire vive de l'appareil. La Protection surveille en arrière-plan les modifications introduites dans le système de fichiers et vérifie si celui-ci contient des objets malveillants. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. La protection analyse chaque fichier au moment où l'utilisateur essaie de l'accéder.
2. La protection analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparants aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.
3. Après l'analyse, la Protection agit en fonction de ses résultats :
   - quand du code malveillant est découvert dans le fichier, la protection le bloque et agit conformément aux paramètres définis ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Les informations sur les résultats du fonctionnement de la protection sont consignées dans le journal de l'application (cf. la rubrique «Journaux de l'application» à la page 88).

L'ACTIVATION / LA DESACTIVATION DE LA PROTECTION

Lorsque la protection est activée, toutes les actions exécutées dans le système sont placées sous un contrôle permanent.

La protection contre les virus et autres programmes malveillants usent les ressources de l'application. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

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

La désactivation de la Protection ne réagit pas sur l'exécution des tâches d'analyse sur les virus et des tâches de mises à jour des bases antivirus de l'application.

L'état actuel de la protection est repris sur l'onglet **Anti-Virus** à côté de l'option de menu **Protection**.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour désactiver la protection, procédez de la manière suivante :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Pour le paramètre **Mode de protection**, sélectionnez la valeur **Act.** (cf. ill. ci-après).

Figure 13 : activation de la protection

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

Pour désactiver la protection, procédez de la manière suivante :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Attribuez la valeur **Désact.** au paramètre **Mode de protection**.
3. Appuyez sur **Retour** pour enregistrer les modifications.

CONFIGURATION DE LA ZONE DE PROTECTION

Vous pouvez sélectionner les fichiers qui seront soumis à la recherche d'éventuels objets malveillants par Kaspersky Endpoint Security 8 for Smartphone pendant le fonctionnement du composant Protection.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour sélectionner le type d'objet à analyser, procédez comme suit :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Fichiers exécutables** : analyse uniquement les fichiers exécutables des applications (par exemple, fichiers au format EXE, SIS, MDL, APP).

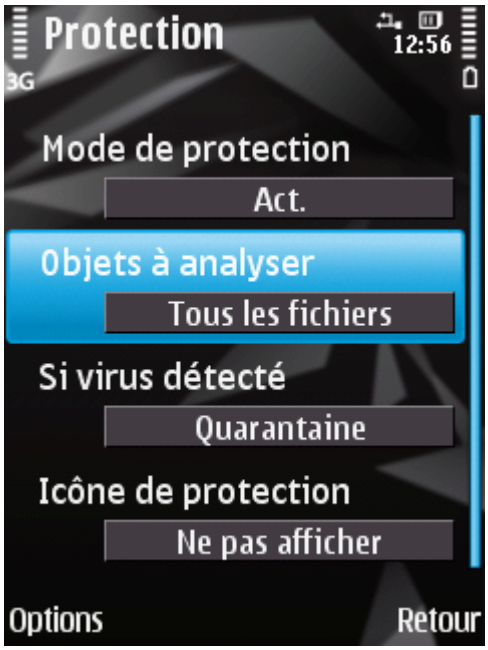

Figure 14: sélection des objets à analyser

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

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS MALVEILLANTS

Vous pouvez sélectionner l'action que Kaspersky Endpoint Security 8 for Smartphone exécute sur l'objet malveillant découvert.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

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

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Définissez l'action que l'application exécutera en cas de découverte d'un objet malveillant. Pour ce faire, attribuez une valeur au paramètre **Si virus détecté** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

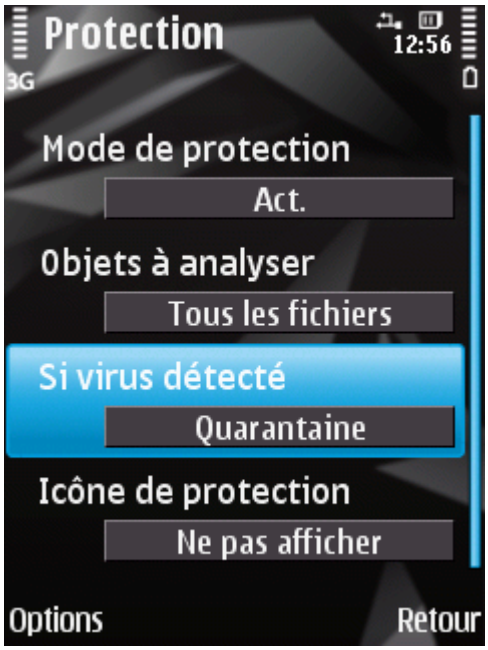

Figure 15: réponse de l'application sur l'objet malveillant

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

RESTAURATION DES PARAMETRES DE PROTECTION PAR DEFAUT

La première fois que vous accédez à l'application, ses paramètres installés par défaut sont les paramètres recommandés par les experts de Kaspersky Lab. Une fois l'application installée, tous les paramètres sont configurés par l'administrateur via le système d'administration distante. Si les paramètres de l'application peuvent être modifiés sur l'appareil, pendant la configuration de la protection vous pouvez toujours revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de la Protection définis par l'administrateur, procédez comme suit :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez **Fonctions** → **Restaurer**.

ANALYSE DE L'APPAREIL

Cette section présente les informations sur l'analyse de l'appareil à la demande, qui permet d'identifier et de neutraliser les menaces sur votre appareil. De plus, la section décrit comment lancer l'analyse de l'appareil, comment configurer l'analyse programmée du système de fichiers, comment sélectionner les fichiers à analyser et définir l'action de l'application en cas de détection d'une menace.

DANS CETTE SECTION

PRESENTATION DE L'ANALYSE DE L'APPAREIL

L'analyse à la demande de l'appareil permet d'identifier et de neutraliser les objets malveillants. Kaspersky Endpoint Security 8 for Smartphone permet de réaliser une analyse complète ou partielle de l'appareil. En cas d'analyse partielle l'application peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier spécifique (y compris les dossiers stockés sur la carte mémoire).

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Endpoint Security 8 for Smartphone analyse les fichiers, définis dans les paramètres de vérification (cf. la rubrique «Sélection du type d'objet à analyser» à la page 37).
2. Pendant la vérification, l'application analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparants aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Après l'analyse, Kaspersky Endpoint Security 8 for Smartphone agit en fonction de ses résultats :

   - · Quand un code malveillant est découvert dans un fichier, Kaspersky Endpoint Security 8 for Smartphone bloque le fichier et exécute l'action sélectionnée conformément aux paramètres définis (cf. la rubrique «Sélection des actions à appliquer sur des objets» à la page 38) ;
   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

L'analyse est lancée manuellement ou automatiquement selon un horaire prédéfini (cf. rubrique «Exécution de l'analyse programmée» à la page 36).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. la rubrique «Journaux de l'application» à la page 88).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer l'analyse complète ou partielle à la demande en mode manuel.

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

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

   L'écran **Analyse** s'ouvre.
2. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

- **Analyser tout** : analyse tout le système de fichiers de l'appareil. L'application analyse par défaut les fichiers stockés dans la mémoire de l'appareil et sur les cartes mémoire.
- **Analyser dossier** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte mémoire. En cas de sélection de l'option **Analyser dossier**, un écran reprenant le système de fichiers de l'appareil s'ouvre. Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick. Pour lancer l'analyse d'un dossier, sélectionnez le dossier souhaité, puis choisissez **Fonctions** →**Analyser**.
- **Analyser RAM** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.
- **Analyser msgs** : analyse les messages reçus via SMS, MMS ou Bluetooth.

Figure 16: sélection de la zone d'analyse

Une fois l'analyse lancée, la fenêtre du processus d'analyse affiche l'état actuel de la tâche : nombre d'objets analysés, chemin au fichier en cours d'analyse et indicateur des résultats de l'analyse en pour cent (cf. ill. ci-après).

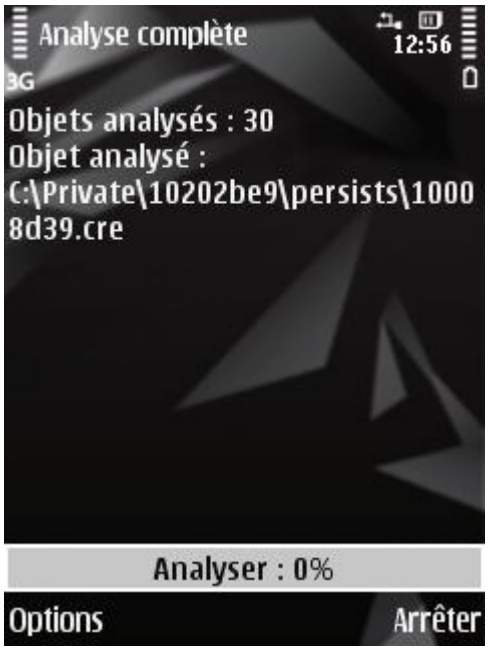

Figure 17: état de l'analyse de l'appareil

Si Kaspersky Endpoint Security 8 for Smartphone découvre un objet malveillant, il exécute l'action sélectionnée conformément aux paramètres d'analyse définis (cf. section Sélection des actions à appliquer sur les objets identifiés à la page 38).

Une fois l'analyse terminée, des statistiques générales reprenant les informations suivantes s'affichent :

- Le nombre d'objets analysés ;
- Le nombre de virus découverts, placés en quarantaine et supprimés ;
- Le nombre d'objets ignorés (par exemple, lorsque le fichier est bloqué par le système d'exploitation ou lorsque le fichier n'est pas un fichier exécutable alors que l'analyse porte uniquement sur les fichiers exécutables) ;
- L'heure de l'analyse.

Pour économiser la batterie, le rétroéclairage de l'écran est désactivé par défaut pendant l'analyse. Vous pouvez modifier les paramètres du rétroéclairage de l'écran (cf. la rubrique «Gestion du rétroéclairage» à la page 91).

EXECUTION DE L'ANALYSE PROGRAMMEE

Kaspersky Endpoint Security 8 for Smartphone permet de configurer le lancement automatique de l'analyse programmée du système de fichiers. L'analyse est exécutée en arrière-plan. Quand un objet malveillant est détecté, l'action définie par le paramètre d'analyse est exécutée sur cet objet.

Pour configurer le lancement automatique de l'analyse programmée et programmer le lancement de l'analyse, procédez comme suit :

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

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Programmation** s'ouvre.

3. Attribuez une valeur au paramètre **Analyse auto** (cf. ill. ci-après) :

   - **Désact.** : désactive le démarrage de l'analyse planifiée.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Indiquez le jour et l'heure de lancement de l'analyse. Pour ce faire, saisissez les valeurs des paramètres **Jour d'analyse** et **Heure d'analyse auto**.
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Indiquez l'heure de lancement de l'analyse dans le champ **Heure d'analyse auto**.

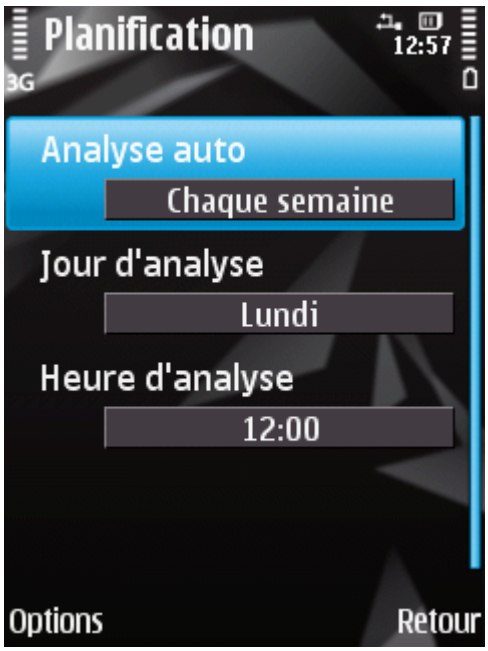

Figure 18: programmation du lancement de l'analyse complète

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

SELECTION DE TYPES DES FICHIERS A ANALYSER

Kaspersky Endpoint Security 8 for Smartphone analyse par défaut tous les fichiers stockés sur l'appareil et sur la carte mémoire. Pour réduire la durée de l'analyse, vous pouvez sélectionner des types d'objets à analyser, c'est-à-dire définir quels formats de fichiers seront soumis à la recherche d'un éventuel code malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour sélectionner un objet à analyser, procédez comme suit :

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

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Fichiers exécutables** : analyse uniquement les fichiers exécutables des applications au format EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

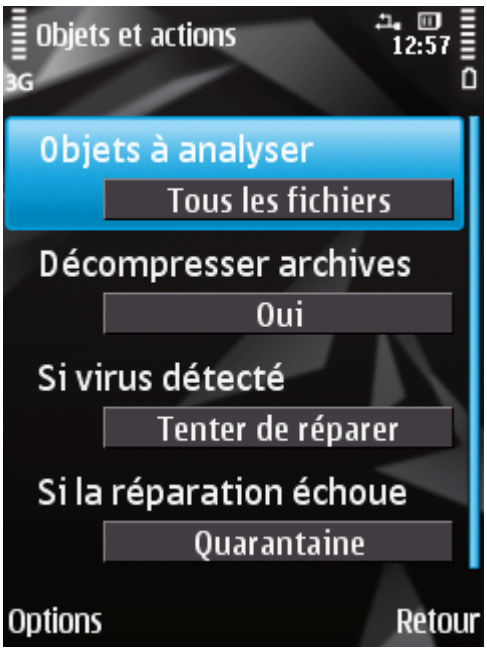

Figure 19: sélection du type de fichiers à analyser

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

CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. L'application permet d'analyser les archives des formats suivants: ZIP, JAR, JAD, SIS et SISX. Pendant l'analyse, les archives sont décompressées, ce qui peut réduire sensiblement la vitesse de l'Analyse à la demande.

Vous pouvez activer / désactiver l'analyse du contenu des archives pendant l'Analyse à la demande pour détecter des codes malveillants éventuels.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour activer l'analyse du contenu des archives, procédez comme suit :

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

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Attribuez au paramètre **Décompresser archives** la valeur **Oui** (cf. ill. ci-dessous).

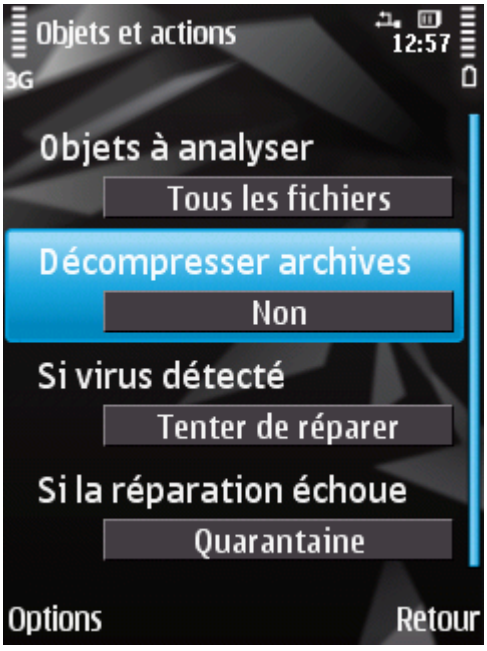

Figure 20: configuration de l'analyse de fichiers compressés

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

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Quand un code malveillant est découvert dans un fichier, Kaspersky Endpoint Security 8 for Smartphone bloque l'action et exécute l'action sélectionnée conformément aux paramètres définis.

Vous pouvez modifier l'action que l'application exécutera sur l'objet malveillant découvert.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour définir l'action que l'application exécutera sur l'objet malveillant découvert, procédez comme suit :

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

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Définissez l'action à exécuter sur les objets malveillants. Pour ce faire, attribuez une valeur au paramètre **Si virus détecté** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants détectés.
   - **Interroger** : confirme l'action auprès de l'utilisateur. En cas de découverte d'une menace, une fenêtre de confirmation de l'action s'ouvre.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application.
   - **Tenter de réparer** : répare les objets malveillants. Si la réparation est impossible, l'action définie pour le paramètre **Si la réparation échoue** est exécutée.

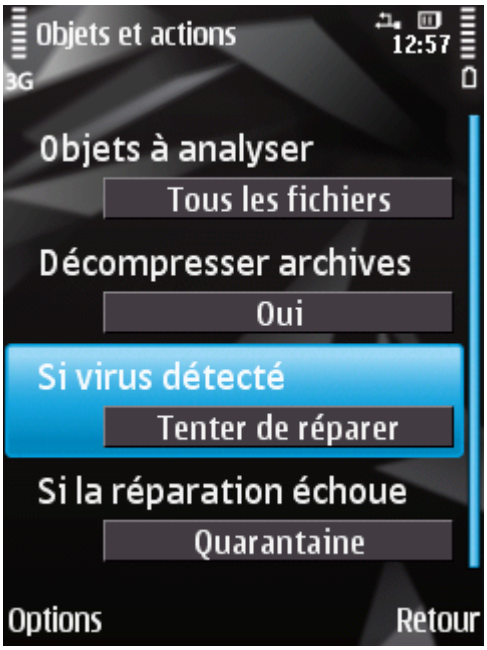

Figure 21 : sélection de l'action appliquée à un objet malveillant

4. Si vous avez choisi l'option **Tenter de réparer**, définissez la deuxième action de l'application qui sera exécutée lorsque la réparation de l'objet ne sera pas possible. Pour ce faire, attribuez une valeur au paramètre **Si la réparation échoue** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Interroger** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.
   - **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application.

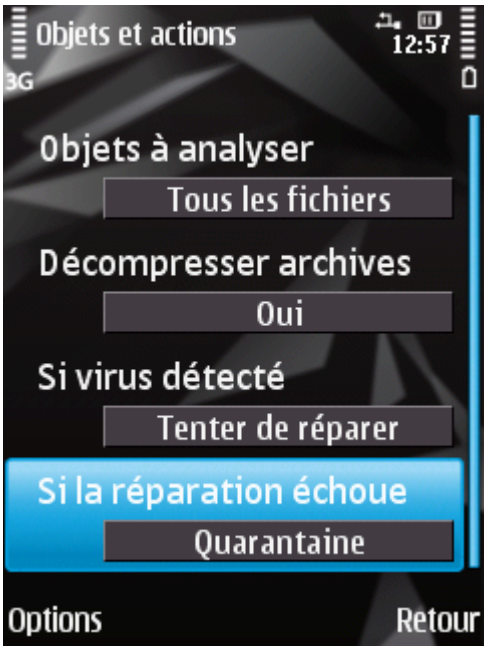

Figure 22: sélection de l'action à exécuter sur les objets malveillants si la réparation est impossible

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

RESTAURATION DES PARAMETRES D'ANALYSE DE L'APPLICATION PAR DEFAUT

La première fois que vous accédez à l'application, ses paramètres installés par défaut sont les paramètres recommandés par les experts de Kaspersky Lab. Une fois l'application installée, tous les paramètres sont configurés par l'administrateur via le système d'administration distante. Si les paramètres de l'application peuvent être modifiés sur l'appareil, pendant la configuration de l'analyse de l'appareil vous pouvez toujours revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de l'analyse définis par l'administrateur, procédez comme suit :

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

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Sélectionnez **Fonctions** → **Restaurer**.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La rubrique présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. De plus, elle décrit comment consulter, restaurer ou supprimer les objets malveillants stockés dans le dossier.

DANS CETTE SECTION

À PROPOS DE LA QUARANTAINE

L'application place les objets malveillants détectés en *quarantaine* dans un dossier spécial isolé pendant l'analyse de l'appareil ou pendant le fonctionnement de la protection. Les objets malveillants 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.

Vous pouvez consulter les fichiers placés en quarantaine, les supprimer ou les restaurer.

AFFICHAGE DES OBJETS EN QUARANTAINE

Vous pouvez consulter les objets qui sont dans la quarantaine. Le nom complet de l'objet et la date à laquelle il a été découvert sont repris.

Vous pouvez également consulter des informations complémentaires sur l'objet infecté sélectionné : chemin d'accès à l'objet sur l'appareil avant sa mise en quarantaine et nom de la menace.

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

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

L'écran **Quarantaine** s'ouvre et présente la liste des objets contenus (cf. ill. ci-après).

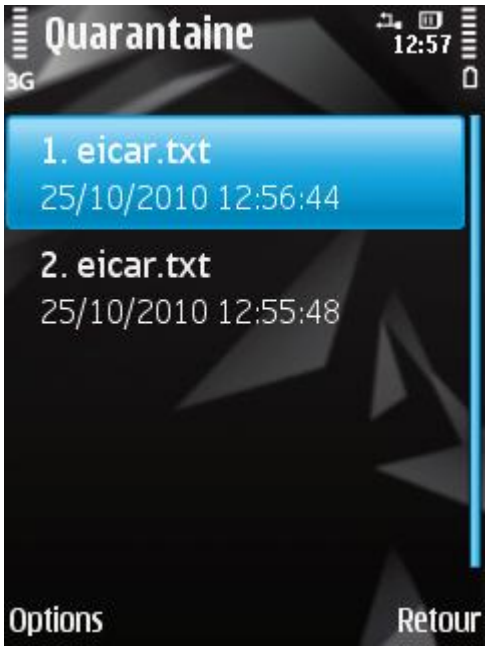

Figure 23 : liste des objets en quarantaine

- *Pour consulter les informations relatives à l'objet sélectionné,*

  choisissez le menu **Fonctions** → **Détails**.

  L'écran propose les informations suivantes sur le fichier : chemin d'accès au fichier où l'application l'a trouvé sur l'appareil et nom de la menace.

RESTAURATION D'OBJETS DE LA QUARANTAINE

Si vous êtes convaincu que l'objet découvert ne constitue pas une menace pour l'appareil, vous pouvez le restaurer depuis la quarantaine. L'objet restauré sera remis dans on répertoire d'origine.

- *Pour restaurer un objet depuis la quarantaine, procédez comme suit :*

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

     L'écran **Quarantaine** s'ouvre.

  2. Sélectionnez l'objet que vous souhaitez restaurer, puis choisissez l'option **Fonctions** → **Restaurer**.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

Il est possible de supprimer un objet placé en quarantaine ou l'ensemble des objets placés en quarantaine.

Pour supprimer un objet de la quarantaine, procédez comme suit :

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

   L'écran **Quarantaine** s'ouvre.

2. Sélectionnez l'objet que vous souhaitez supprimer, puis sélectionnez **Fonctions** → **Supprimer**.

L'objet sélectionné sera supprimé.

Pour supprimer tous les objets de la quarantaine, procédez comme suit :

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

   L'écran **Quarantaine** s'ouvre.

2. Sélectionnez **Fonctions** → **Supprimer tout**.

Tous les objets en quarantaine seront éliminés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

Cette section présente les informations sur Anti-Spam qui interdit la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche que vous avez créées. De plus, la section décrit comment sélectionner le mode de filtrage Anti-Spam des appels et des SMS entrants, comment configurer les paramètres avancés de filtrage pour les appels et les SMS entrants et comment créer la liste noire et la liste blanche.

DANS CETTE SECTION

A PROPOS DE L'ANTI-SPAM

L'Anti-Spam empêche la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche que vous avez créées.

Les listes contiennent les enregistrements. L'enregistrement dans chaque liste contient les informations suivantes :

- Numéro de téléphone que l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche.
- Type d'événement que l'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche. Types d'informations représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, Anti-Spam va refuser les SMS avec cette expression clé et accepter les autres SMS sans cette expression clé. S'il s'agit des numéros de la liste blanche, Anti-Spam va accepter les SMS avec cette expression clé et refuser les SMS sans cette expression clé.

Anti-Spam filtre les appels et les SMS entrants selon le mode sélectionné (cf. la rubrique «Présentation des modes de l'Anti-Spam» à la page 44). Anti-Spam analyse selon le mode sélectionné chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non (spam). L'analyse se termine dès que l'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section « Journaux du logiciel» à la page 88).

PRESENTATION DES MODES DE L'ANTI-SPAM

Le mode détermine les règles utilisées par Anti-Spam pour filtrer les appels et les SMS entrants.

Les modes de fonctionnement Anti-Spam disponibles :

- **Les deux listes** : accepte les appels et les SMS en provenance des numéros de la liste blanche et interdit ceux qui proviennent des numéros de la liste noire. Après la conversation ou la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Anti-Spam vous invitera à ajouter ce numéro sur une des listes.
- **Liste noire** : accepte tous les appels et les SMS, sauf ceux qui proviennent des numéros de la liste noire.

- **Liste blanche** : accepte uniquement les appels et les SMS en provenance des numéros de la liste blanche.
- **Désactivé** : accepte tous les appels et les SMS entrants.

Vous pouvez modifier le mode de l'Anti-Spam (cf. la rubrique "Modification du mode de l'Anti-Spam» à la page 45). Le mode actuel de l'Anti-Spam s'affiche sur l'onglet **Anti-Spam** à côté de l'option **Mode**.

MODIFICATION DU MODE DE L'ANTI-SPAM

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions** → **Modifier**.

Pour modifier le mode de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Filtre app. / SMS** sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une valeur pour le paramètre **Mode Anti-Spam** (cf. ill. ci-dessous).

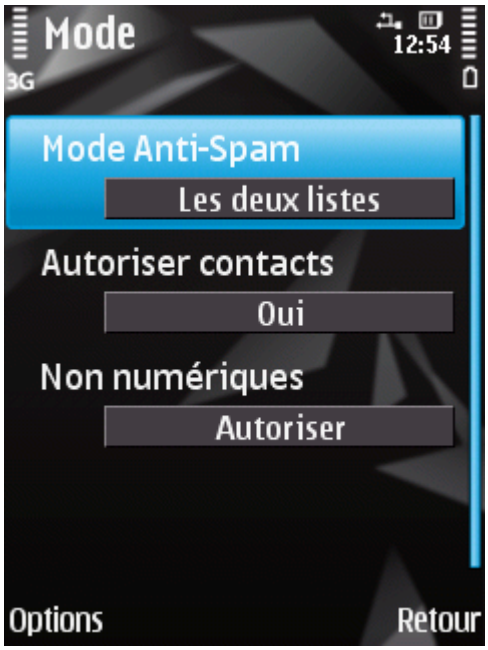

Figure 24: modification du mode de l'Anti-Spam

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

COMPOSITION DE LA LISTE NOIRE

Les enregistrements de la liste noire contiennent les numéros de téléphone interdits dont les appels et les SMS sont refusés par Anti-Spam. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS non sollicités (spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

L'Anti-Spam bloquera uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste noire. L'Anti-Spam acceptera les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste noire.

Il est impossible d'ajouter le même numéro de téléphone avec les mêmes critères de filtrage sur la liste noire et sur la liste blanche.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section « Journaux du logiciel» à la page 88).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Endpoint Security 8 for Smartphone vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions** → **Modifier**.

Pour ajouter une entrée dans la liste noire de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Fonctions** → **Ajouter** (cf. ill. ci-après).

Figure 25: ajout d'un enregistrement à la liste noire

3. Définissez les paramètres suivants (cf. ill. ci-après) :

   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS :** bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Depuis le numéro** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*» et "?» (où "*» représente n'importe quel nombre de caractères et "?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? dans la liste noire. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS. Le paramètre est accessible si la valeur **SMS seulement** a été attribuée au paramètre **Bloquer tout**.

   Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cette entrée, vide.

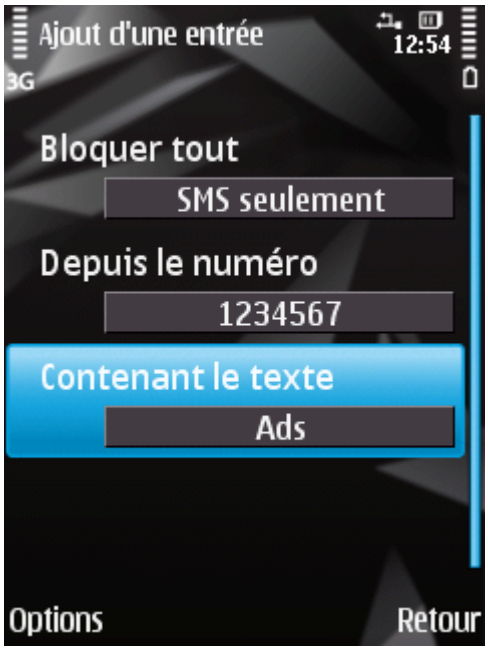

Figure 26 : paramètres d'une entrée de la liste noire

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez modifier les valeurs de tous les paramètres de l'entrée de la liste noire.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions → Modifier**.

Pour modifier un enregistrement de la liste noire de l'Anti-Spam, exécutez les opérations suivantes :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis sélectionnez **Fonctions → Modifier**.

3. Modifiez les paramètres requis de l'enregistrement :
   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS :** bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Depuis le numéro** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*» et "?» (où "*» représente n'importe quel nombre de caractères et "?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? dans la liste noire. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS. Le paramètre est accessible si la valeur **SMS seulement** a été attribuée au paramètre **Bloquer tout**.

   Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Contenant le texte** de cette entrée, vide.
4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer ce numéro de la liste noire. De plus, vous pouvez purger la liste noire de l'Anti-Spam en supprimant tous les enregistrements qu'elle contient.

Pour supprimer un enregistrement de la liste noire de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.
2. Sélectionnez dans la liste l'enregistrement qu'il faut supprimer, puis choisissez **Fonctions** → **Supprimer**.

Pour purger la liste noire de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste noire**.
2. L'écran **Liste noire** s'ouvre.
3. Sélectionnez **Fonctions** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Les enregistrements de la Liste blanche contiennent les numéros de téléphone autorisés dont les appels et les SMS sont acceptés par Anti-Spam. Chacun de ces enregistrements contient les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

Anti-Spam accepte uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste blanche. Anti-Spam refuse les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste blanche.

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Endpoint Security 8 for Smartphone vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions** → **Modifier**.

Pour ajouter un enregistrement à la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez l'option **Fonctions** → **Ajouter** (cf. ill. ci-après).

Figure 27: ajout d'un enregistrement à la liste blanche

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :
   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste blanche :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seulement :** autorise uniquement les appels entrants.
     - **SMS seulement** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone dont les informations entrantes sont acceptées par Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*» et "?» (où "*» représente n'importe quel nombre de caractères et "?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro. Le paramètre est accessible si la valeur **SMS seulement** a été attribuée au paramètre **Autoriser tout**.

   Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cette entrée, vide.

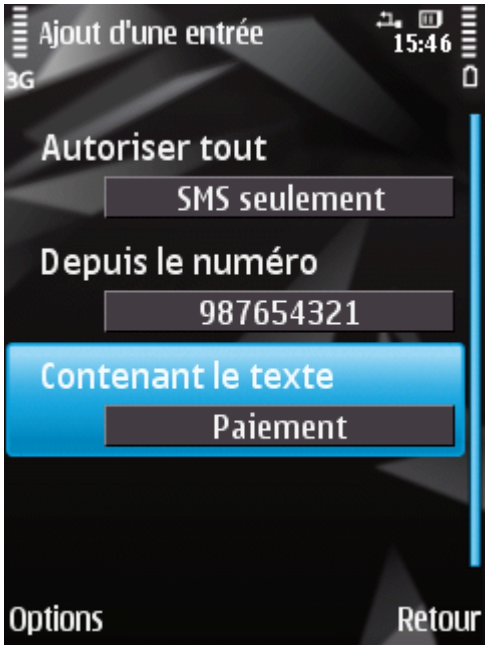

Figure 28 : paramètres d'une entrée de la liste blanche

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions** → **Modifier**.

Pour modifier un enregistrement de la liste blanche de l'Anti-Spam, exécutez les opérations suivantes :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Fonctions** → **Modifier**.
3. Modifier les paramètres requis de l'enregistrement :
   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste blanche :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seulement :** autorise uniquement les appels entrants.
     - **SMS seulement** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone dont les informations entrantes sont acceptées par Anti-Spam. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+» et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*» et "?» (où "*» représente n'importe quel nombre de caractères et "?», n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro. Le paramètre est accessible si la valeur **SMS seulement** a été attribuée au paramètre **Autoriser tout**.

   Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cette entrée, vide.
4. Appuyez sur **Retour** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer une seule entrée de la liste blanche ou purger la liste.

Pour supprimer un enregistrement de la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
2. Sélectionnez dans la liste l'enregistrement qu'il faut supprimer, puis choisissez **Fonctions** → **Supprimer**.

Pour purger la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
2. Sélectionnez **Fonctions** → **Supprimer tout**.

REACTION AUX SMS ET AUX APPELS EN PROVENANCE DES NUMEROS QUI NE FIGURENT PAS DANS LES CONTACTS

Si le mode **Les deux listes** ou **Liste blanche** a été sélectionné pour Anti-Spam, alors vous pouvez définir également la réaction de l'Anti-Spam en cas de réception d'un SMS ou d'un appel en provenance d'un numéro qui ne figure pas dans les Contacts. Anti-Spam permet d'élargir la liste blanche en y introduisant les numéros des contacts.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour définir la réaction de l'Anti-Spam face aux numéros ne figurant pas dans le répertoire téléphonique de l'appareil, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Autoriser contacts** (cf. ill. ci-après) :

   - Pour que l'Anti-Spam considère un numéro du répertoire téléphonique comme un ajout à la liste blanche, sélectionnez la valeur **Oui** ;
   - Pour que l'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini de l'Anti-Spam, choisissez la valeur **Non**.

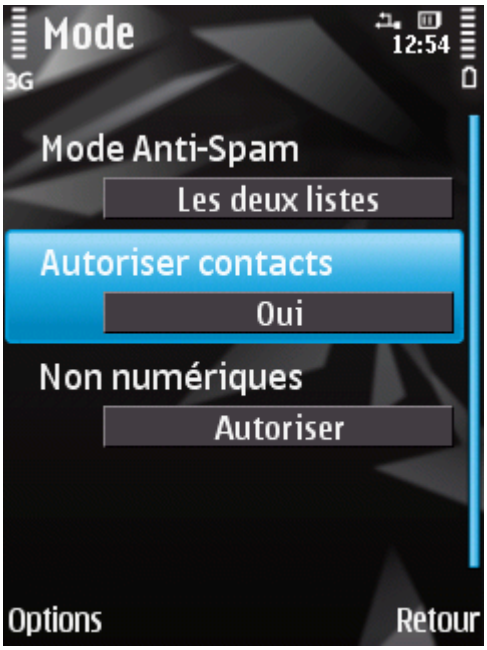

Figure 29: réaction de l'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

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

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode choisi pour Anti-Spam est **Les deux listes** ou **Liste noire**, vous pouvez enrichir la liste noire en y ajoutant tous les numéros sans chiffres (composés de lettres). Alors Anti-Spam pourra bloquer les SMS en provenance de numéros sans chiffres.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Afin de définir les réactions de l'Anti-Spam face aux SMS en provenance de numéros sans chiffres, procédez comme suit :

1. Sous l'onglet **Filtre app. / SMS** sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Choisissez la valeur du paramètre **Non numériques** (cf. ill. ci-après) :

   - Pour que l'Anti-Spam supprime automatiquement les SMS en provenance de numéros sans chiffres, sélectionnez l'option **Bloquer** ;
   - Pour que l'Anti-Spam filtre les SMS en provenance de numéros sans chiffres uniquement sur la base du mode sélectionné pour Anti-Spam, sélectionnez la valeur **Autoriser**.

Figure 30: Sélection des actions exécutées par Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres

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

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Si le mode choisi est **Les deux listes**, Anti-Spam analyse les SMS entrants sur la base des listes noire et blanche.

Après la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Anti-Spam vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez choisir une des actions suivantes à exécuter sur le SMS (cf. ill. ci-après) :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, sélectionnez **Fonctions** → **Ajouter à la liste noire**.
- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste blanche, sélectionnez **Fonctions** → **Ajouter à la liste blanche**.
- Pour accepter le SMS sans consigner le numéro de téléphone de l'appelant dans aucune des listes, appuyez sur **Ignorer**.

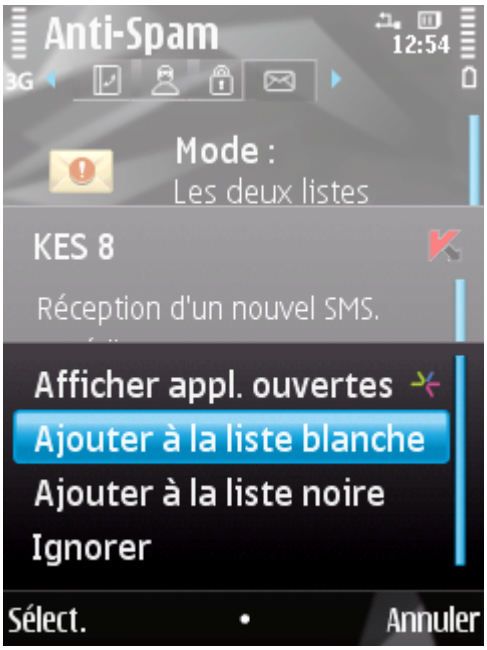

Figure 31: notification de l'Anti-Spam sur le SMS reçu

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page 88).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Si le mode choisi est **Les deux listes**, Anti-Spam analyse les appels entrants sur la base des listes noire et blanche. Après la réception d'un appel en provenance du numéro qui ne figure sur aucune des listes, Anti-Spam vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez choisir une des actions suivantes pour le numéro de l'appelant (cf. ill. ci-après) :

- Pour ajouter le numéro de téléphone de l'appelant à la liste noire, sélectionnez **Fonctions** → **Ajouter à la liste noire**.
- Pour ajouter le numéro de téléphone de l'appelant à la liste blanche, sélectionnez **Fonctions** → **Ajouter à la liste blanche**.
- Choisissez **Ignorer** si vous ne souhaitez pas consigner le numéro de l'appelant dans aucune des listes.

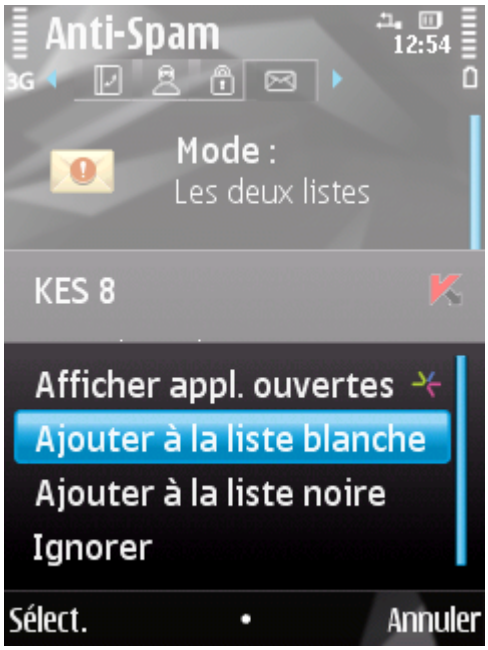

Figure 32: notification de l'Anti-Spam sur l'appel reçu

Les informations sur les appels bloqués sont consignées dans le journal de l'application (cf. la rubrique “Journaux de l'application» à la page 88).

PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL

La section présente le composant Antivol, qui protège les données stockées sur l'appareil mobile contre l'accès non autorisé en cas de perte ou de vol, toute en facilitant sa recherche.

Elle explique également comment activer/désactiver les fonctions de l'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la fonction Antivol depuis un autre appareil mobile.

DANS CETTE SECTION

À PROPOS DU COMPOSANT ANTIVOL

Antivol protège les données sur votre appareil mobile contre l'accès non autorisé.

Antivol dispose des fonctions suivantes :

- **Verrouillage** permet de verrouiller l'appareil à distance et de définir le texte qui apparaîtra à l'écran de l'appareil bloqué.
- **Suppression** permet de supprimer à distance les données personnelles de l'utilisateur (entrées dans les Contacts, SMS, galerie, calendrier, journaux, paramètres de connexion à Internet), ainsi que les données de la carte mémoire et les dossiers de la liste à supprimer.
- **SIM-Surveillance** permet de garder le numéro de téléphone en cas de remplacement de la carte SIM et de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte. Le message avec le nouveau numéro de téléphone est envoyé vers le numéro de téléphone et/ou l'adresse de la messagerie électronique que vous avez spécifié.
- **Géolocalisation** : permet de déterminer les coordonnées de l'appareil. Le message avec les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis le SMS spécial, ainsi que à l'adresse de la messagerie électronique.

Kaspersky Endpoint Security 8 for Smartphone permet de lancer à distance la fonction Antivol via l'envoi d'une instruction SMS (cf. la rubrique “Lancement à distance de la fonction Antivol» à la page 65) depuis un autre appareil mobile.

Pour exécuter les fonctions Antivol à distance, il faudra utiliser le code secret de l'application qui a été défini à la première exécution de Kaspersky Endpoint Security 8 for Smartphone.

L'état du fonctionnement actuel de chaque fonction apparaît sur l'onglet **Antivol** à côté du nom de la fonction.

Les informations sur le fonctionnement du composant sont conservées dans le journal du composant (cf. la rubrique “Journaux de l'application» à la page 88).

VERROUILLAGE DE L'APPAREIL

Après la réception d'une instruction SMS spéciale, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données qu'il renferme. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Cette fonction ne verrouille pas l'appareil mais active uniquement la possibilité de le verrouiller à distance.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Fonctions** → **Modifier**.

Pour activer la fonction de verrouillage, procédez comme suit :

1. Sélectionnez **Antivol**, choisissez l'option **Verrouillage**.

   L'écran **Verrouillage** s'ouvre.

2. Attribuez la valeur **Act.** pour le paramètre **Mode de verrouillage**.

3. Pour afficher un message à l'écran de l'appareil verrouillé, choisissez le paramètre **Texte lors du verr.** et remplissez le champ **Entrez le texte** (cf. ill. ci-après). Un texte standard est utilisé par défaut. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

   Pour ne pas afficher le message, choisissez le paramètre **Texte lors du verr.**, puis supprimer le contenu du champ **Entrez le texte** et appuyez sur **OK**.

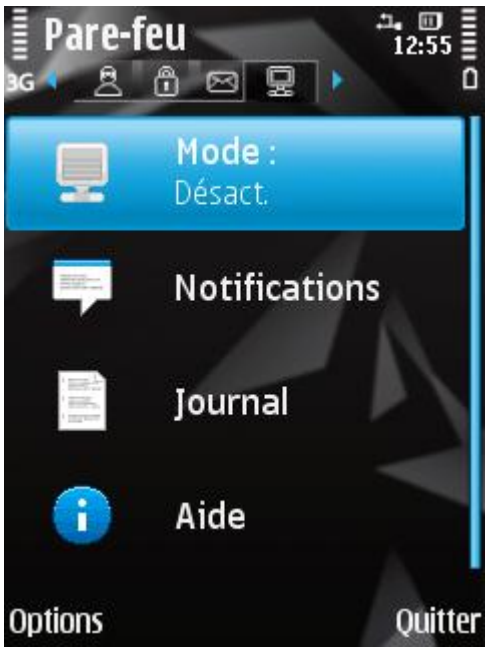

Figure 33: paramètres de la fonction Verrouillage

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

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

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction **Envoi d'une instruction**. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour verrouiller l'appareil à distance, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sélectionnez **Avancé** et choisissez l'option **Envoi instr.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Commencer**.
3. Saisissez l'instruction **Verrouillage** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 34: verrouillage à distance de l'appareil

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

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

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction SMS spéciale, la fonction Suppression permet de supprimer les informations suivantes sur l'appareil :

- données personnelles de l'utilisateur (entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet) ;
- données sur la carte mémoire ;
- Les données dans le dossier **C:\Data** et dans d'autres dossiers dans la liste **Dossiers à supprimer**.

Cette fonction ne supprime pas les données enregistrées sur l'appareil mais active la possibilité de le faire après la réception de l'instruction SMS.

Pour activer la fonction de suppression des données, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppre des donn.**

   L'écran **Suppression de données** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Choisissez l'option **Mode Suppr. des données** et choisissez la valeur **Act.** (cf. ill. ci-dessous).

4. Sélectionnez les données qui seront supprimées dès la réception de l'instruction SMS spéciale par l'appareil :

   - Pour supprimer les données personnelles, pour le paramètre **Supprimer contacts pers.** attribuez la valeur **Oui** ;
   - Pour supprimer les fichiers du dossier **C:\Data** et de la liste **Dossiers à supprimer**, attribuez au paramètre **Supprimer les dossiers** la valeur **Oui**.

Figure 35: paramètres de la fonction de suppression de données

5. Appuyez sur **Retour** pour enregistrer les modifications.
6. Passez à la constitution de la liste **Dossiers à supprimer** (cf. rubrique “**Composition de la liste des objets à supprimer**» à la page 61).

La suppression des données personnelles de l'appareil peut être réalisée d'une des manières suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour supprimer à distance les informations de l'appareil, il est conseillé d'utiliser une méthode sûre en exécutant la fonction Envoi d'une instruction. Dans ce cas, le code secret est envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Env. instr.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Commencer**.
3. Choisissez l'instruction **Suppression** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 36: lancement à distance de la fonction Suppression

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour rédiger un SMS avec les fonctions standards de messagerie SMS de votre téléphone,

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

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception de l'instruction SMS spéciale.

Pour que l'Antivol supprime les dossiers de la liste après la réception de l'instruction SMS spéciale, assurez-vous que sous l'onglet **Antivol** dans l'option **Mode** pour le paramètre **Supprimer supr. dossiers** la valeur **Oui** est attribuée.

La liste des dossiers à supprimer peut contenir les dossiers, ajoutés par l'administrateur. Ces dossiers ne peuvent pas être supprimés de la liste.

Pour ajouter un dossier à la liste des dossiers à supprimer, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppre des donn.**

   L'écran **Suppression de données** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Sélectionnez **Fonctions** → **Ajouter** (cf. ill. ci-après).

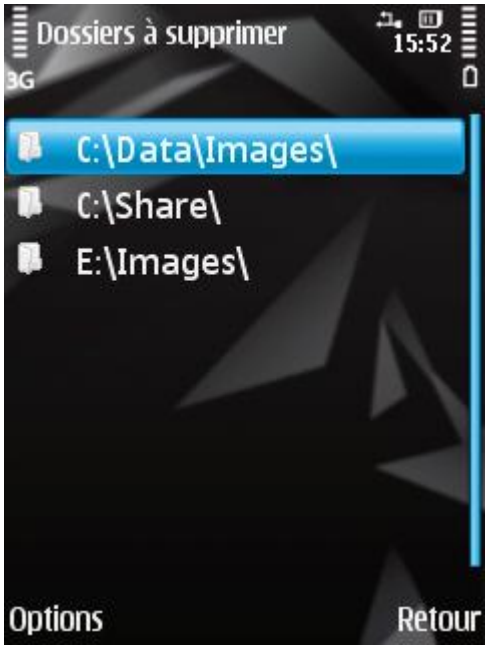

Figure 37: ajout d'un dossier

4. Sélectionnez le dossier requis dans l'arborescence, puis cliquez sur **Fonctions** → **Sélection**.

   Le dossier sera ajouté à la liste.

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

Pour supprimer un dossier de la liste, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppre des donn.**

   L'écran **Suppression de données** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Sélectionnez un dossier dans la liste, puis choisissez l'option **Fonctions** → **Supprimer**.

4. Pour confirmer la suppression, cliquez sur **Oui**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

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

Pour activer la fonction SIM-Surveillance et contrôler le remplacement de la carte SIM sur l'appareil, procédez comme suit :

1. Sélectionnez **Antivol**, choisissez l'option **SIM-Surveillance**.

   L'écran **SIM-Surveillance** s'ouvre.

2. Choisissez l'option **Mode de SIM-Surveillance** et attribuez la valeur **Act**.

3. Configurez les paramètres suivants de SIM-Surveillance (cf. ill. ci-après) :

   - **Msgs. à l'adresse électronique**. Pour recevoir un message électronique indiquant le nouveau numéro de téléphone de votre appareil, saisissez ici une adresse électronique.
   - **SMS au numéro**. Pour recevoir automatiquement un SMS indiquant le nouveau numéro de téléphone de votre appareil, saisissez le numéro de téléphone vers lequel le message sera envoyé. Ces numéros peuvent commencer par un chiffre ou par le signe “+» et ne peuvent contenir que des chiffres.
   - **Verrouiller l'appareil**. Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, sélectionnez la valeur **Oui**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret de l'application.
   - **Texte en cas de verrouillage**. Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Entrez le texte**. Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

Figure 38: paramètres de la fonction SIM-Surveillance

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

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Géolocalisation détermine les coordonnées géographiques de l'appareil et les envoie par SMS ou courrier électronique à l'appareil à l'origine de la demande.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. Le récepteur GPS est activé automatiquement après la réception de l'instruction SMS spéciale. Si l'appareil se trouve dans une zone couverte par satellite, la fonction Géolocalisation reçoit et envoie les coordonnées de l'appareil. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver sont lancées par la Géolocalisation à intervalles réguliers.

Pour activer la fonction Géolocalisation, procédez comme suit :

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

   L'écran **Géolocalisation** s'ouvre.

2. Attribuez la valeur **Act**. au paramètre **Mode de localisation**.

3. Pour le paramètre **Msgs. à l'adresse électronique**, saisissez l'adresse électronique à laquelle les coordonnées géographiques de l'appareil seront envoyées (cf. ill. ci-après).

Figure 39: paramètres de la fonction Géolocalisation

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

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

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS, et l'application enverra les coordonnées de l'appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra un SMS et l'application enverra les coordonnées de l'appareil.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile de l'autre appareil nomade.

Pour déterminer les coordonnées de l'appareil, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, le code secret sera envoyé en mode crypté.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Env. instr.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Choisissez l'instruction **Géolocalisation**, puis cliquez sur **Suivant** (cf. ill. ci-après).

Figure 40 : détermination des coordonnées de l'appareil

3. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
4. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour rédiger un SMS avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à l'appareil un SMS contenant le texte `find:<code>` (où `<code>` est le code secret de l'application 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.

Le SMS contenant les coordonnées géographiques de l'appareil sera envoyé au numéro de téléphone à l'origine de l'envoi de l'instruction SMS et à une adresse électronique, si celle-ci a été définie dans les paramètres de la fonction Localisation.

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

L'application permet d'envoyer une instruction spéciale par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Endpoint Security 8 for Smartphone. L'instruction SMS est envoyée sous forme d'un SMS crypté qui contient le code secret de l'application, installée sur l'autre appareil. La réception de l'instruction passera inaperçue sur l'autre appareil.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Pour envoyer une instruction SMS vers un autre appareil, procédez comme suit :

1. Sélectionnez **Avancé** et choisissez l'option **Envoi instr.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.
2. Cliquez sur **Commencer**.
3. Sélectionnez une des fonctions proposées à lancer à distance (cf. ill. ci-après) :
   - Verrouillage (cf. la rubrique “Verrouillage de l'appareil» à la page 57).
   - Suppression des données (cf. la rubrique Suppression de données personnelles à la page 59).
   - Géolocalisation.
   - Contacts personnels (cf. rubrique “Présentation des modes de Contacts personnels» à la page 66).

Figure 41: lancement à distance de la fonction Antivol

La fonction doit être activée sur l'appareil qui reçoit l'instruction par SMS.

4. Cliquez sur **Suivant**.
5. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
6. Entrez le code secret spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

La section présente le composant Contacts personnels, qui permet de dissimuler les données confidentielles de l'utilisateur.

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

Les Contacts personnels dissimulent les informations confidentielles sur la base de la Liste de contacts créée qui reprend les numéros confidentiels. Les Contacts personnels masquent les entrées dans les Contacts, les SMS entrants, sortants et brouillons, ainsi que les enregistrements dans le journal des appels pour des numéros confidentiels. Les Contacts personnels bloquent le signal de réception du SMS et le masquent dans la liste des SMS reçus. Les Contacts personnels interdisent les appels entrants d'un numéro confidentiel et l'écran n'indiquera rien au sujet de ces appels. Dans ce cas, la personne qui appelle entendra la tonalité “occupé». Il faut désactiver la dissimulation des informations confidentielles pour pouvoir consulter les appels et les SMS entrants pour la période d'activation de cette fonction. A la réactivation de la dissimulation les informations ne seront pas affichées.

Vous pouvez activer la fonction de dissimulation des informations confidentielles depuis Kaspersky Endpoint Security 8 for Smartphone ou à distance depuis un autre appareil mobile. Vous ne pouvez désactiver la fonction de dissimulation des informations confidentielles que depuis l'application.

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. la rubrique “Journaux de l'application» à la page 88).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

Vous pouvez gérer le mode de fonctionnement de Contacts personnels. Le mode détermine si la fonction de dissimulation des données confidentielles est activée ou non.

Les modes suivants sont prévus pour Contacts personnels :

- **Afficher** : les données confidentielles sont affichées. Les paramètres de Contacts personnels peuvent être modifiés.
- **Masquer** : les données confidentielles sont masquées. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique (cf. rubrique “Activation automatique de la dissimulation des informations confidentielles» à la page 68) de la dissimulation des données personnelles ou son activation à distance depuis un autre appareil (cf. rubrique “Activation de la dissimulation des informations confidentielles à distance» à la page 69).

L'état actuel de dissimulation des informations confidentielles figure sur l'onglet **Contacts personnels** à côté de l'option de menu **Mode**.

La modification du mode de fonctionnement du composant Contacts personnels peut prendre un certain temps.

MODIFICATION DU MODE DE CONTACTS PERSONNELS

Le mode du composant Contacts personnels peut être modifié d'une des manières suivantes :

- Depuis l'interface de l'application ;
- A l'aide d'un code secret lorsque l'appareil est en mode d'attente actif.

Pour modifier le mode de Contacts personnels, procédez comme suit :

1. Sélectionnez **Contacts personnels**, sélectionnez l'option **Mode**.

   L'écran **Mode Contacts personnels.**

2. Attribuez une valeur au paramètre **Mode Contacts pers.** (cf. ill. ci-après).

Figure 42: modification du mode de Contacts personnels

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

Pour modifier le mode du composant Contacts personnels à l'aide du code secret lorsque l'appareil est en mode d'attente actif,

saisissez dans l'ordre ***code secret#**.

Une notification apparaîtra à l'écran pour indiquer la modification du mode du composant Contacts personnels.

ACTIVATION AUTOMATIQUE DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES

Vous pouvez configurer l'activation automatique de la dissimulation des informations confidentielles après un certain temps. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Désactivez la dissimulation des informations confidentielles avant de modifier les paramètres des Contacts personnels.

Pour activer automatiquement la dissimulation des informations confidentielles à l'issue d'une période déterminée, procédez comme suit :

1. Sélectionnez **Contacts personnels**, sélectionnez l'option **Mode**.

   L'écran **Mode Contacts personnels.**

2. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, sélectionnez une des valeurs proposées pour le paramètre **Masquer automatiq.**. (cf. ill. ci-après).

   - **Sans délai**.
   - **1 minute**.
   - **5 minutes**.
   - **15 minutes**.
   - **1 heure**.
   - **Désact.**

Figure 43: paramètres de lancement automatique de Contacts personnels

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

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Endpoint Security 8 for Smartphone permet d'activer à distance la dissimulation des informations confidentielles depuis un autre appareil mobile. Pour ce faire, il faut d'abord activer sur votre appareil la fonction **Masquer par instruction SMS**.

Pour autoriser l'activation à distance de la dissimulation des informations confidentielles, procédez comme suit :

1. Sélectionnez **Contacts personnels**, sélectionnez l'option **Mode**.

   L'écran **Mode Contacts personnels.**

2. Sélectionnez pour le paramètre **Masquer à l'instr. SMS** la valeur **Oui** (cf. ill. ci-après).

Figure 44 : paramètres d'activation à distance du composant Contacts personnels

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

Vous pouvez activer à distance la dissimulation des informations confidentielles d'une des méthodes suivantes :

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8 for Smartphone) pour rédiger et envoyer un SMS vers votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS qui déclenchera la dissimulation des informations confidentielles. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra un SMS qui déclenchera la dissimulation des informations confidentielles.

Le coût du SMS envoyé est celui de l'opérateur de téléphonie mobile du portable utilisé pour envoyer ce SMS.

- *Pour activer à distance la dissimulation des informations confidentielles à l'aide d'une instruction spéciale envoyée par SMS, procédez comme suit :*

  1. Sélectionnez **Avancé** et choisissez l'option **Envoi instr.**.

     L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

  2. Cliquez sur **Commencer**.
  3. Choisissez l'instruction **Contacts personnels** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 45 : lancement à distance de Contacts personnels

  4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
  5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Quand l'appareil aura reçu l'instruction par SMS, la dissimulation des informations confidentielles sera activée automatiquement.

- *Pour activer à distance la dissimulation des informations confidentielles avec les fonctions standards de messagerie SMS de votre téléphone,*

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

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

La liste des contacts contient les numéros confidentiels dont les informations et les événements sont masqués par le composant Contacts personnels. La liste des numéros peut être enrichie manuellement, via importation depuis les contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter un numéro dans la Liste des contacts manuellement (par exemple, +12345678) ou l'importer depuis les Contacts ou depuis la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

Pour ajouter un enregistrement à la Liste de contacts, procédez comme suit :

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.

2. Exécutez une des opérations suivantes (cf. ill. ci-après) :

   - Pour ajouter un numéro manuellement, sélectionnez **Fonctions** → **Ajouter** → **Numéro**. Dans l'écran **Numéro** qui s'ouvre, remplissez le champ **Saisissez le numéro**. Après avoir saisi, cliquez sur **OK**.
   - Pour ajouter un numéro depuis les Contacts, sélectionnez **Fonctions** → **Ajouter** → **Contacts**. Dans l'écran **Contacts** qui apparaît, sélectionnez le contact requis dans le répertoire via le menu **Fonctions** → **Sélectionner**. Après avoir saisi, cliquez sur **OK**.
   - Pour ajouter un numéro enregistré sur la carte SIM, sélectionnez **Fonctions** → **Ajouter** → **Contact de la carte SIM**. Sur l'écran **Contacts SIM** qui apparaît, choisissez le numéro requis dans la liste des numéros de la carte SIM à l'aide de l'option **Fonctions** → **Sélectionner**. Après avoir saisi, cliquez sur **OK**.

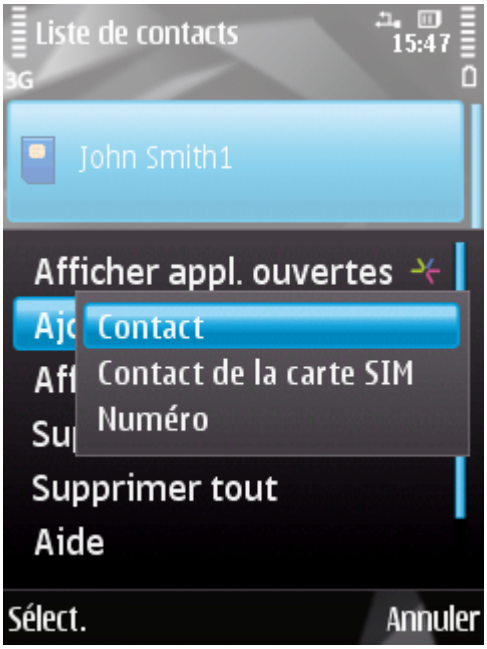

Figure 46: ajout d'un enregistrement à la liste des contacts protégés

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

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Seuls les numéros qui ont été saisis manuellement dans la Liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans le répertoire ou dans la liste des numéros de la carte SIM.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

- *Pour modifier le numéro dans la Liste de contacts, procédez comme suit :*

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.
2. Sélectionnez le numéro à modifier dans la Liste de contacts, puis choisissez **Fonctions** → **Modifier**.

   Le numéro de téléphone du contact sélectionné apparaît à l'écran.
3. Modifiez les données dans le champ **Saisissez le numéro**.
4. Une fois la modification terminée, cliquez sur **OK**.

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro ou effacer tout le contenu de la Liste de contacts.

Avant de rédiger la liste des contacts, désactivez la dissimulation des informations confidentielles.

- *Pour supprimer un numéro de la Liste de contacts, procédez comme suit :*

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.
2. Sélectionnez le numéro dans la liste, puis choisissez **Fonctions** → **Supprimer**.
3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

- *Pour purger la Liste de contacts, procédez comme suit :*

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.
2. Sélectionnez **Fonctions** → **Supprimer tout**.
3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

Les Contacts personnels permettent de dissimuler les informations suivantes pour les numéros de la Liste des contacts : contacts, SMS, entrées du journal des appels, SMS et appels entrants. Vous pouvez choisir les informations et les événements que la fonction Contacts personnels va dissimuler pour les numéros confidentiels.

Désactivez la dissimulation des informations confidentielles avant de modifier les paramètres des Contacts personnels.

- *Pour choisir les informations et les événements à masquer pour les numéros confidentiels, procédez comme suit :*

1. Sélectionnez sous l'onglet **Contacts personnels** l'option **Obj. à masquer.**

   L'écran **Objets à masquer** apparaît.

2. Sélectionnez les informations et les événements qui seront masqués pour les numéros confidentiels. Attribuez à chaque paramètre souhaité la valeur **Masquer** via l'option **Fonctions** → **Modifier**. Il est possible de masquer les informations suivantes et les événements (cf. ill. ci-après) :

   - **Contacts :** masque toutes les informations relatives aux numéros confidentiels.
   - **Messages** : masque les SMS dans les dossiers **Boîte de réception**, **Messages envoyés**, **Brouillons** pour les numéros confidentiels.
   - **Enreg. des appels** : accepte les appels en provenance des numéros confidentiels sans identifier le numéro de l'appelant et sans afficher les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).
   - **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité “occupé»). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.
   - **SMS entrants** : masquer la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.

Figure 47: sélection des informations et des événements à dissimuler

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

FILTRAGE DE L'ACTIVITE DE RESEAU PARE-FEU

La section présente le composant Pare-feu, qui contrôle les connexions de réseau sur votre appareil. De plus, elle décrit comment activer / désactiver le composant Pare-feu et comment sélectionner le mode de fonctionnement requis.

DANS CETTE SECTION

À PROPOS DU PARE-FEU

Le Pare-feu contrôle les connexions de réseau sur votre appareil selon le mode sélectionné. Pare-feu permet de désigner les connexions autorisées (par exemple, pour synchroniser avec le Serveur d'administration), ainsi que les connexions interdites (par exemple, pour l'utilisation d'Internet et le téléchargement de fichiers).

Pare-feu permet de configurer les notifications des connexions bloquées (cf. la rubrique “Notifications sur le blocage des connexions» à la page 76).

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section “Journaux de l'application» à la page 88).

PRESENTATION DES NIVEAUX DE SECURITE DE PARE-FEU

Vous pouvez sélectionner le mode Pare-feu pour définir les connexions autorisées et interdites. Les modes de fonctionnement Pare-feu disponibles :

- **Désact.** : autorisation de la moindre activité de réseau.
- **Les connexions entrantes sont interdites** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Les connexions sortantes des protocoles SSH, HTTP, HTTPS, IMAP, SMTP, POP3 sont autorisées** : toutes les connexions entrantes sont bloquées. La réception du courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Bloq. tout** : bloque toute activité de réseau, sauf la mise à jour des bases antivirus et la connexion au système d'administration distante.

Vous pouvez modifier le mode Pare-feu (cf. la rubrique “Sélection du mode Pare-feu» à la page 75). Le mode actuel est indiqué sur l'onglet **Pare-feu** à côté de l'option de menu **Mode**.

SELECTION DU MODE PARE-FEU

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour sélectionner le mode du Pare-feu, procédez comme suit :

1. Sélectionnez **Pare-feu**, choisissez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez un des modes Pare-feu proposés. Pour ce faire, mettez le curseur sur le nom du mode requis (cf. ill. ci-après).

Figure 48: sélection du mode Pare-feu

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

NOTIFICATIONS SUR LE BLOCAGE DES CONNEXIONS

Pare-feu bloque toutes les connexions interdites sur la base du mode sélectionné (cf. la rubrique “Sélection du mode Pare-feu» à la page 75). Pour que Pare-feu vous signale les connexions bloquées sur l'appareil, configurez la réception des notifications Pare-feu.

Pour configurer la réception des notifications sur le blocage, procédez comme suit :

1. Sous l'onglet **Pare-feu**, choisissez l'option **Notification**.
2. Sélectionnez pour le paramètre **En cas de verrouillage** une des valeurs suivantes (cf. ill. ci-après) :
   - **Avertir** : active la réception des notifications. Le Pare-feu signale le blocage de la connexion.
   - **Ne pas avertir** : désactive la réception des notifications. Le Pare-feu ne signale pas le blocage de la connexion.

Figure 49: configuration des notifications du Pare-feu

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

CHIFFREMENT DES DONNEES PERSONNELLES

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. De plus, la section décrit comment chiffrer et déchiffrer les dossiers sélectionnées.

DANS CETTE SECTION

À PROPOS DU CHIFFREMENT

La fonction Chiffrement chiffre les informations de la liste des dossiers à chiffrer que vous avez créée. La fonction Chiffrement repose sur une fonction de cryptage intégrée au système d'exploitation de votre appareil. La fonction Chiffrement permet de chiffrer tous les dossiers, sauf les dossiers système. Vous pouvez sélectionner pour le chiffrement des dossiers stockés dans la mémoire de l'appareil ou sur une carte mémoire. Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret défini à la première exécution de l'application.

Avant de lancer des fichiers exe exécutables depuis le dossier chiffré, il faut déchiffrer ce dossier. Pour ce faire, saisissez le code secret de l'application.

Pour pouvoir accéder aux informations chiffrées, il faut saisir le code secret de l'application. Vous pouvez définir la période (cf. rubrique “Interdiction d'accès aux données chiffrées» à la page 80), à l'issue de laquelle l'interdiction d'accès aux dossiers chiffrés sera activée et un code secret de l'application sera nécessaire pour accéder à ces dossiers. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Les informations sur le fonctionnement du Chiffrement sont consignées dans le journal de l'application (cf. la rubrique “Journaux de l'application» à la page 88).

CHIFFREMENT DES DONNEES

Le Chiffrement permet de chiffrer un nombre quelconque de dossiers non systèmes qui se trouvent dans la mémoire de l'appareil ou sur une carte mémoire.

La liste de tous les dossiers chiffrés ou déchiffrés antérieurement est accessible dans l'écran **Chiffrement** via l'option **Liste des dossiers**.

Vous pouvez également chiffrer un dossier ou chiffrer directement tous les dossiers qui se trouvent dans la liste des dossiers.

- *Pour ajouter un dossier à la liste des dossiers à chiffrer pour le chiffrer, procédez comme suit :*

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Fonctions** → **Ajouter** (cf. ill. ci-après).

Figure 50: chiffrement des données

   L'écran reprenant l'arborescence du système de fichiers de l'appareil apparaît.

3. Sélectionnez le dossier à chiffrer, puis choisissez **Fonctions** → **Chiffrer**.

   Pour vous déplacer dans le système de fichiers, utilisez le stylet 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.

4. Appuyez sur **OK**.

   Le dossier chiffré sera ajouté à la liste des dossiers.

Pour le dossier chiffré, le menu **Fonction** remplace l'option **Chiffrer** par l'option **Déchiffrer**.

Après le chiffrement, les donnée sont déchiffrées et chiffrées automatiquement lorsque vous manipulez des données depuis un dossier chiffré, lorsque vous les extrayez du dossier chiffré ou y placer de nouvelles données.

- *Pour chiffrer directement tous les dossiers de la liste, procédez comme suit :*

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Fonctions** → **Actions compl.** → **Tout chiffrer**.

3. Appuyez sur **OK**.

DECHIFFREMENT DES DONNEES

Il est possible de déchiffrer les données préalablement chiffrées (cf. la rubrique “Chiffrement de données» à la page 78) Vous pouvez déchiffrer un seul dossier ou tous les dossiers que vous avez chiffrés sur l'appareil.

Si la liste des dossiers à chiffrer contient les dossiers chiffrés par l'administrateur, vous ne pourrez ni les déchiffrer ni les supprimer de la liste.

Pour déchiffrer un dossier chiffré, procédez comme suit :

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** apparaît. Il reprend la liste de tous les dossiers chiffrés et déchiffrés antérieurement.

2. Sélectionnez dans la liste le dossier que vous voulez déchiffrer, puis choisissez **Fonctions** → **Déchiffrer** (cf. ill. ci-après).

Figure 51: déchiffrement des données

3. Cliquez sur **OK** à la fin du déchiffrement des données.

Une fois que la procédure de déchiffrement sera terminée, l'option **Déchiffrer** du menu **Fonctions** du dossier sélectionné deviendra **Chiffre**r. Vous pouvez à nouveau chiffrer un dossier (cf. la rubrique “Chiffrement de données» à la page 78).

Pour déchiffrer directement tous les dossiers de la liste des dossiers à déchiffrer, procédez comme suit :

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Fonctions** → **Actions compl.** → **Tout déchiffrer**.

3. Appuyez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le Chiffrement permet de définir la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. La fonction est activée au moment de passage de l'appareil en mode d'économie de l'énergie. Pour utiliser les informations chiffrées, il faudra saisir le code secret de l'application.

De plus, vous pouvez immédiatement bloquer l'accès aux dossiers chiffrés après leur ouverture et activer la saisie du code secret de l'application.

Pour interdire l'accès à un dossier chiffré à l'issue d'une période déterminée, procédez comme suit :

1. Sous l'onglet **Chiffrement**, sélectionnez l'option **Interdiction de l'accès**.

   L'écran **Interdiction de l'accès** s'ouvre

2. Déterminez la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. Pour ce faire, choisissez une des valeurs proposées (cf. ill. ci-après) :

   - **Sans délai** ;
   - **1 minute** ;
   - **5 minutes** ;
   - **15 minutes** ;
   - **1 heure**.

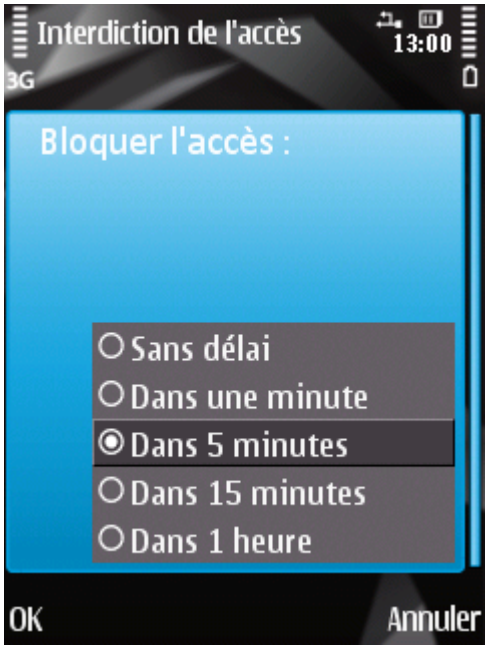

Figure 52: blocage de l'accès aux données chiffrées

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

Pour bloquer l'accès aux dossiers chiffrés immédiatement après leur ouverture et activer la saisie du code secret de l'application,

cliquez simultanément sur les boutons “0» et “1» du périphérique. L'interdiction de l'accès aux informations chiffrées sera activée.

MISE A JOUR DES BASES DU PROGRAMME

La section présente la mise à jour des bases anti-virus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

DANS CETTE SECTION

À PROPOS DE LA MISE A JOUR DES BASES

La recherche d'application malveillante s'opère à l'aide d'une base antivirus qui contient les descriptions de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus.

Il est conseillé d'actualiser régulièrement les bases de l'application. Si plus de 15 jours se sont écoulés depuis la dernière mise à jour, les bases de l'application sont considérées comme étant fortement dépassées. Dans ce cas, la fiabilité de la protection sera réduite.

Kaspersky Endpoint Security 8 for Smartphone effectue la mise à jour des bases de l'application depuis les serveurs de mises à jour définis par l'administrateur.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur Internet.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. Les bases de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial.
2. Kaspersky Endpoint Security 8 for Smartphone exécute une des opérations suivantes :
   - Si les bases de l'application que vous utilisez sont à jour, la mise à jour sera annulée. Un message d'information s'affichera à l'écran.
   - Si les bases installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

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

Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres de la connexion à Internet ne sont pas définis automatiquement, configurez-les (cf. la rubrique “Configuration des paramètres de connexion à Internet» à la page 86).

Vous pouvez lancer la tâche de mise à jour manuellement à n'importe quel moment, si l'appareil n'est pas occupé par l'exécution d'autres tâches ou programmer l'exécution de la mise à jour.

Si vous êtes en itinérance, vous pouvez désactiver la mise à jour des bases antivirus de Kaspersky Endpoint Security 8 for Smartphone pour réduire les dépenses.

Les informations détaillées sur les bases utilisées sont accessibles sous l'onglet **Avancé** dans l'option du menu **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. la rubrique “Journaux de l'application» à la page 88).

AFFICHAGE D'INFORMATIONS SUR LES BASES

Vous pouvez consulter les informations sur les bases antivirus de l'application installées : dernier lancement de la mise à jour, date de publication des bases, taille des bases et nombre d'entrées dans les bases.

- *Pour consulter les informations sur les bases antivirus existantes,*

  sous l'onglet **Avancé**, choisissez l'option **Infos des bases** (cf. ill. ci-après).

Figure 53: informations relatives aux bases antivirus de l'application installées

LANCEMENT MANUEL DE LA MISE A JOUR

Vous pouvez lancer manuellement la mise à jour des bases antivirus de l'application.

Pour lancer la mise à jour manuelle des bases antivirus de l'application, procédez comme suit :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Sélectionnez l'option **Mise à jour** (cf. ill. ci-après).

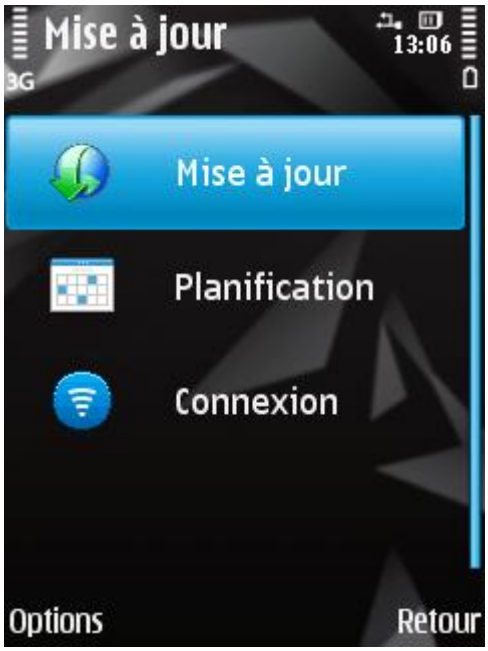

Figure 54: lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur, défini par l'administrateur. Les informations sur la mise à jour apparaissent à l'écran.

LANCEMENT PROGRAMME DE LA MISE A JOUR

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Pour votre confort, vous pouvez configurer l'exécution automatique de la mise à jour des bases antivirus et de programmer son exécution.

Pour exécuter une mise à jour programmée, veillez à ce que l'appareil soit allumé au moment de la mise à jour.

Vous pouvez également configurer les paramètres de mise à jour automatique si vous vous trouvez par exemple en itinérance (cf. la rubrique « Mise à jour en itinérance» à la page 85).

Pour configurer le lancement programmé de la mise à jour, procédez comme suit :

1. Sélectionnez **Anti-Virus**, choisissez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Programmation** s'ouvre.

3. Attribuez au paramètre **Mise à jour auto** une des valeurs proposées (cf. ill. ci-après) :

   - **Désact.** : la mise à jour programmée des bases de l'application n'aura pas lieu.
   - **Chaque semaine** : actualise les bases de l'application une fois par semaine. Sélectionnez une des valeurs pour les paramètres **Jour de mise à jour** et **Heure de mise à jour**.
   - **Chaque jour** : actualise les bases chaque jour. Saisissez la valeur pour le paramètre **Heure de mise à jour**.

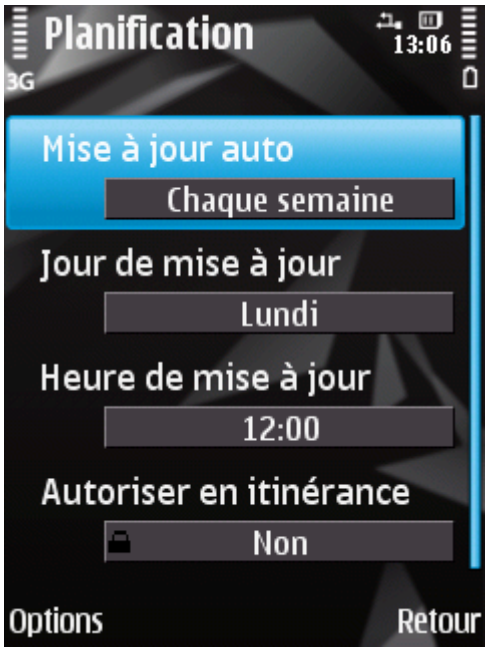

Figure 55: programmation de la mise à jour automatique

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

MISE A JOUR EN ITINERANCE

Vous pouvez contrôler le lancement de la mise à jour programmée en itinérance, vu que le trafic Internet est payé au tarif d'itinérance.

Si le lancement de la mise à jour programmée est interdit en itinérance, le lancement manuel de la mise à jour sera accessible en mode normal.

Pour désactiver la mise à jour programmée en cas d'itinérance, procédez comme suit :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Programmation** s'ouvre.

3. Attribuez la valeur **Non** au paramètre **Autoriser en itinérance** (cf. ill. ci-après).

Figure 56: programmation du lancement de la mise à jour en itinérance

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

CONFIGURATION DES PARAMETRES DE CONNEXION A INTERNET

Pour se connecter à Internet, Kaspersky Endpoint Security 8 for Smartphone utilise un point d'accès défini par défaut.

Les paramètres du point d'accès sont communiqués par le fournisseur.

Si Kaspersky Endpoint Security 8 for Smartphone n'a pas défini les paramètres de connexion automatiquement, configurez-les à la main.

Pour configurer les paramètres de connexion à Internet, procédez comme suit :

1. Sélectionnez **Anti-Virus**, choisissez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

2. Sélectionnez l'option **Connexion**.

3. Sélectionnez le point d'accès utilisé pour vous connecter au serveur de mise à jour. Pour ce faire, sélectionnez la valeur du paramètre **Point d'accès**, puis appuyez sur **OK** (cf. ill. ci-après) :

   La liste reprendra tous les points d'accès définis sur l'appareil nomade.

Figure 57: paramètres de connexion à Internet

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

JOURNAUX DU LOGICIEL

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus)

DANS CETTE SECTION

À PROPOS DES JOURNAUX

Les journaux reprennent les rapports sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Endpoint Security 8 for Smartphone. Il existe un journal des événements pour chaque composant. Vous pouvez sélectionner et consulter le rapport sur les événements survenus pendant l'utilisation du composant. Les entrées du rapport sont classées dans l'ordre chronologique décroissant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

Pour consulter les enregistrements dans le journal du composant, procédez comme suit :

1. Sous l'onglet du composant nécessaire, choisissez l'option **Journal**.

   Le journal du composant sélectionné s'ouvre (cf. ill. ci-après).

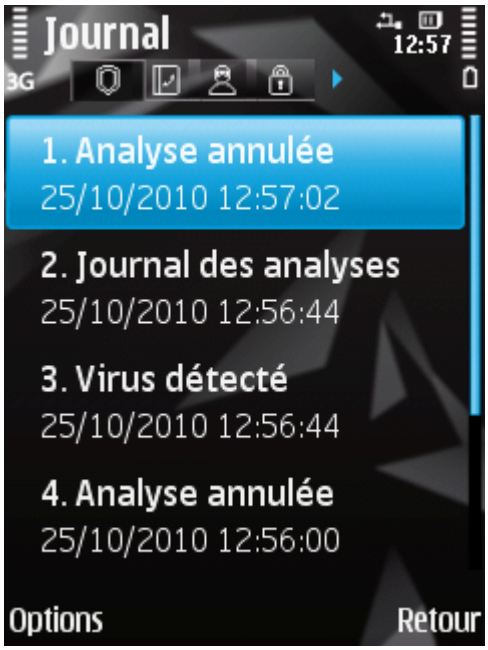

Figure 58: journal du composant sélectionné

2. Naviguez dans le journal à l'aide du stylet ou des boutons du joystick : **Haut** et **Bas** pour consulter les événements dans le journal en cours et **Gauche** et **Droite** pour consulter les événements dans les journaux des autres composants.

Pour afficher des informations détaillées sur les enregistrements du journal,

sélectionnez l'enregistrement nécessaire, puis sélectionnez **Fonctions** → **Afficher les informations**.

SUPPRESSION D'EVENEMENTS DANS LES JOURNAUX

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Endpoint Security 8 for Smartphone seront supprimées.

Pour supprimer tous les événements des journaux, procédez comme suit :

1. Sous l'onglet de n'importe quel composant, sélectionnez l'option **Journal**.

   L'écran **Journal Anti-Virus** s'ouvre

2. Sélectionnez **Fonctions** → **Effacer le journal**.

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section présente les informations sur les fonctionnalités complémentaires de Kaspersky Endpoint Security 8 for Smartphone : comment modifier le code secret, comment administrer les notifications sonores de l'application et le rétroéclairage, et comment activer / désactiver l'affichage des astuces, de l'icône de protection ou de la fenêtre d'état de la protection.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret de l'application, défini à la première exécution de l'application.

Pour changer le code secret de l'application, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.
2. Choisissez le paramètre **Modifier le code**.
3. Saisissez le code actuel dans le champ **Saisissez le code**, puis cliquez sur **OK**.
4. Saisissez le nouveau code dans le champ **Saisissez le nouveau code**, puis cliquez sur **OK**.
5. Saisissez à nouveau le code dans le champ **Confirmation du code**, puis cliquez sur **OK**.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Endpoint Security 8 for Smartphone affiche par défaut des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Endpoint Security 8 for Smartphone.

Pour configurer l'affichage des astuces, procédez comme suit :

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

   L'écran **Configuration** s'ouvre.
2. Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :
   - **Afficher** : affiche l'astuce avant de configurer les paramètres de la fonction sélectionnée ;
   - **Masquer** : aucune astuce n'est affichée.
3. Appuyez sur **Retour** pour enregistrer les modifications.

ADMINISTRATION DES NOTIFICATIONS SONORES

De différents événements résultent de l'exécution de l'application, par exemple, découverte d'un objet infecté ou d'un virus, expiration de la licence. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Kaspersky Endpoint Security 8 for Smartphone active la notification sonore uniquement selon le mode défini de l'appareil.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour administrer les notifications sonores de l'application, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Notifications sonores** (cf. ill. ci-après) :

   - **Toujours** : utilise les notifications sonores quel que soit le profil sélectionné de l'utilisateur ;
   - **Selon le mode** : utilise les notifications sonores en fonction du mode sélectionné pour l'appareil ;
   - **Désactiver** : n'utilise pas les notifications sonores.

Figure 59 : contrôle des notifications sonores

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

CONTROLE DU RETRO ECLAIRAGE

Quand l'application exécute une tâche de protection, l'appareil puise dans son autonomie. Pour épargner la batterie durant l'exécution des tâches, l'application permet de désactiver automatiquement le rétroéclairage de l'écran.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour configurer le rétroéclairage de l'écran pendant l'exécution des tâches, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Rétro éclairage** (cf. ill. ci-après) :

   - **Selon le mode** : utilise le rétroéclairage en fonction du mode sélectionné pour l'appareil ;
   - **Activé** : utilise toujours le rétroéclairage de l'écran.

Figure60 : contrôle du rétroéclairage

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

AFFICHAGE DE LA FENETRE D'ETAT

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

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour configurer l'affichage de la fenêtre d'état au démarrage de l'application, procédez comme suit.

1. Sous l'onglet **Avancé** sélectionnez l'option **Paramètres**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Fenêtre d'état** (cf. ill. ci-après) :

   - **Afficher** : affiche la fenêtre d'état ;
   - **Masquer** : n'affiche pas la fenêtre d'état.

Figure61 : configuration de l'affichage de la fenêtre d'état

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

AFFICHAGE DE L'ICONE DE PROTECTION

Pour voir l'état de la protection, vous pouvez configurer l'affichage de l'icône de la protection sur l'écran de l'appareil mobile (cf. la rubrique “Icône de la protection» à la page 26).

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Fonctions** → **Modifier**.

Pour modifier les paramètres d'affichage de l'icône de la protection, procédez comme suit.

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Icône de protection** (cf. ill. ci-après) :

   - **Afficher partout** : affiche l'icône de protection sur l'écran de l'appareil ;
   - **Menu uniquement** : affiche l'icône de protection uniquement lorsque le menu de l'appareil ou le menu de Kaspersky Endpoint Security 8 for Smartphone est ouvert ;
   - **Ne pas afficher** : n'affiche pas l'icône de la protection.

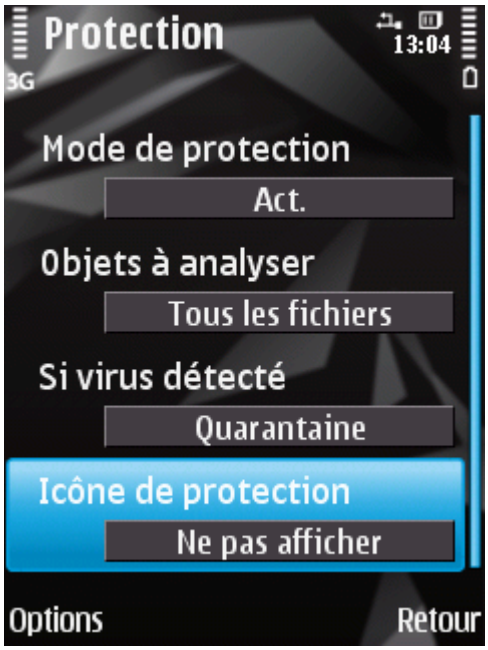

Figure 62: paramètres d'affichage de l'icône de la protection

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

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'application ne peut être activée qu'avec une licence installée.

ANALYSE A 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 ANTIVIRUS

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.

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.

C

CODE SECRET DE L'APPLICATION

Le code secret de l'application permet d'éviter l'accès non autorisé aux paramètres de l'application et aux données protégées de l'appareil. Il est saisi par l'utilisateur à la première exécution de l'application et compte au moins quatre chiffres. Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder aux paramètres de l'application ;
- Pour accéder aux dossiers cryptés ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Géolocalisation, Contacts personnels ;
- Pour supprimer l'application.

D

DESINFECTION OU REPARATION 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.

L

LISTE BLANCHE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont acceptés par Anti-Spam.

- Type d'événement en provenance de ce numéro que l'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

LISTE NOIRE

Les entrées de cette liste contiennent les informations suivantes :

- Numéro de téléphone dont les appels et/ou les SMS sont bloqués par Anti-Spam.
- Type d'événement en provenance de ce numéro que l'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet à Anti-Spam d'identifier des SMS non sollicités (spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

MASQUE DU NUMERO DE TELEPHONE

Présentation du numéro de téléphone dans la liste noire ou blanche par les caractères communs. Les deux caractères génériques de base utilisés dans les masques de numéro de téléphone sont "*» et "?» (où * représente une suite de caractères quelconques et ? un seul caractère). Il s'agit, par exemple, du numéro *1234 ? dans la liste noire. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de maintenir la protection à jour. Elle copie les bases antivirus depuis les serveurs de mises à jour de Kaspersky Lab sur l'appareil en les intégrant à l'application en mode automatique.

N

NON-NUMERIQUES

Numéro de téléphone contenant des lettres ou composé intégralement de lettres.

O

OBJET INFECTE.

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une 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.

OBJET PROBABLEMENT INFECTE

Objet dont le code contient soit un code modifié d'un virus connu, soit un code qui ressemble à un virus, mais jusqu'alors a été inconnu de Kaspersky Lab. Les fichiers probablement infectés sont détectés à l'aide de l'analyseur euristique.

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.

Q

QUARANTAINE.

Dossier spécial où sont placés tous les objets probablement infectés, détectés pendant l'analyse ou par la protection.

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 SMS

Méthode de traitement d'un 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.

SYNCHRONISATION

Un processus d'établissement de la connexion entre l'appareil mobile et le système d'administration distante suivi de la transmission des données. Lors de la synchronisation, l'appareil reçois les paramètres de l'application, installés par l'administrateur. L'appareil envoie dans le système d'administration distante les rapports sur le fonctionnement des composants de l'application.

SYSTEME D'ADMINISTRATION DISTANTE

Un système qui permet de contrôler les appareils à distance et de les administrer en temps réel.

KASPERSKY LAB ZAO

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes seniors 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 œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour 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 : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab 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. Nous offrons à nos clients une assistance technique 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 Web de Kaspersky Lab :	http://www.kaspersky.com/fr
L'Encyclopédie des virus:	http://www.securelist.com/fr
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)

UTILISATION DE CODE TIERS

Le code développé par d'autres éditeurs a été utilisé pour créer l'application.

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique.

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

INDEX

A

B

C

D

E

F

I

J

K

L

M

N

O

P

Q

R

S

V