# Kaspersky Endpoint Security 8 for Smartphone

*pour Android ™ 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.



Date d'édition : 10 mai 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.

### DANS CETTE SECTION



# DANS CE DOCUMENT

Ce document reprend les sections suivantes :

### Sources d'informations complémentaires

Cette section contient des informations supplémentaires concernant l'application et les ressources Internet où vous pouvez discuter de l'application, échanger des idées, poser des questions et obtenir des réponses.

### Kaspersky Endpoint Security 8 for Smartphone

Cette section contient une description des fonctionnalités de l'application et offre des informations succinctes sur ses composants et leurs fonctions principales. Cette section contient les informations concernant le pack livré. La section décrit également la configuration matérielle et logicielle requises pour l'installation de Kaspersky Endpoint Security 8 for Smartphone.

### Installation de Kaspersky Endpoint Security 8 for Smartphone

Cette section contient les instructions qui vous aideront à installer l'application sur l'appareil mobile.

### Suppression de l'application

Cette section contient les instructions qui vous aideront à supprimer l'application de l'appareil mobile.

### Premiers pas

Cette section contient les informations comment commencer à travailler avec Kaspersky Endpoint Security 8 for Smartphone : l'activer, saisir le code secret de l'application, activer la fonction de restauration du code secret, restaurer le code secret et lancer le programme.

### Gestion de la licence

Cette section contient les informations sur les concepts de base utilisées pour l'octroi de licence de l'application. La section présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Endpoint Security 8 for Smartphone et de la renouveler.

### Interface de l'application

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

### Protection du système de fichiers

La section 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.

### 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'un objet malveillant.

### 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.

### Protection des données 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.

### Dissimulation des informations personnelles

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

### Mise à 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.

### Configuration des paramètres complémentaires

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.

### Contacter le Service d'assistance technique

Cette section contient des recommandations pour contacter Kaspersky Lab en utilisant l'espace personnel du Service d'assistance technique du site ou par téléphone.

### Glossaire

Cette section contient la liste des termes présents dans le document ainsi que leurs définitions.

### Kaspersky Lab

Cette section présente la société Kaspersky Lab.

### Informations sur le code tiers

La section reprend les informations relatives au code tiers utilisé dans l'application.

### Index

Cette section vous aidera à trouver rapidement les informations nécessaires dans le document.

# CONVENTIONS

Les conventions décrites dans le tableau ci-dessous sont utilisées dans le document.

*Таблица 1. Conventions*

| EXEMPLE DE TEXTE | DESCRIPTION DE LA CONVENTION |
|---|---|
| Veuillez noter que ... | Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations importantes, par exemple, les informations liées aux actions critiques pour la sécurité de l'ordinateur. |
| Il est conseillé d'utiliser... | Les remarques sont encadrées. Les remarques fournissent des conseils et des informations d'assistance. |
| **Exemple** :<br>... | Les exemples sont présentés sur un fond jaune sous le titre "Exemple". |
| La *mise à jour*, c'est ... | Les nouveaux termes sont en italique. |
| **ALT+F4** | Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.<br>Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. |
| **Activer** | Les noms des éléments de l'interface sont en caractères mi-gras : les champs de saisie, les commandes du menu, les boutons. |
| *Pour planifier une tâche, procédez comme suit :* | Les phrases d'introduction sont en italique. |
| `help` | Les textes dans la ligne de commande ou les textes des messages affichés sur l'écran par l'application sont en caractères spéciaux. |
| <adresse IP de votre ordinateur> | Les variables sont écrites entre chevrons. La variable est systématiquement remplacée par sa valeur. Les parenthèses angulaires sont omises. |

# 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 l'application :

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

### Page sur le site 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 questions sont regroupées par sujet, par exemple « Utilisation des fichiers de licence », « Mise à jour des bases » ou « Résolution des problèmes ». 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 **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.

# DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB DANS LE FORUM

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 sections 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. L'objet du message devra être « Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Smartphone ».

# KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protège les appareils mobiles (ci-après, les appareils) tournant sous Android™. L'application permet de protéger les informations sur l'appareil contre toute infection de menaces inconnues, prévenir la réception de SMS indésirable et d'appels, protéger les informations sur l'appareil en cas de vol ou perte et masquer également les informations relatives aux contacts confidentiels. 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.

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 votre appareil à distance à l'aide d'un autre appareil, de supprimer les informations qui s'y trouvent et de localiser ses coordonnées géographiques. 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 dans Contacts pour ces numéros, l'historique des appels et SMS, des appels reçues et SMS.

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

### DANS CETTE SECTION



## SPECIFICATIONS MATERIELLES ET LOGICIELLES

Kaspersky Endpoint Security 8 for Smartphone s'installe sur les appareils mobiles travaillant sous la direction des systèmes d'exploitation Android OS 1.5, 1.6, 2.0, 2.1, 2.2.

# 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



## 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.

# 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 un ordinateur en marche.

   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).

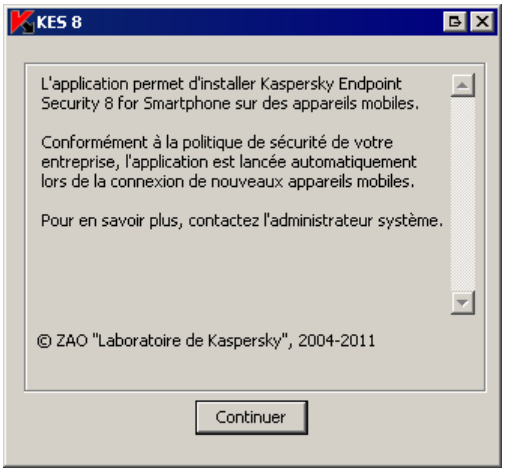


*Figure 1: programme d'installation de Kaspersky Endpoint Security 8 for Smartphone*

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 du nom 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.

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 d'administrateur avec des paramètres d'installation de l'application depuis votre appareil mobile ou votre 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.

   Si vous téléchargez la distribution de l'application sur l'appareil mobile, elle sera enregistrée par défaut dans une carte mémoire.

3. Exécutez une des opérations suivantes :
   - si vous avez téléchargé la distribution de l'application sur l'appareil mobile, ouvrez-la ;
   - si vous avez téléchargé la distribution de l'application sur le poste de travail, connectez l'appareil mobile à l'ordinateur, copiez la distribution sur l'appareil et ouvrez-la.

     L'installation de l'application sera effectuée automatiquement et l'application sera installée sur l'appareil.
4. Lancez l'application (cf. la rubrique "Lancement de l'application" à la page 25). Pour ce faire, passez de l'écran d'accueil à l'écran des applications et sélectionnez Kaspersky Endpoint Security 8 for Smartphone.

   L'écran **Paramètres de synchronisation** (cf. ill. ci-après) apparaît.


*Figure 3: paramètres de synchronisation*

5. 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 la configuration des paramètres de connexion au système d'administration distante n'est pas nécessaire, cette étape est omise.

6. Saisissez l'adresse électronique de votre organisation dans le champ **Adresse de courrier électronique** et cliquez sur **Continuer**.

   L'adresse de courrier électronique sert à enregistrer l'appareil dans le système d'administration à distance. N'oubliez pas qu'il est impossible de modifier l'adresse indiquée lors de l'installation de l'application.

7. Saisissez le code personnel de l'application (cf. la section « Saisie du code personnel » à la page 25). Pour ce faire, remplissez le champ **Définissez le code personnel**, puis le champ **Confirmation du code** et cliquez sur **OK**.

8. Activez la fonction de restauration du code personnel (cf. section « Activation de la fonction de restauration du code personnel » à la page 26).

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

# SUPPRESSION DE L'APPLICATION

La suppression de l'application de l'appareil est possible uniquement si le masque des informations confidentielles est désactivé. Après cela, vous devez vous assurez que cette condition est remplie.

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

1. Désactivez dissimulations des informations confidentielles (à la page 67).
2. Passez de l'écran d'accueil à l'écran des applications et choisissez l'option **Paramètres** → **Applications** → **Gérer les applications**
3. Sélectionnez Kaspersky Endpoint Security 8 for Smartphone dans la liste des applications.
4. L'écran **Informations sur l'application** s'affiche.Cliquez sur **Désinstaller**.

   La fenêtre de confirmation de suppression s'ouvre.
5. Confirmer la suppression de Kaspersky Endpoint Security 8 for Smartphone en cliquant sur **OK**.

   L'application sera supprimée de l'appareil.
6. Dès que la suppression est terminée, cliquez sur **OK**.

# 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.

L'administrateur peut interdire la modification de tous les paramètres du composant ou de certains de ses paramètres. Si en haut de l'écran de configuration du composant un verrou et un message d'avertissement s'affichent, les paramètres du composant de l'appareil mobile ne peuvent pas être modifiés.

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 synchronisation de l'appareil avec le système d'administration à distance (cf. la section « Synchronisation avec le système d'administration à distance » à la page 21).

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 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 le composant Anti-Spam, effectuer l'analyse antivirus de votre appareil mobile et utiliser les composants de 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 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 :

- rechercher la présence éventuelle de virus ;
- configurer les paramètres avancés de l'application ;
- synchroniser l'appareil avec le système d'administration à distance ;
- désactiver de la dissimulation des informations confidentielles ;
- consulter le système d'aide.

Si la licence n'a pas été installée dans les trois jours après l'installation, il faudra l'installer via la fonction de synchronisation de l'appareil avec le système d'administration à distance.

# AFFICHAGE DES INFORMATIONS DE LICENCE

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

*Pour consulter les informations sur la licence, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

# 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.

La synchronisation manuelle s'impose si la licence n'a pas été installée dans les trois jours qui suivent l'installation de l'application.

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).

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

## DANS CETTE SECTION

# LANCEMENT DE LA SYNCHRONISATION A LA MAIN

- *Pour réaliser la synchronisation manuelle de l'appareil avec le système d'administration à distance après l'installation de l'application,*

  appuyez sur **Lancer la synchronisation** à l'écran principal après le message d'avertissement (cf. ill. ci-après).

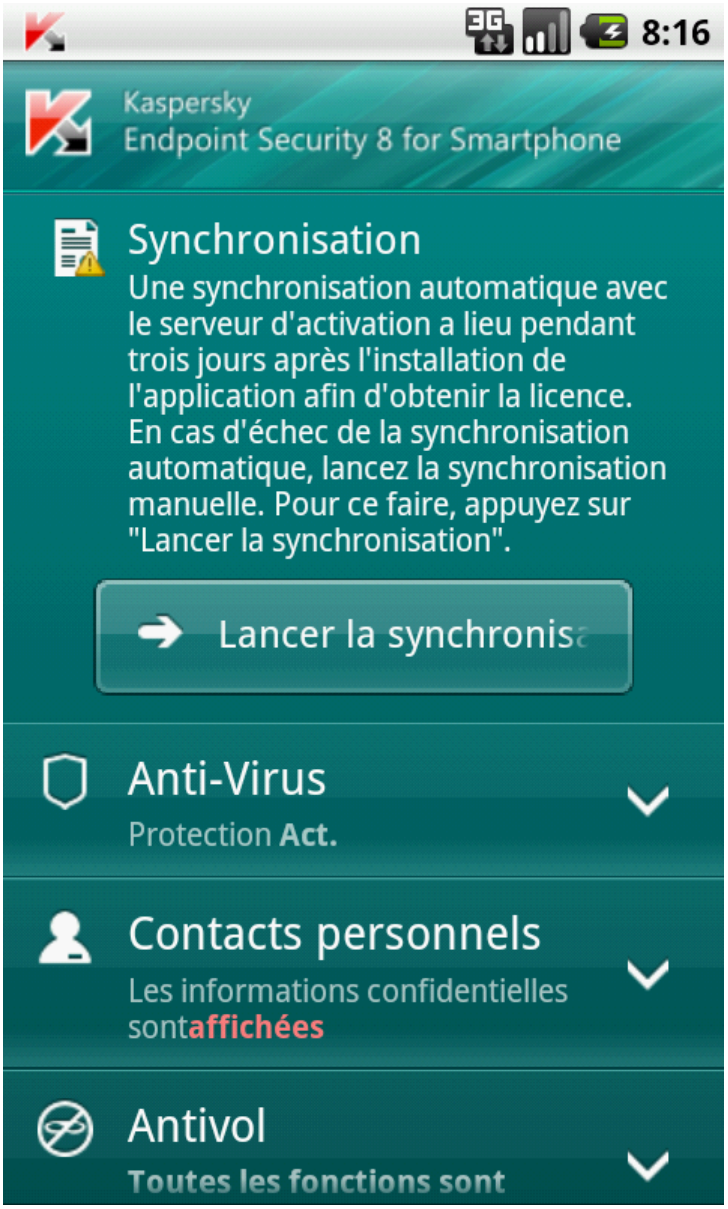


*Figure 4 : lancement de la synchronisation*

La possibilité de lancer la synchronisation sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone est accessible après l'installation de l'application en cas d'échec de la connexion automatique au système d'administration à distance.

Quand la synchronisation est exécutée, les paramètres de l'application sont appliqués à l'appareil et la licence est installée. Le bouton **Lancer la synchronisation** n'apparaît plus sur l'écran principal de l'application.

*Pour synchroniser l'appareil avec le système d'administration distante à la main, procédez comme suit :*

1. Développez le groupe **Avancé** sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone.

   L'écran **Avancé** s'ouvre.

2. Appuyez sur **Synchroniser**.

   Si, au cours de l'installation de l'application, l'utilisateur n'a pas été invité à saisir les paramètres de connexion au système d'administration à distance, alors la connexion au système d'administration à distance est établie.

   Si l'utilisateur a été invité à saisir les paramètres de connexion au système d'administration à distance pendant l'installation de l'application, l'option du menu s'appelle **Synchronisation** et l'écran **Synchronisation** s'affiche. Appuyez sur **Synchroniser**. 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 à distance sans être guidé par l'administrateur.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Synchronisation**.

   L'écran **Synchronisation** (cf. ill. ci-après) s'ouvre.


*Figure 5: paramètres de synchronisation*

3. Modifiez la valeur des paramètres suivants dans le groupe **Paramètres de synchronisation** :
   - **Serveur** ;
   - **Port** ;
   - **Groupe**.

# PREMIERS PAS

Cette section contient les informations comment commencer à travailler avec Kaspersky Endpoint Security 8 for Smartphone : l'activer, saisir le code secret de l'application, activer la fonction de restauration du code secret, restaurer le code secret et lancer le programme.

### DANS CETTE SECTION



## DEMARRAGE DU LOGICIEL

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

1. Passez de l'écran principal à celui des applications.
2. Sélectionnez **Kaspersky Endpoint Security 8 for Smartphone**.
3. L'écran **Kaspersky Endpoint Security 8 for Smartphone** s'ouvre.
4. Saisissez le code secret de l'application puis cliquez sur **Entr.**

L'écran principal de l'application s'ouvre.

## 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 la saisie du code personnel dans les cas suivants :

- Pour accéder à l'application ;
- Pour envoyer une instruction SMS depuis un autre appareil mobile pour activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Localisation, Contacts personnels.

Le code secret de l'application est composé de chiffres. Le nombre minimal de chiffres est 4.

Si vous avez oublié le code secret, vous pouvez le restaurer (cf. section "Restauration du code secret" à la page 26). Pour ce faire, il faut d'abord activer la fonction de restauration du code secret (cf. section Activation de la fonction de restauration du code secret à la page 26).

*Pour saisir le code secret, procédez comme suit :*

1. Apres activation de l'application dans le champ **Saisissez le code secret**, tapez les chiffres de votre code.

   La robustesse du code saisi est vérifiée automatiquement.

   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**. Répétez la saisie du code secret de l'application.

2. Tapez de nouveau ce code dans la zone **Confirmation du code**.

   Le code secret sera sauvegardé.

# ACTIVATION DE LA FONCTION DE RESTAURATION DU CODE SECRET

Après la première activation, vous pouvez activer l'option de restauration du code secret de l'application. Alors par la suite, vous allez pouvoir restaurer le code secret oublié de l'application.

Si vous avez refusé l'activation de cette fonction après la première activation de l'application, vous pouvez l'activer après la réinstallation de Kaspersky Endpoint Security 8 for Smartphone sur l'appareil.

Vous pouvez restaurer le code secret de l'application (cf. section "Restauration du code secret" à la page 26), uniquement si la fonction de restauration du code secret est activée. Si vous avez oublié le mot de passe et que la fonction de restauration est désactivée, il sera impossible d'administrer les fonctions Kaspersky Endpoint Security 8 for Smartphone.

*Pour activer la possibilité de restaurer le code secret, procédez comme suit :*

1. Après installation du code secret de l'application (cf. section Installation du code secret à la page. 25), entrez votre adresse électronique dans l'écran **Activation de la fonction de restauration du code secret**.
2. Confirmez l'activation de la fonction de restauration du code secret, en cliquant sur **Activer**.

   L'adresse saisie sera utilisée lors de la restauration du code secret.

   L'application établira une connexion Internet avec le serveur de restauration du code secret, enverra les informations saisies et activera la fonction de restauration du code secret.

# RESTAURATION DU CODE SECRET

Vous pouvez restaurer le code secret uniquement si la fonction de restauration du code secret (cf. section "Activation de la fonction de restauration du code secret" à la page 26) avait été activée.

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

1. Passez de l'écran principal à celui des applications.
2. Sélectionnez **Kaspersky Endpoint Security 8 for Smartphone**.

   L'écran **Kaspersky Endpoint Security 8 for Smartphone** s'ouvre.
3. Cliquez sur **Menu** → **Restauration du code secret**.

   Le message contenant les informations suivantes s'affiche à l'écran :

   - site Web de Kaspersky Lab pour la restauration du code personnel ;
   - code d'identification de l'appareil.
4. Appuyez sur **Passer**.

   Passez au site web http://mobile.kaspersky.com/recover-code pour restaurer le code secret.
5. Saisissez les informations suivantes dans les champs correspondants :

   - adresse du courrier électronique que vous avez désigné auparavant pour restaurer le code secret ;
   - code d'identification de l'appareil.

   Finalement, le code de restauration sera envoyé à l'adresse du courrier électronique que vous avez indiqué.
6. Passez à l'écran **Kaspersky Endpoint Security 8**.
7. Cliquez sur **Menu** → **Saisie du code de rest.** et entrez le code de restauration reçu.
8. Saisissez un nouveau code secret de l'application. Pour ce faire, saisissez le nouveau code personnel dans les champs **Définissez le nouveau code personnel** et **Confirmez le nouveau code**.
9. Cliquez sur **Entrée**.

# 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 sur l'application, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez le groupe **Informations**, le point **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

# ECRAN PRINCIPAL DE L'APPLICATION

Après le lancement de l'application, l'écran principal s'ouvre (cf. ill. ci-après).

Les groupes déroulants sont disposés sur l'écran principal. Chaque groupe permet de passer à la configuration de l'un des composants du programme et à l'exécution des tâches.

L'état des principaux composants de l'application est également affiché sur l'écran principal.

Les informations suivantes, au-dessus du nom de chaque group, vous sont proposées :

- **Anti-Virus** : état de la protection de l'appareil contre les virus et autres programmes malveillants (cf. section Protection des fichiers systèmes à la page 31) ;
- **Contacts personnels** : état de la dissimulation des informations confidentielles.
- **Antivol** : états de la fonction Antivol.
- **Anti-Spam** : mode de filtrage des appels et des SMS.
- **Avancé** : informations concernant les paramètres avancés de l'application, rassemblés dans un même groupe (cf. section Paramètres avancés de l'appareil à la page 78).

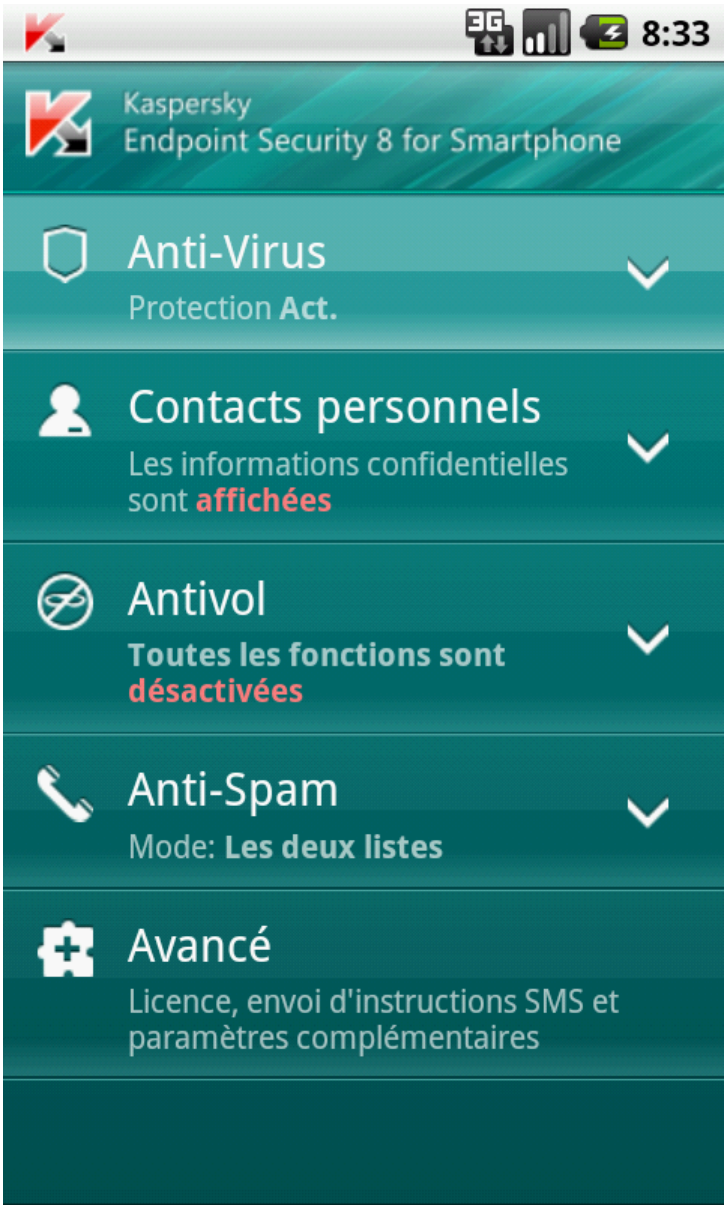


*Figure 6 : écran principal de l'application*

# GADGET DE L'ECRAN PRINCIPAL

Le gadget de l'écran principal est accessible pour l'utilisation de Kaspersky Endpoint Security 8. (cf. ill. ci-après).

*Figure 7 : gadget de l'écran principal*

L'indicateur de couleur du gadget de l'écran principal informe sur l'état de protection de votre appareil, sur les Contacts personnels et sur la licence, et permet de passer à la configuration des paramètres de l'application.

Voici les indicateurs de couleur :

- Le bouclier vert signifie que la Protection est activée ;
- Le bouclier gris signifie que la Protection est désactivée ;
- Arrière-plan vert signifie que les informations confidentielles sont masquées ;
- Arrière-plan gris signifie que les informations confidentielles sont visibles ;
- Le point d'exclamation dans un triangle jaune signifie que la validité de la licence a expiré ou que la licence n'a pas été installée.

# PROTECTION DU SYSTEME DE FICHIERS

La section 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 est lancée en même temps que le système d'exploitation et se trouve en permanence dans la mémoire vive de l'appareil.

L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. La protection analyse chaque fichier au moment où vous essayez 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 de l'application 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 :
   - en cas de découverte un code malveillant dans un fichier, la Protection effectue action correspondant aux paramètres de la tâche (cf. section Sélection de l'action à réaliser sur les objets découverts à la page 34) ;
   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

La Protection analyse l'application installée à la présence lors de son premier lancement. La Protection analyse les bases des données antivirus. Si la Protection découvre un virus lors de l'analyse du programme, elle vous proposera de le supprimer.

## 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 les autres menaces est effectuée en utilisant les ressources de l'appareil. 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 n'affecte pas les tâches d'analyse antivirus et de mise à jour des bases antivirus de l'application.

L'état actuel de Protection est affiché sur l'écran principal de l'application dans le groupe **Anti-Virus**.

➧ *Pour désactiver la protection, procédez de la manière suivante :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Cochez la case **Activer la protection** (cf. ill. ci-après).

*Pour désactiver la protection, procédez de la manière suivante :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Désélectionnez la case **Activer la protection**.

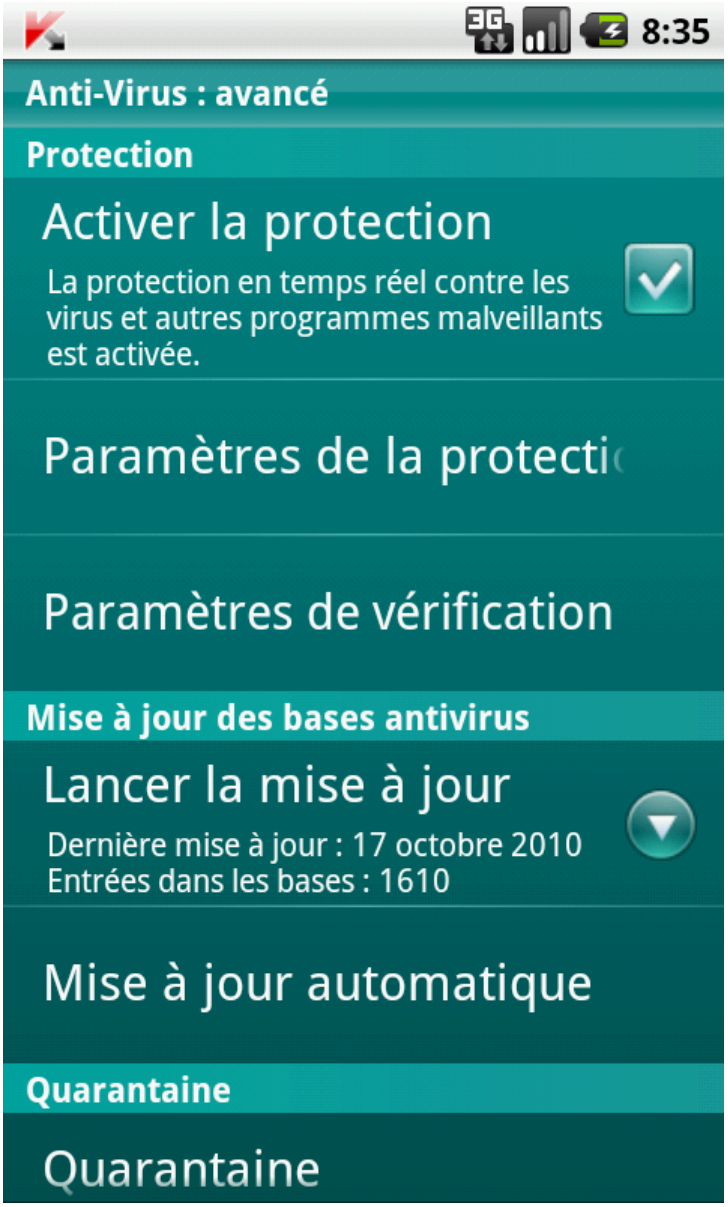


*Figure 8 : activation de la protection*

# CONFIGURATION DE LA ZONE DE PROTECTION

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

Assurez-vous que la Protection a été activée avant s configuration.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres Protection** → **Type de fichiers protégés**.
4. Sélectionnez la valeur pour le paramètre **Type de fichiers protégés** (cf. ill. ci-après) :
   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables seulement** : analyse uniquement les fichiers exécutables de l'application (par exemple, fichiers au format EXE, MDL, APP, DLL, SO, ELF).

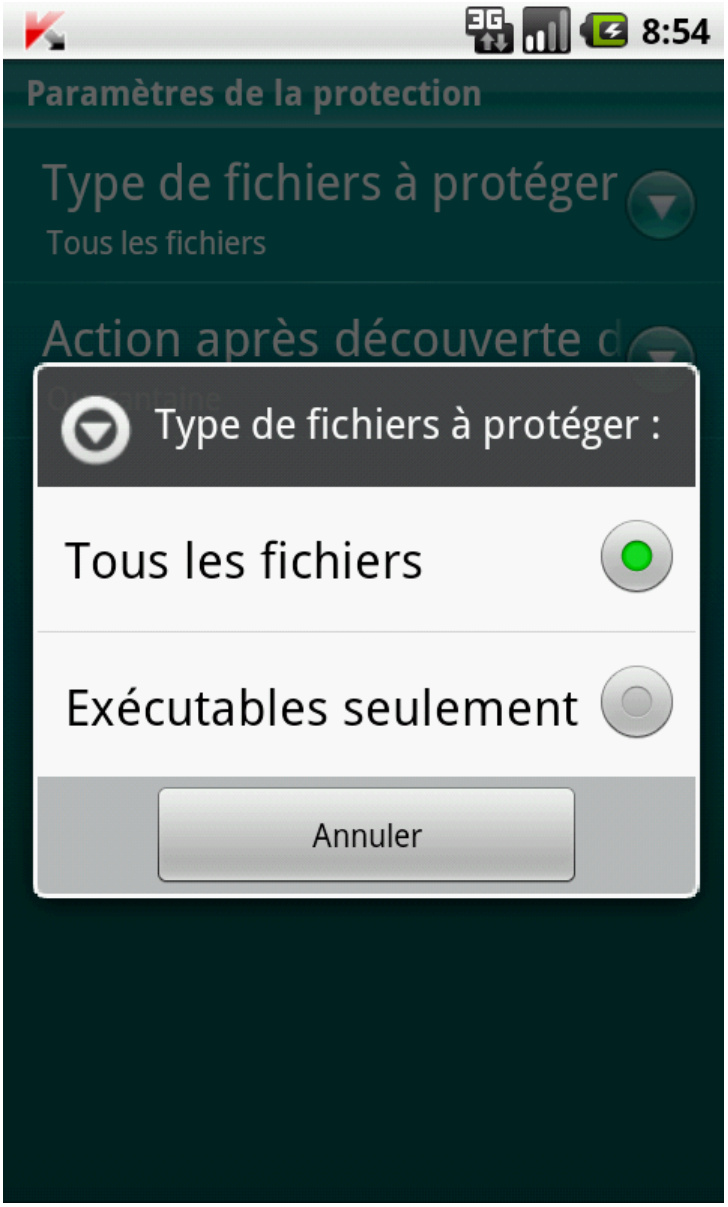


*Figure 9: sélection des objets à analyser*

# SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut, Kaspersky Endpoint Security 8 for Smartphone supprime la menace découverte. Vous pouvez sélectionner l'action que Kaspersky Endpoint Security 8 for Smartphone exécute sur la menace découverte.

*Pour configurer la réaction du programme lors de découverte d'une menace, réalisez les actions suivantes :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres de protection** → **Action lors détection d'une menace**.
4. Définissez l'action que l'application exécutera en cas de découverte d'une menace. Pour ce faire, sélectionnez la valeur pour le paramètre **Action lors détection d'une menace** (cf. ill. ci-après) :
   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Ignorer** : ignore les objets malveillants, ne les supprime pas de l'appareil.


*Figure 10 : sélection de l'action lors de la découverte de la menace*

# 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'un objet malveillant.

### 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 du type défini (cf. section « Sélection du type d'objet à analyser » à la page 38).
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.

   Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

   Si l'application découvre un code malveillant après analyse du fichier, elle exécutera l'action sélectionnée correspondant aux paramètres désignés Paramètres établis (cf. section Sélection de l'action à réaliser lors de la découverte d'un objet à la page 39).

L'analyse est lancée manuellement ou automatiquement selon un horaire prédéfini (cf. rubrique "Exécution de l'analyse programmée" à la page 37).

## 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Sélectionnez **Lancez l'analyse**.
3. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :
   - **Analyse complète** : analyse tout le système de fichiers de l'application. L'application analyse par défaut les fichiers stockés dans la mémoire de l'appareil et sur les cartes mémoire.
   - **Analyser dossiers** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte mémoire. Lors de la sélection du point **Analyser dossiers**, l'écran **Sélection du dossier** s'ouvre pour présenter le système fichier de l'appareil. Pour lancer l'analyse du dossier, supprimez le dossier nécessaire et cliquez sur le signe de l'analyse, à droite du nom du dossier.
   - **Analyse de la mémoire** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.

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). Dans la fenêtre de l'analyse, vous pouvez suspendre l'analyse en cliquant sur **Suspendre** ou l'interrompre en cliquant sur **Annuler**.

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 page39).

Par défaut, quand Kaspersky Endpoint Security 8 for Smartphone découvre un objet malveillant, il tente de le réparer. S'il est impossible de traiter un objet malveillant, le programme le supprimera.

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

- Le nombre de fichiers analysés ;
- Le nombre des virus découverts 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.


*Figure 11: sélection de la zone d'analyse*

# EXECUTION DE L'ANALYSE PROGRAMMEE

Vous pouvez configurer le lancement automatique planifié de l'analyse du système de fichiers. L'analyse est exécutée en arrière-plan. Quand un objet infecté est détecté, l'application exécute l'action sélectionnée dans la configuration de l'analyse (cf. section "Sélection des actions à appliquer sur les objets identifiés" à la page 39).

Par défaut, l'exécution d'analyse programmée est désactivée.

*Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres d'analyse**.

   L'écran **Paramètres d'analyse** s'ouvre.
4. Sélectionnez le mode de lancement de l'analyse. Pour ce faire, sélectionnez la valeur pour le paramètre **Analyse programmée** (cf. ill. ci-après) :
   - **Une fois/sem.** : l'analyse s'exécutera une fois par semaine. Pour ce mode, 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**.
   - **Une fois/j.** : l'analyse s'exécutera tous les jours. Pour ce mode, indiquez l'heure de lancement de l'analyse. Indiquez la valeur pour le paramètre **Heure de l'analyse**.
   - **Désactivée**: désactiver le démarrage de l'analyse planifiée.


*Figure 12 : Planification des analyses automatiques*

# SELECTION DU TYPE D'OBJET 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.

*Pour sélectionner un objet à analyser, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres d'analyse** → **Zone d'analyse**.

   L'écran **Zone d'analyse** s'ouvre.
4. Sélectionnez la valeur pour le paramètre **Type fichiers** (cf. ill. ci-après) :
   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables seulement** : analyse uniquement les fichiers exécutables des applications au format EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.

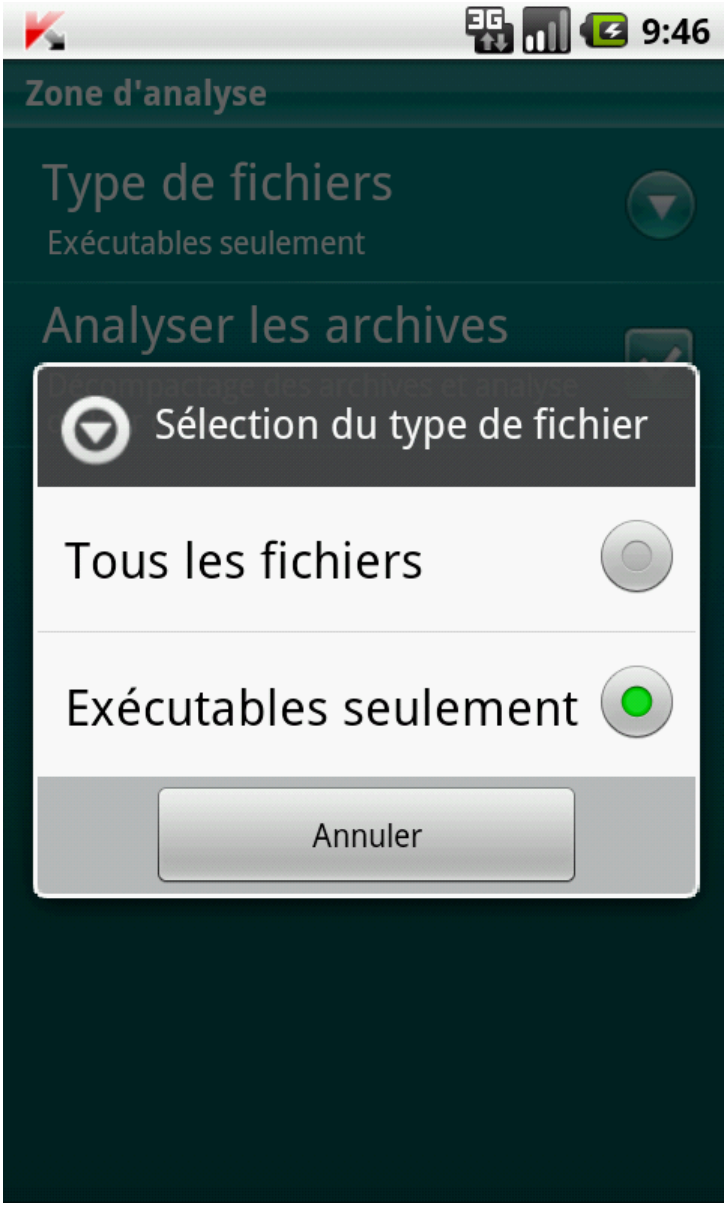


*Figure 13: sélection du type de fichiers à analyser*

# CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. L'application permet d'analyser les archives aux formats suivants : ZIP, JAR, JAD, SIS, SISX, CAB et APK. 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.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres d'analyse** → **Zone d'analyse**.

   L'écran **Zone d'analyse** s'ouvre.
4. Cochez la case **Analyser archives**.

# SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut, Kaspersky Endpoint Security 8 for Smartphone tente de réparer l'objet contenant la menace. Si la réparation est impossible, il la supprime. Vous pouvez configurer les actions du programme, si une menace a été découverte.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Paramètres d'analyse** → **Action lors détection d'une menace**.

   L'écran **Action lors détection d'une menace** s'ouvre.
4. Procédez à la première action sur la menace découverte. Décochez la case **Réparer**, pour que l'application tente de réparer la menace découverte. Cochez la case **Réparer**, pour que l'application ne tente pas de réparer la menace découverte.

5. Procédez à la deuxième action de l'application, s'il est impossible de réparer la menace découverte. Pour ce faire, attribuez une valeur au paramètre **Si la réparation impossible** (cf. ill. ci-après) :

   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Confirmer** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Ignorer** : ignore les objets malveillants, ne les supprime pas de l'appareil.


*Figure 14: sélection de l'action à exécuter sur les objets malveillants si la réparation est impossible*

# QUARANTAINE DES OBJETS MALVEILLANTS

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 la liste des objets malveillants, que l'application a mis en quarantaine. Le nom complet de l'objet dans la liste et la date à laquelle il a été découvert sont repris.

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

- *Pour consulter la liste des objets en quarantaine, procédez comme suit :*

  1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
  2. Cliquez sur **Avancé**.

     L'écran **Anti-Virus : avancé** s'ouvre.
  3. Appuyez sur **Quarantaine**.

     L'écran **Quarantaine** apparaît et affiche la liste des fichiers placés en quarantaine.

## 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
  2. Cliquez sur **Avancé**.

     L'écran **Anti-Virus : avancé** s'ouvre.
  3. Appuyez sur **Quarantaine**.

     L'écran **Quarantaine** s'ouvre.

4. Sélectionnez le fichier à restaurer, puis choisissez l'option **Menu** →□**Restaurer**.

Le fichier sélectionné dans la quarantaine est restauré dans son dossier d'origine.

# 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Appuyez sur **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.
4. Sélectionnez l'objet à supprimer, puis choisissez l'option **Menu** →□**Supprimer**.

L'objet sélectionné est supprimé de la quarantaine.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Appuyez sur **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.
4. Appuyez sur **Menu** → **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 DU COMPOSANT 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 43). 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 appels et aux SMS bloqués sont consignées dans le journal Anti-Spam (cf. section « Affichage des événements du journal » à la page 55).

## 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 :

- **Désactivé** : accepte tous les appels et les SMS entrants.
- **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.

- **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.

Vous pouvez modifier le mode de l'Anti-Spam (cf. la rubrique "Modification du mode de l'Anti-Spam" à la page 44). Le mode actuel de l'Anti-Spam s'affiche sous l'onglet **Anti-Spam** à côté de l'option **Mode**.

# MODIFICATION DU MODE DE L'ANTI-SPAM

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Mode : <mode actuel du composant>**.

   L'écran **Anti-Spam** s'ouvre.
3. Sélectionnez une valeur pour le paramètre **Mode Anti-Spam** (cf. ill. ci-dessous).

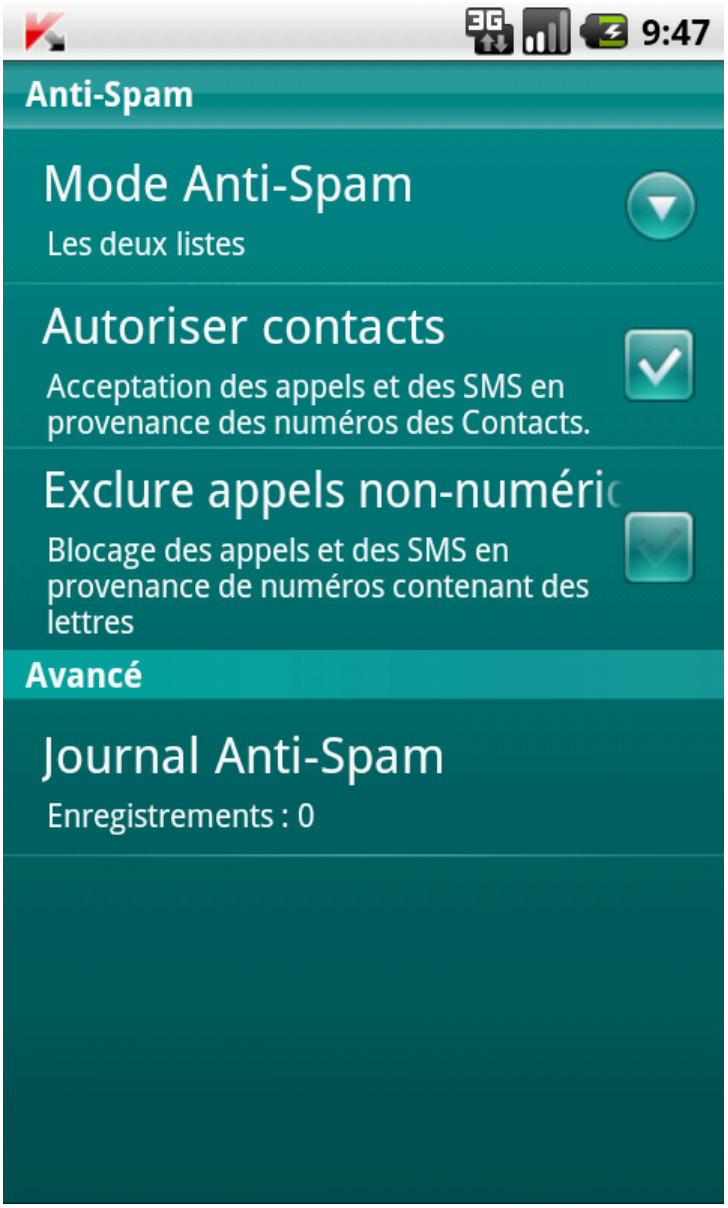


*Figure 15: modification du mode de l'Anti-Spam*

# 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 appels et aux SMS bloqués sont consignées dans le journal Anti-Spam (cf. section « Affichage des événements du journal » à la page 55).

## 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 ajouter un enregistrement à la liste noire de l'Anti-Spam, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste noire**.

   L'écran **Liste noire** apparaît.
3. Appuyez sur **Ajouter** (cf. ill. ci-dessous).
4. Indiquez la valeur des paramètres suivants :
   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste noire :
     - **SMS** : bloque uniquement les SMS entrants.
     - **Appels :** bloque uniquement les appels entrants.
     - **Appels et SMS** : bloque les appels et les SMS entrants.

- **Numéro de téléphone interdit** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Il est possible également d'utiliser en guise de numéro des masques « * » et « ? » (où « * » représente n'importe quelle série 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.
- **Texte interdit** : 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.

  Les paramètres accessibles pour ce type d'événement **SMS**.

Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Texte interdit** de cet enregistrement vide.

5. Cliquez sur **Enregistrer**.

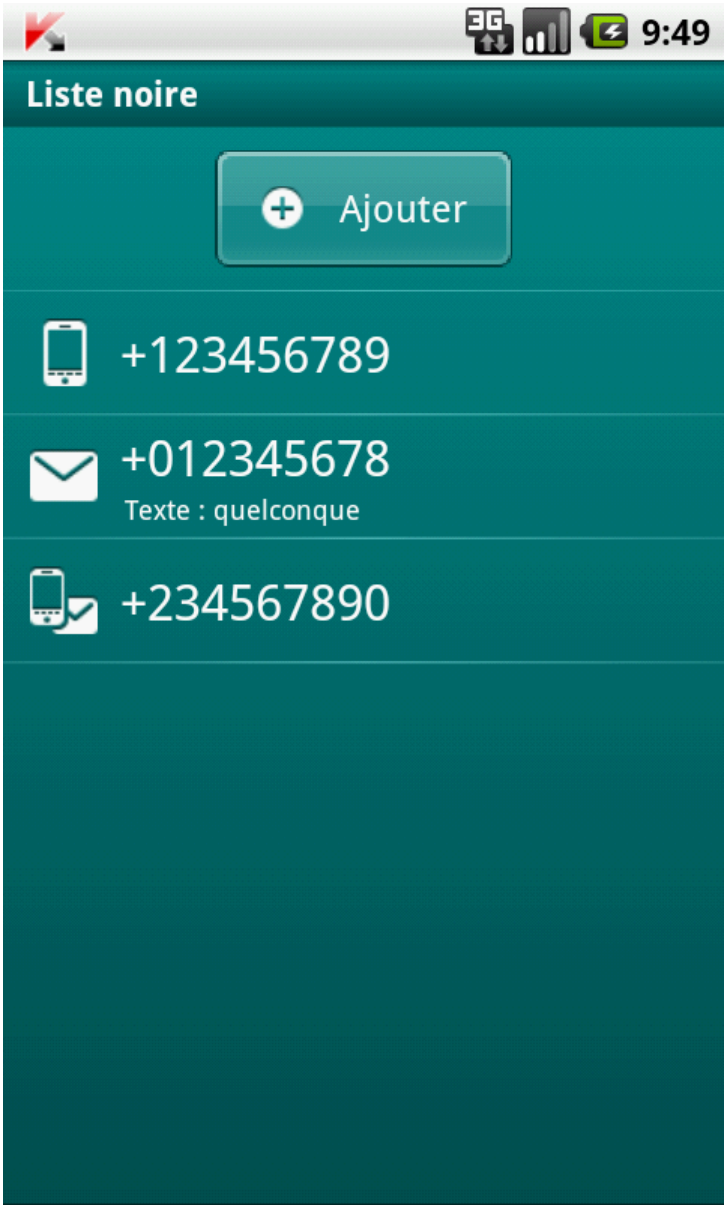


*Figure 16: ajout d'un enregistrement à la liste noire*

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste noire**.

   L'écran **Liste noire** apparaît.
3. Dans la liste, choisissez l'entrée à modifier et sélectionnez **Modifier** dans le menu contextuel.
4. Modifiez les paramètres requis.
   - **Numéro de téléphone interdit** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Il est possible également d'utiliser en guise de numéro des masques « * » et « ? » (où « * » représente n'importe quelle série 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.
   - **Texte interdit** : 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.

     Les paramètres accessibles pour ce type d'événement **SMS**.

     Si vous souhaitez interdire tous les SMS en provenance d'un numéro de la liste noire, laisser le champ **Texte interdit** de cet enregistrement vide.
5. Cliquez sur **Enregistrer**.

# 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste noire**.

   L'écran **Liste noire** apparaît.
3. Choisissez l'entrée à supprimer dans la liste, et sélectionnez **Supprimer** dans le menu contextuel.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste noire**.

   L'écran **Liste noire** apparaît.
3. Sélectionnez dans le menu contextuel **Supprimer tout**.

   La fenêtre de confirmation s'ouvre.
4. Pour confirmer la suppression, cliquez sur **Oui**.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
3. Appuyez sur **Ajouter** (cf. ill. ci-dessous).
4. Indiquez pour la nouvelle entrée, les paramètres suivants :
   - **Autoriser tout** : type d'événements en provenance du numéro de téléphone que l'Anti-Spam refusera pour les numéros de la liste blanche :
     - **SMS** : autorise les messages SMS entrants uniquement.
     - **Appels :** autorise uniquement les appels entrants.
     - **Appels et SMS** : autorise les appels et les SMS entrants.

- **Numéro de téléphone autorisé** : numéro de téléphone dont les informations entrantes sont acceptées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Il est possible également d'utiliser en guise de numéro des masques « * » et « ? » (où « * » représente n'importe quelle série de caractères et « ? », n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? dans la liste blanche. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
- **Texte autorisé** : 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.

  Les paramètres accessibles pour ce type d'événement **SMS**.

Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Texte autorisé** de cet enregistrement vide.

5. Cliquez sur **Enregistrer**.

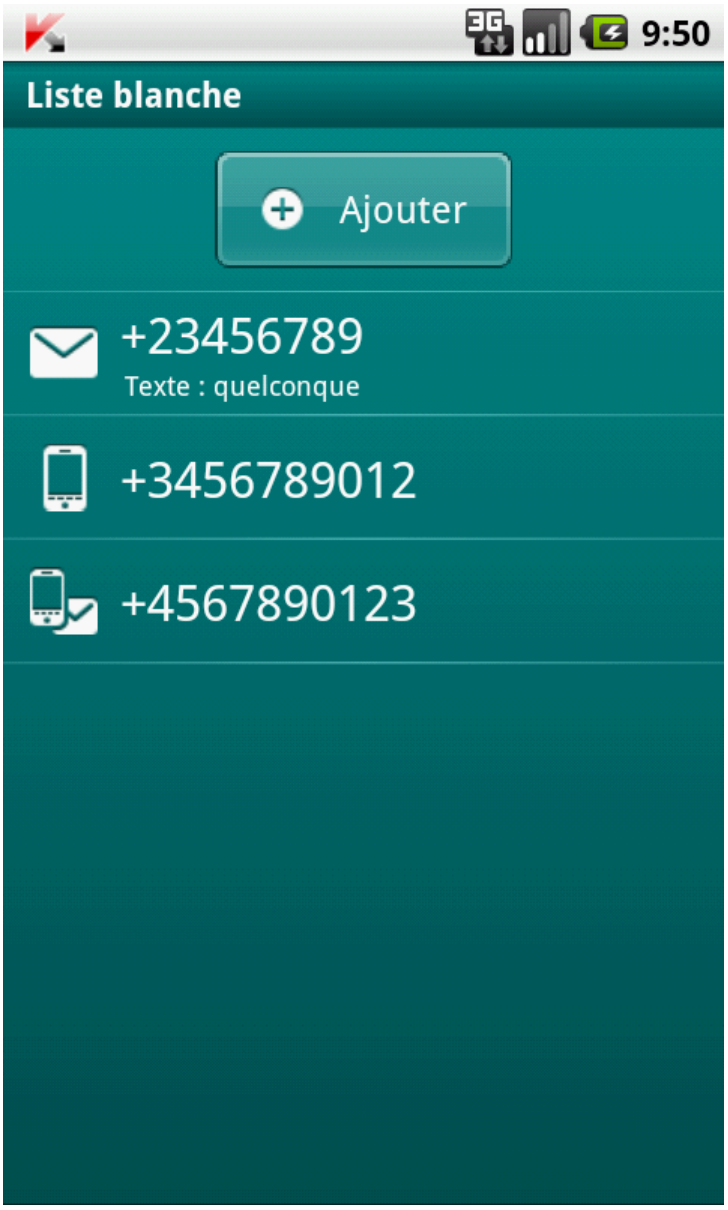


*Figure 17: ajout d'un enregistrement à la liste blanche*

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
3. Dans la liste, choisissez l'entrée à modifier et sélectionnez **Modifier** dans le menu contextuel.
4. Modifiez les paramètres requis.

   - **Numéro de téléphone autorisé** : numéro de téléphone dont les informations entrantes sont acceptées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Il est possible également d'utiliser en guise de numéro des masques « * » et « ? » (où « * » représente n'importe quelle série de caractères et « ? », n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? dans la liste blanche. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Texte autorisé** : 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.

     Les paramètres accessibles pour ce type d'événement **SMS**.

   Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Texte autorisé** de cet enregistrement vide.
5. Cliquez sur **Enregistrer**.

# 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
3. Choisissez l'entrée à supprimer dans la liste, et sélectionnez **Supprimer** dans le menu contextuel.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.
3. Sélectionnez dans le menu contextuel **Supprimer tout**.

   La fenêtre de confirmation s'ouvre.
4. Pour confirmer la suppression, cliquez sur **Oui**.

La liste blanche devient vide.

# REACTION AUX SMS ET APPELS DE CONTACTS QUI NE FIGURENT PAS DANS LE REPERTOIRE TELEPHONIQUE

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.

*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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Mode : <mode actuel du composant>**.

   L'écran **Anti-Spam** s'ouvre.
3. Choisissez la valeur de paramètre **Autoriser contacts** (cf. ill. ci-après) :
   - Pour que l'Anti-Spam considère un numéro des contacts comme un ajout à la liste blanche et qu'il n'accepte pas les SMS et les appels en provenance de numéros qui ne figurent pas dans les Contacts, cochez la case **Autoriser contacts** ;
   - Pour que l'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini de l'Anti-Spam, décochez la case **Autoriser contacts**.

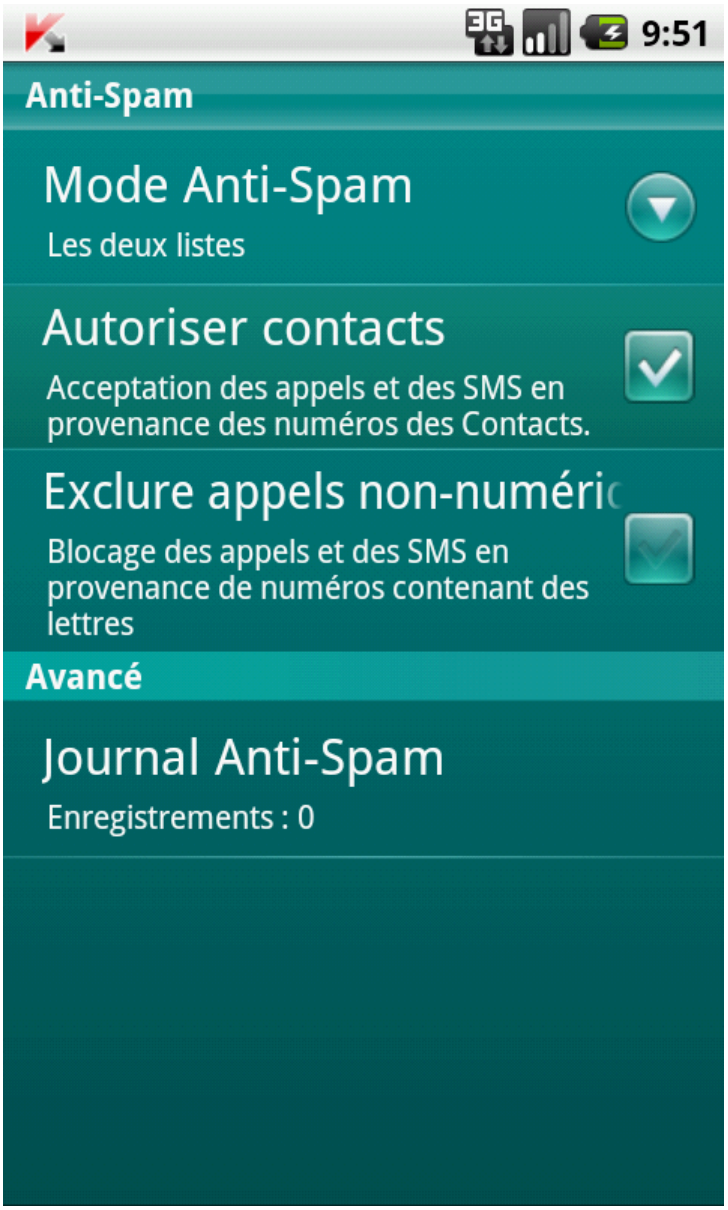


*Figure 18: réaction de l'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil*

# REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Pour le mode **Les deux listes** ou **Liste noire** de l'Anti-Spam, vous pouvez enrichir la liste noire en y ajoutant tous les numéros de téléphone alphanumériques. Si cette case est cochée, Anti-Spam traite les SMS en provenance des numéros sans chiffres comme s'il s'agit des numéros de la liste noire.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Mode : <mode actuel du composant>**.

   L'écran **Anti-Spam** s'ouvre.
3. Choisissez une valeur pour le paramètre **Interdire non numériques** (cf. ill. ci-après) :
   - afin que l'Anti-Spam bloque les messages en provenance de numéros sans chiffres, cochez la case **Exclure appels non numériques** ;
   - afin que l'Anti-Spam filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour Anti-Spam, décochez la case **Exclure appels non numériques**.

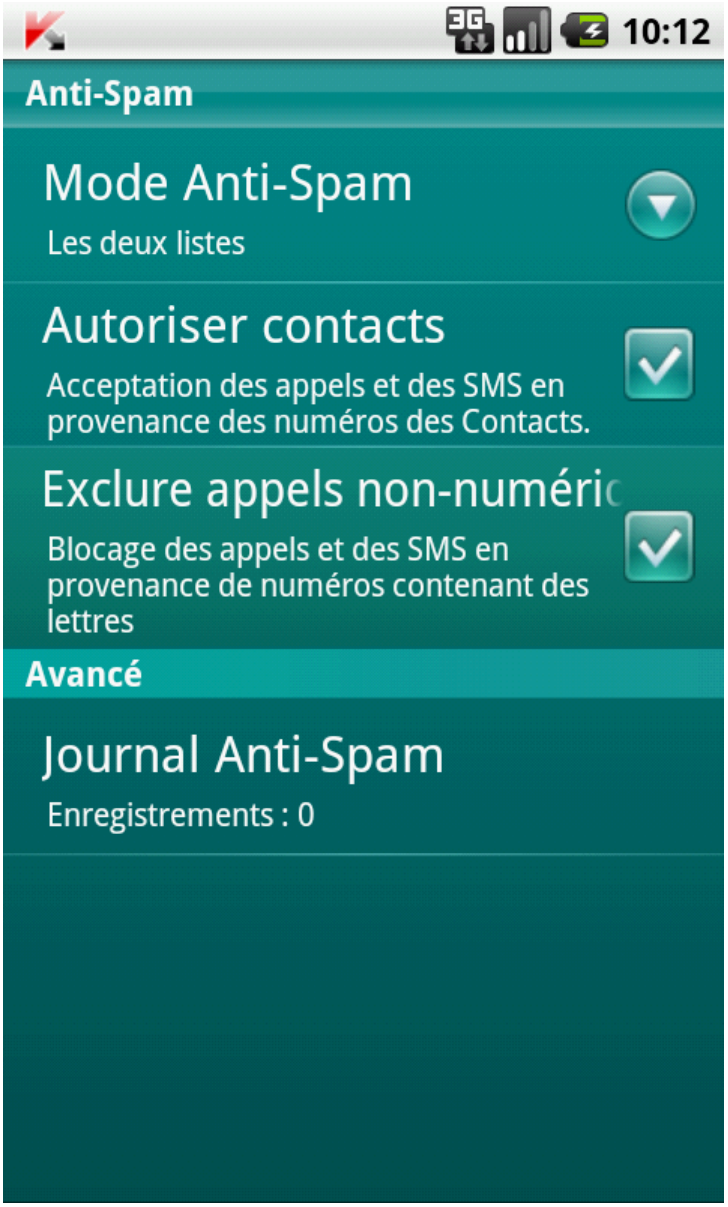


*Figure 19: Sélection des actions exécutées par Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres*

# SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

En mode **Les deux listes**, Anti-Spam vérifie si les SMS entrants correspondent aux entrées de la liste noire et à celles de la liste blanche.

Après la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, Anti-Spam suggère d'ajouter ce numéro sur une des listes (cf. ill. ci-après).

Vous pouvez choisir l'une des actions suivantes à appliquer sur le SMS :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, cliquez sur **Ajouter à la liste noire**.
- Pour livrer le SMS et ajouter le numéro de l'appelant à la liste blanche, cliquez sur **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**.

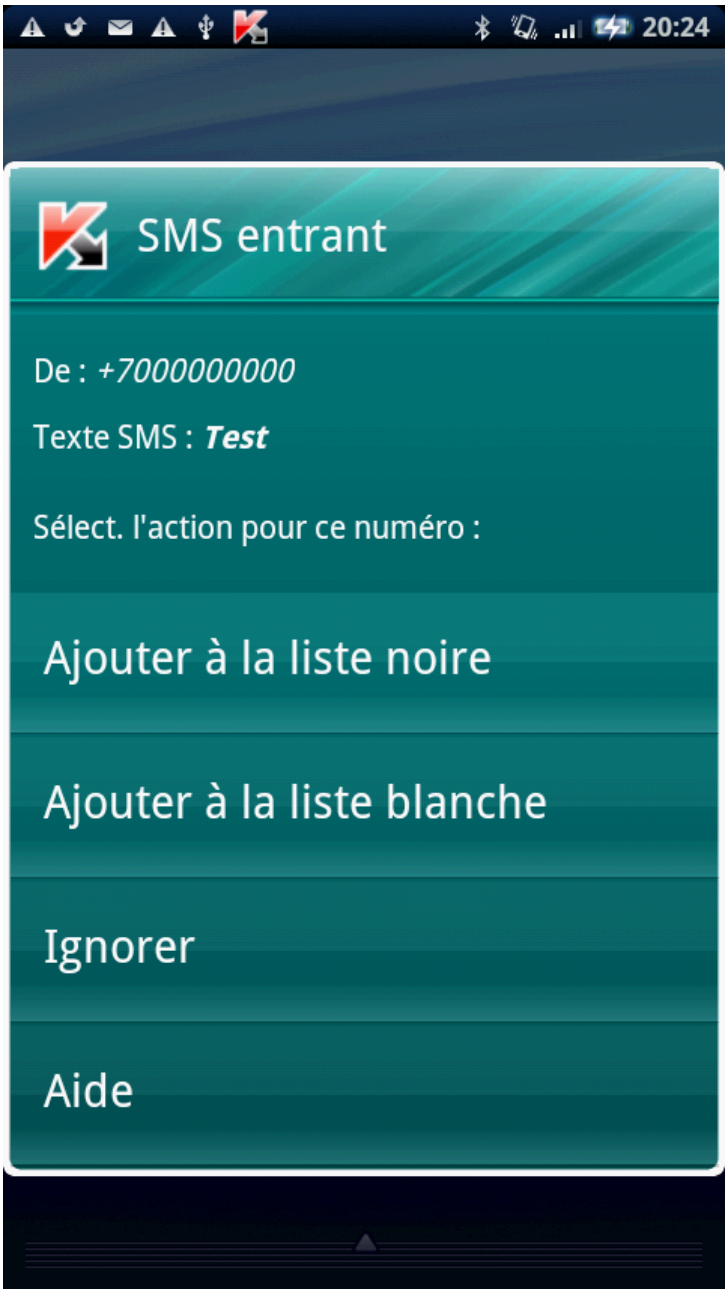


*Figure 20: notification de l'Anti-Spam sur le SMS reçu*

Les informations relatives aux SMS bloqués sont consignées dans le journal Anti-Spam (cf. la section « Affichage des événements du journal » à la page 55).

# SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

En mode **Les deux listes**, Anti-Spam vérifie si les appels entrants correspondent aux entrées de la liste blanche et de la liste noire. 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 (cf. ill. ci-après).

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

Les informations relatives aux appels bloqués sont consignées dans le journal Anti-Spam (cf. la section « Affichage des événements du journal » à la page 55).

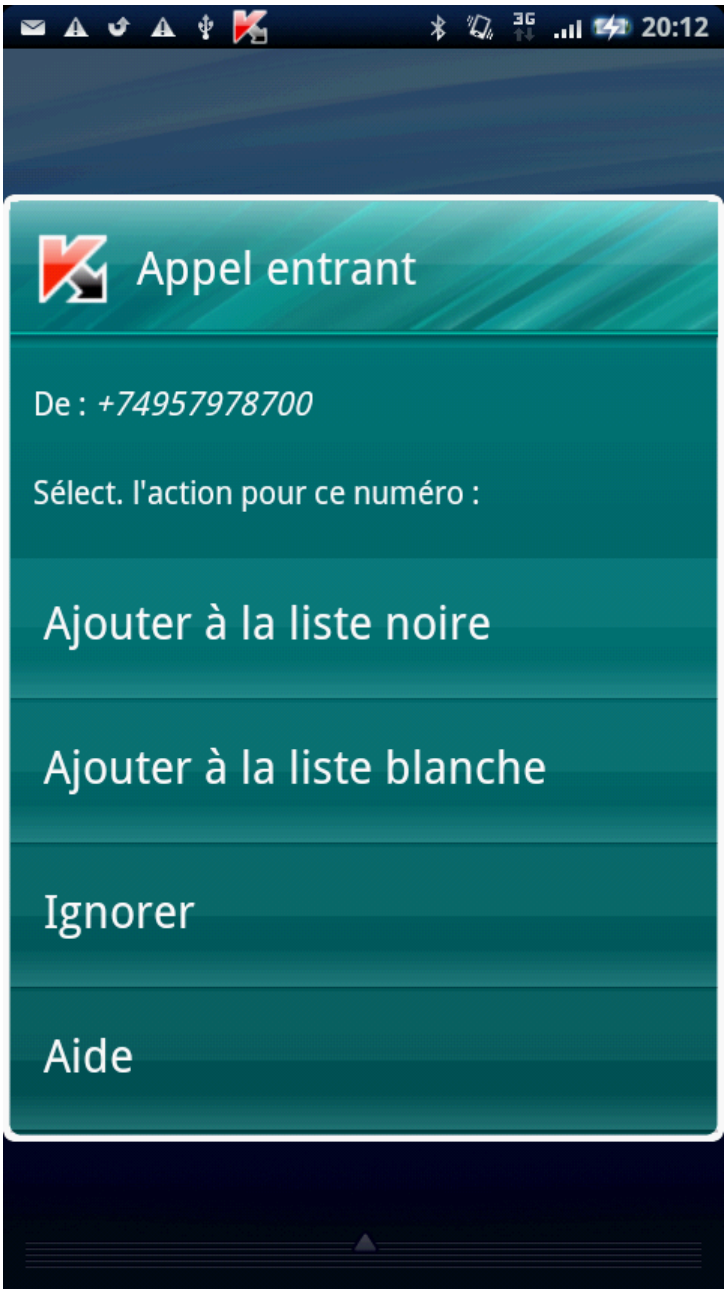


*Figure 21: notification de l'Anti-Spam sur l'appel reçu*

# AFFICHAGE DES EVENEMENTS DU JOURNAL

Vous pouvez consulter les informations relatives aux appels et aux SMS bloqués dans le journal Anti-Spam. Les entrées du journal sont classées dans l'ordre chronologique décroissant.

Les informations suivantes sont proposées pour chaque entrée :

- numéro de téléphone dont l'événement a été bloqué par l'Anti-Spam ;
- date du blocage ;
- heure du blocage.

*Pour visualiser les informations sur les appels et SMS bloqués, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Spam**.
2. Sélectionnez **Mode : <mode actuel du composant>**.

   L'écran **Anti-Spam** s'ouvre.
3. Dans le groupe **Avancé**, choisissez l'option **Journal d'événements**.

L'écran **Journal Anti-Spam** s'ouvre.

*Pour visualiser les informations détaillées concernant les événements bloqués,*

sélectionnez l'entrée nécessaire dans le journal.

# 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



## A PROPOS DU COMPOSANT ANTIVOL

L'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 informations suivantes stockées sur l'appareil : les entrées dans les Contacts et sur la carte SIM, les SMS, le journal des appels, le calendrier, les paramètres de connexion à Internet, les comptes d'utilisateurs (excepté le compte Google™), ainsi que les fichiers de la liste des dossiers à supprimer.

  Kaspersky Endpoint Security 8 for Smartphone supprime les contacts de la carte SIM sur les appareils doté de la version 2.0 ou supérieure uniquement du système d'exploitation Android.

- **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 spécifiée.
- **Localisation** : 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.

Après l'installation de Kaspersky Endpoint Security 8 for Smartphone, toutes les fonctions de l'Antivol sont désactivées.

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 lancer la fonction Antivol à distance, vous devez connaître le code secret de l'application saisi lors du premier lancement de Kaspersky Endpoint Security 8 for Smartphone sur l'appareil ayant reçu l'instruction SMS.

L'état actuel de chaque fonction s'affiche sur l'écran principal dans le groupe **Antivol** à côté du nom de la fonction correspondante.

# 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 que la fonction Verrouillage fonctionne, l'application Kaspersky Endpoint Security 8 for Smartphone doit être installée comme écran principal par défaut.

Si l'application n'est pas installée comme écran principal par défaut, il est impossible de garantir la protection de l'appareil en cas de déclenchement de la fonction Verrouillage. Pour installer Kaspersky Endpoint Security 8 for Smartphone en tant qu'écran principal, il faut d'abord supprimer les paramètres de configuration pour l'écran par défaut actuel.

*Pour activer la fonction de verrouillage, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **Verrouillage** : **<état actuel de la fonction>**.

   L'écran **Verrouillage** s'ouvre.
3. Cochez la case **Activer le verrouillage**.
4. Dans le champ **Texte en cas de verrouillage**, modifiez le message qui apparaîtra sur l'écran d'un autre appareil (cf. ill. ci-après). Un texte standard est utilisé par défaut. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

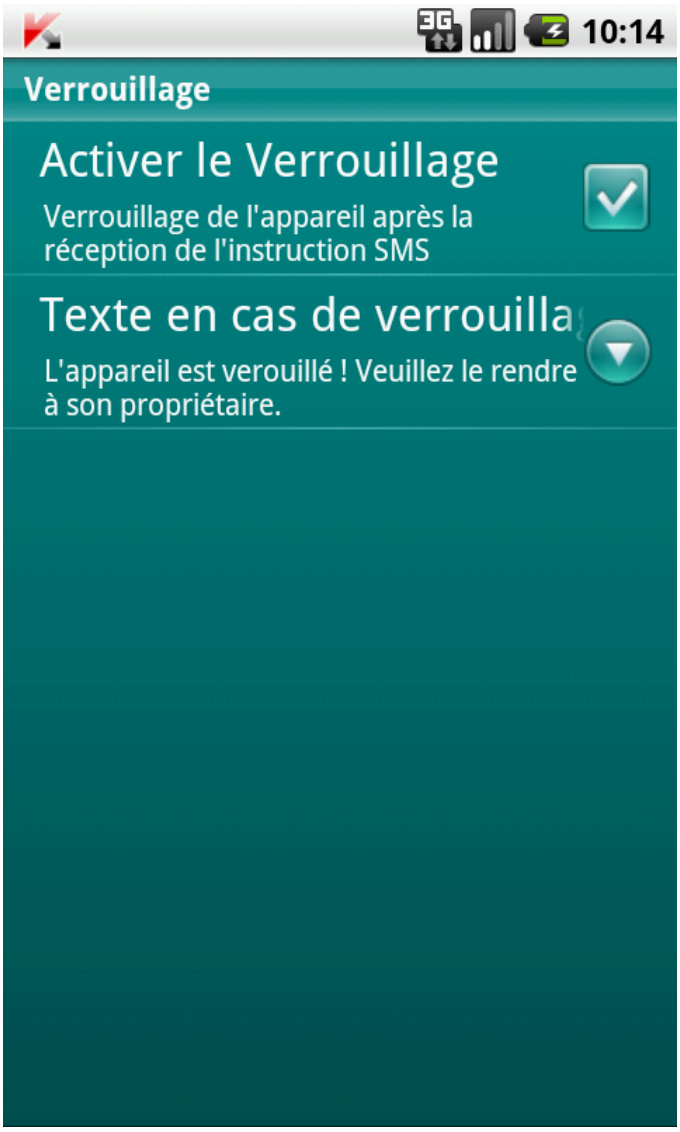


*Figure 22: paramètres de la fonction Verrouillage*

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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.
2. Choisissez l'option **Envoi d'une instr. SMS**.
3. Sélectionnez pour le paramètre **Instruction SMS** la valeur **Verrouillage**.
4. Dans le champ, entrez le **Numéro de téléphone recevant l'instruction SMS**, le numéro de téléphone de l'appareil qui a reçu l'instruction SMS.
5. Dans le champ, entrez le **Code secret de l'appareil recevant l'instruction SMS**, le code secret de l'application, reçu via l'instruction SMS de l'appareil.
6. Appuyez sur **Envoyer**.

*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 :

- Les données personnelles de l'utilisateur (entrées dans Contacts et sur la carte SIM, SMS, journal des appels, calendrier, paramètres de connexion Internet, comptes utilisateurs excepté celui de Google™) ;
- Fichiers de la liste des dossiers à supprimer, sauvegardés dans la carte mémoire (cf. section Création de la liste des dossiers à supprimer à la page 60).

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

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **Suppression** : **<état actuel de la fonction>**.

   L'écran **Suppression** s'ouvre.
3. Cochez la case **Activer la suppression de données**.
4. Sélectionnez les informations à supprimer. Pour ce faire, dans le groupe **Informations supprimées**, cochez les cases en regard des paramètres requis (cf. ill. ci-après) :
   - Pour supprimer les données personnelles, cochez la case **Données personnelles** ;
   - pour supprimer les fichiers de la liste des dossiers à supprimer, cochez la case **Dossiers** et allez à création d'une liste de dossiers à supprimer (cf. section Création d'une liste des dossiers supprimés à la page 60).


*Figure 23: paramètres de la fonction de suppression de données*

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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez **Envoi d'une instr. SMS**.
3. Sélectionnez pour le paramètre **Instruction SMS**, la valeur **Suppression**.
4. Dans le champ, entrez le **Numéro de téléphone recevant l'instruction SMS**, le numéro de téléphone de l'appareil qui a reçu l'instruction SMS.
5. Dans le champ, entrez le **Code secret de l'appareil recevant l'instruction SMS**, le code secret de l'application, reçu via l'instruction SMS de l'appareil.
6. Appuyez sur **Envoyer**.

*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. Vous pouvez sélectionner des dossiers qui se trouvent sur une carte mémoire.

Pour que l'Antivol supprime les dossiers de la liste après la réception de l'instruction spéciale par SMS, assurez-vous que la case **Dossiers** est cochée dans les paramètres de la fonction Suppression de données.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **Suppression**.

   L'écran **Suppression** s'ouvre.

3. Cliquez sur **Ajouter un dossier** (cf. ill. ci-après).

   L'écran **Sélection du dossier** s'ouvre.

4. Sélectionnez le dossier nécessaire en cliquant droit sur le nom du dossier.

   Le dossier sera ajouté à la liste des dossiers à supprimer, qui se trouve sous le paramètre **Dossiers**.


*Figure 24: ajout d'un dossier*

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **Suppression**.

   L'écran **Suppression** s'ouvre.

3. Passez à la liste des dossiers à supprimer.
4. Sélectionnez le dossier dans la liste et cliquez sur **Supprimer** dans le menu contextuel.

   Le dossier sera supprimé de la liste des dossiers à supprimer.

# 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **SIM-Surveill.** : **<état actuel du composant>**.

   L'écran **SIM-Surveillance** s'ouvre.
3. Cochez la case **Activer SIM-Surveillance**.
4. Pour contrôler le remplacement de la carte SIM sur l'appareil, configurez les paramètres suivants (cf. ill. ci-dessous) :
   - Pour recevoir automatiquement un SMS avec votre nouveau numéro de téléphone, dans le groupe **Envoi du nouveau numéro** pour le paramètre **Numéro de téléphone**, entrez le numéro de téléphone qui sera envoyé par SMS.

     Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres.
   - Pour recevoir un courrier électronique avec votre nouveau numéro de téléphone, dans le groupe **Envoi du nouveau numéro** pour le paramètre **Adresse du courr. élec.**, entrez l'adresse du courrier électronique.

- Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, dans le group **Verrouillage** cochez la case **Verrouiller**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.
- Pour que le message s'affiche à l'écran en mode verrouillage, saisissez dans le group **Verrouillage** pour le paramètre **Texte en cas de verrouillage**, entrez un nouveau texte.

  Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

  Le paramètre est accessible si la case **Verrouiller** est installée.


*Figure 25: paramètres de la fonction SIM-Surveillance*

# 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.

Si l'appareil est doté d'un récepteur GPS, il est activé automatiquement à la réception de l'instruction SMS spéciale. Si la fonction Localisation ne peut pas recevoir les coordonnées de l'appareil à l'aide de GPS, elle définit les coordonnées approximatives de l'appareil selon les stations de base.

*Pour activer la fonction Localisation, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Antivol**.
2. Cliquez sur **Localisation**: **<état actuel du composant>**.

   L'écran **Localisation** s'ouvre.
3. Cochez la case **Activer la Localisation**.

   A réception d'une instruction spécifique SMS, Kaspersky Endpoint Security 8 for Smartphone envoie automatiquement les coordonnées de l'appareil dans la réponse SMS au numéro d'où l'instruction SMS a été envoyée.
4. Pour recevoir également les coordonnées de l'appareil via un courrier électronique, dans le group **Envoi des coordonnées de l'app.** pour le paramètre **Adresse du courr. élec.**, entrez l'adresse du courrier électronique (cf. ill. ci-après).

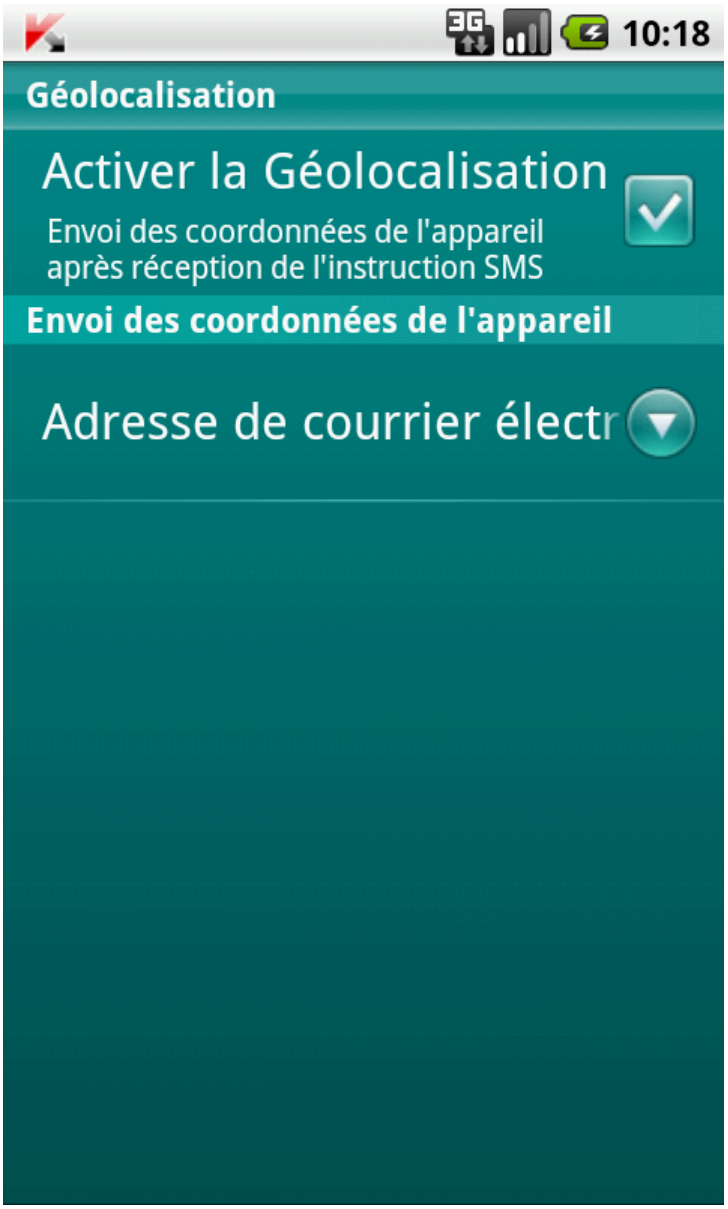


*Figure 26: paramètres de la fonction Localisation*

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.
2. Cliquez sur **Envoi d'une instr. SMS**.
3. Sélectionnez pour le paramètre **Instruction SMS**, la valeur **Localisation**.
4. Dans le champ, entrez le **Numéro de téléphone recevant l'instruction SMS**, le numéro de téléphone de l'appareil qui a reçu l'instruction SMS.
5. Dans le champ, entrez le **Code secret de l'appareil recevant l'instruction SMS**, le code secret de l'application, reçu via l'instruction SMS de l'appareil.
6. Appuyez sur **Envoyer**.

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

envoyez à un autre appareil un SMS contenant le texte `find:<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.

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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.
2. Sélectionnez la fonction à lancer à distance sur un autre appareil mobile. Sélectionnez une des valeurs proposées pour le paramètre **Instruction SMS** (cf. ill. ci-après) :
   - **Verrouillage** ;
   - **Suppression** ;
   - **Localisation** ;
   - **Dissimulation des infos**.

3. Dans le champ, entrez le **Numéro de téléphone recevant l'instruction SMS**, le numéro de téléphone de l'appareil qui a reçu l'instruction SMS.
4. Dans le champ, entrez le **Code secret de l'appareil recevant l'instruction SMS**, le code secret de l'application, reçu via l'instruction SMS de l'appareil.
5. Appuyez sur **Envoyer**.

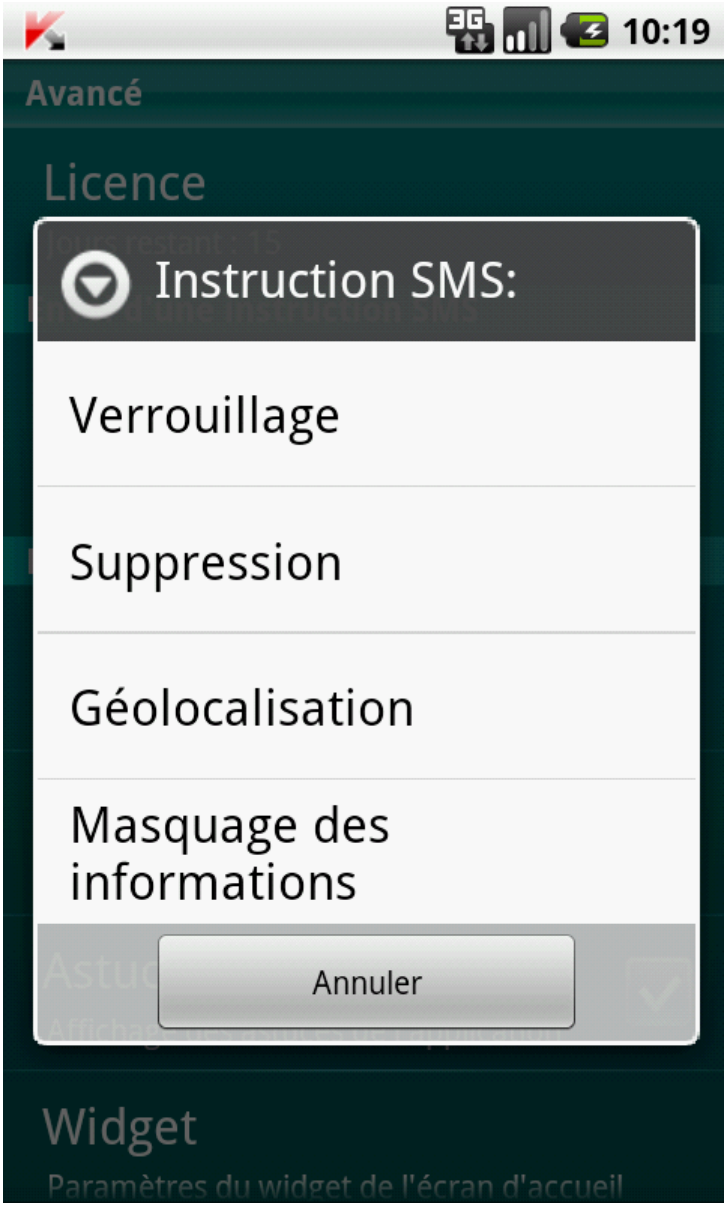


*Figure 27 : lancement à distance de la fonction Antivol et des Contacts personnels*

# 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.

## 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.

La dissimulation est désactivée par défaut.

Les modes suivants sont prévus pour Contacts personnels :

- **Les informations confidentielles sont affichées** : le masque des informations confidentielles est désactivé. Les paramètres de Contacts personnels peuvent être modifiés.
- **Les informations confidentielles sont masquées** : le masque des informations confidentielles est activé. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique de la dissimulation des données personnelles (cf. section "Activation automatique de Contacts personnels" à la page 69) ou son activation à distance depuis un autre appareil (cf. section "Activation de la dissimulation des informations confidentielles à distance" à la page 71).

Le mode actuel du masque des informations confidentielles s'affiche sur l'écran principal de l'application, dans le groupe **Contacts personnels**.

# ACTIVATION/DESACTIVATION DE CONTACTS PERSONNELS

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Contacts personnels**.
2. Cliquez sur **Masquer les info** (cf. ill. ci-après).

   La valeur du point dépend du mode des Contacts personnels. Si le mode **Les informations confidentielles sont affichées** s'affiche, alors le point s'appelle **Masquer les infos**. Si le mode **Les informations confidentielles sont masquées** s'affiche, alors le point s'appelle **Afficher les infos**.

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

Le mode actuel Contacts personnels s'affiche dans le group **Contacts personnels**.

Le signe du commutateur à droite du point **Masquer les infos** / **Afficher les infos** sera modifié en fonction du mode sélectionné.


*Figure 28: modification du mode de Contacts personnels*

# ACTIVATION AUTOMATIQUE DE CONTACTS PERSONNELS

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 personnelles 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Contacts personnels**.
2. Cliquez sur **Paramètres**.

   L'écran **Paramètres Contacts personnels** s'ouvre.

3. Choisissez la valeur pour le paramètre **Dissimulation automatique** dépend des tâches suivantes (cf. ill. ci-après) :
   - Pour désactiver l'activation automatique du masque des informations confidentielles, sélectionnez **Désactivé**.
   - Pour que le masque les informations confidentielles soit activé après le passage de l'appareil en mode Economiseur d'énergie, choisissez l'une des valeurs, comme suit :
     - **Sans délai**.
     - **Dans 1 minute**.
     - **Dans 5 minutes**.
     - **Dans 10 minutes**.
     - **Dans 15 minutes**.
     - **Dans 30 minutes**.

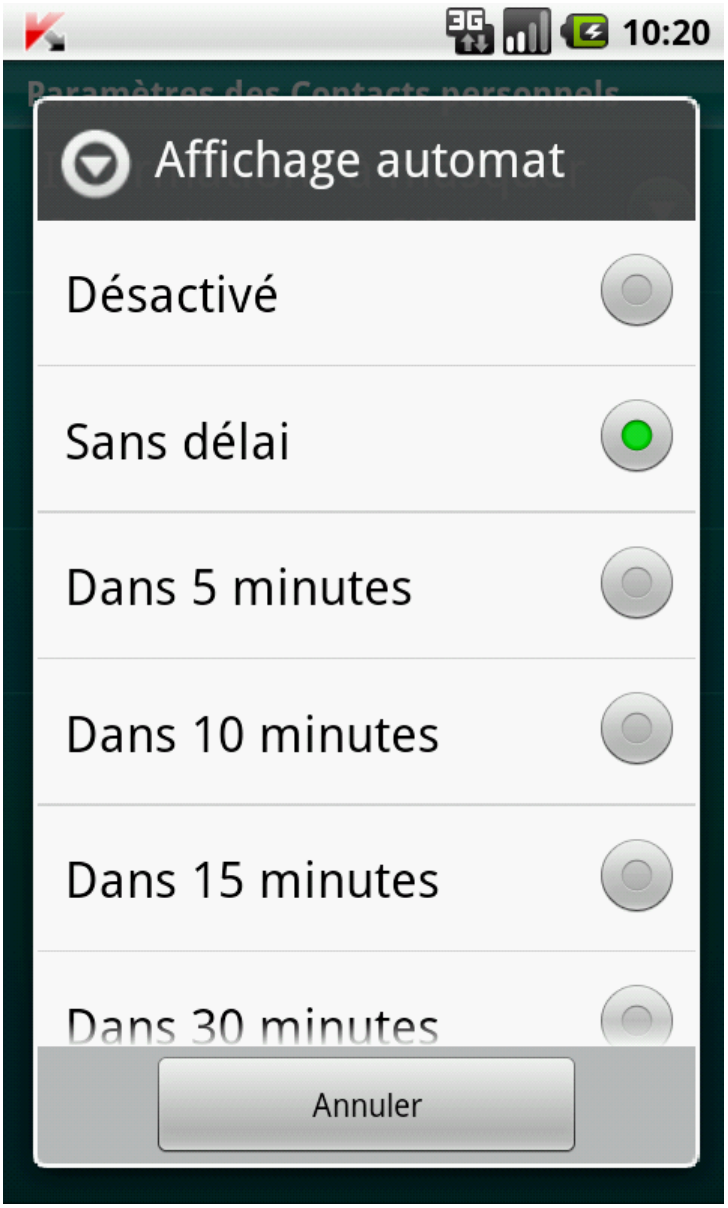


*Figure 29: paramètres de lancement automatique de Contacts personnels*

# 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Contacts personnels**.
2. Cliquez sur **Paramètres**.

   L'écran **Paramètres Contacts personnels** s'ouvre.
3. Cochez la case **Masquer sur instruction SMS** (cf. ill. ci-après).


*Figure 30 : paramètres d'activation à distance du composant Contacts personnels*

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 le masque des informations confidentielles depuis un autre appareil mobile à l'aide de l'instruction SMS, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.
2. L'écran **Avancé** s'ouvre.
3. Sélectionnez **Envoi d'une instr. SMS**.
4. Sélectionnez pour le paramètre **Instruction SMS**, la valeur **Dissimulation des infos**.
5. Dans le champ, entrez le **Numéro de téléphone recevant l'instruction SMS**, le numéro de téléphone de l'appareil qui a reçu l'instruction SMS.
6. Dans le champ, entrez le **Code secret de l'appareil recevant l'instruction SMS**, le code secret de l'application, reçu via l'instruction SMS de l'appareil.
7. Appuyez sur **Envoyer**.

Lorsque l'appareil recevra l'instruction SMS, Kaspersky Endpoint Security 8 for Smartphone activera le masque des informations confidentielles, et les informations sur l'appareil seront masquées.

*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.

# 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 personnelles 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone déployez le group **Contacts personnels**.
2. Cliquez sur **Paramètres**.

   L'écran **Paramètres Contacts personnels** s'ouvre (cf. ill. ci-après).
3. Choisissez les informations et les événements qui seront masqués pour les numéros confidentiels. Pour ce faire, choisissez **Informations masquées** et cochez la case sous les paramètres. Les paramètres suivants sont prévus:
   - **Contacts :** masque toutes les informations relatives aux numéros confidentiels.
   - **Histoire SMS** : masque les SMS dans les dossiers **Entrant**, **Sortant**, **Transmis** pour les numéros confidentiels.
   - **SMS entrant** : masque le SMS en provenance des numéros confidentiels.
   - **Histoire 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.

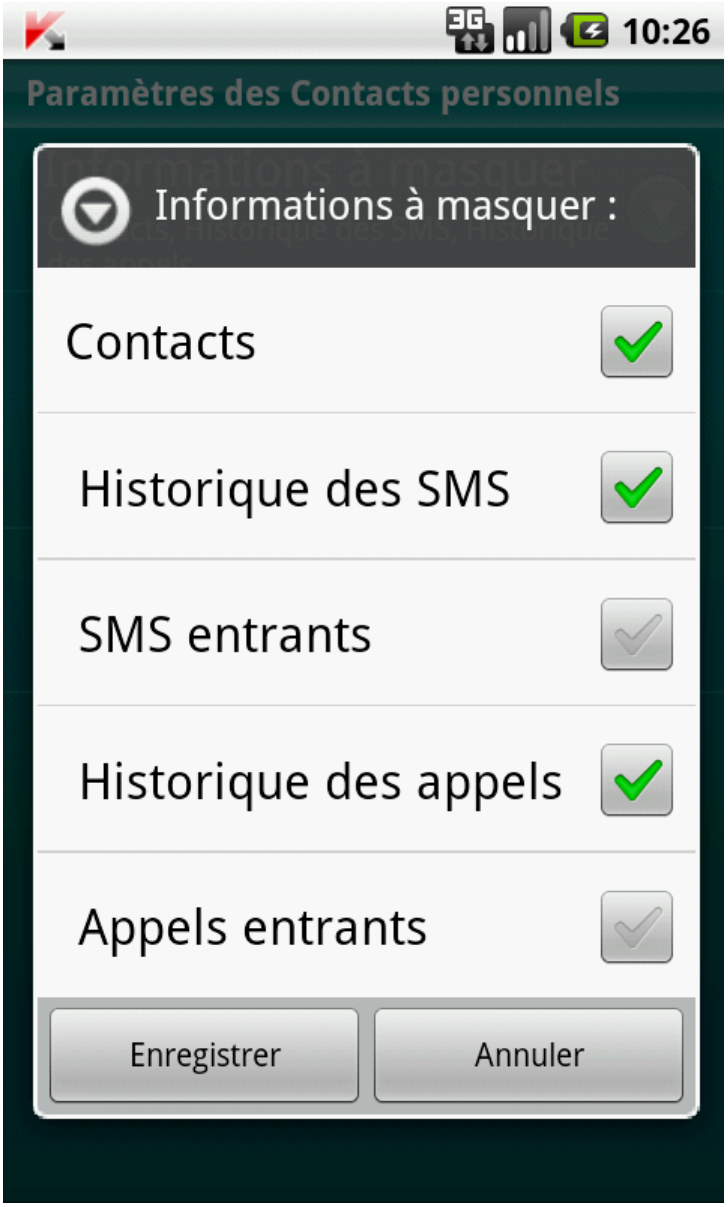


*Figure 31 : sélection des informations et des événements masqués*

# 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

Dans la Liste des contacts, vous pouvez ajouter des numéros de téléphone ou les importer depuis les Contacts.

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

*Pour ajouter un numéro de téléphone à la Liste de contacts, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Contacts personnels**.
2. Cliquez sur **Liste des contacts**.

   L'écran **Liste des contacts** apparaît.
3. Exécutez l'une des opérations suivantes (cf. ill. ci-après) :
   - Pour ajouter un numéro depuis les Contacts, cliquez sur **Ajouter** → **Contact**. Sur l'écran ouvert, sélectionnez l'entrée nécessaire dans la liste des Contacts.
   - Pour ajouter un numéro, cliquez sur **Ajouter** → **Numéro de téléphone**, remplissez le champ **Numéro de téléphone** et cliquez sur **Enregistrer**.

Le numéro est alors ajouté à la liste des contacts.

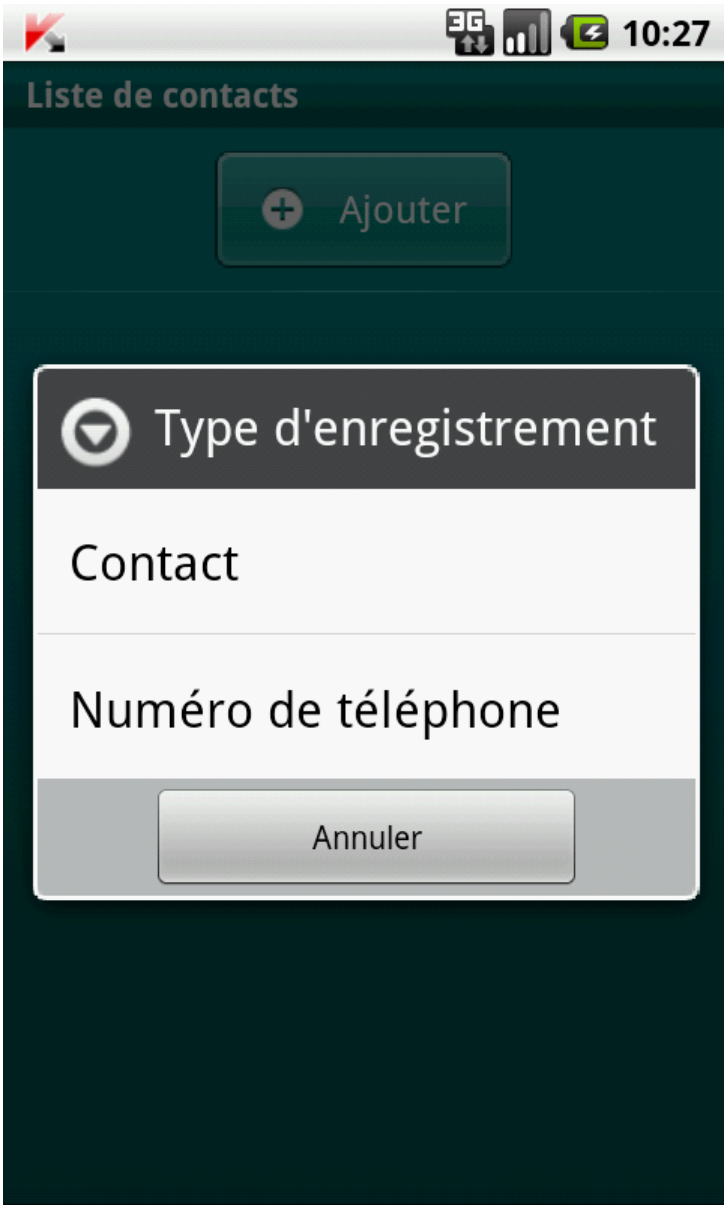


*Figure 32: ajout d'un enregistrement à la liste des contacts protégés*

# MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

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

Seuls les numéros qui ont été saisis manuellement dans la Liste des contacts peuvent être modifiés. Impossible de modifier le numéro sélectionné à depuis Contacts.

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

  1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Contacts personnels**.
  2. Cliquez sur **Liste des contacts**.

     L'écran **Liste des contacts** apparaît.
  3. Choisissez un numéro à modifier dans la Liste des contacts et sélectionnez **Modifier** dans le menu contextuel.

     L'écran **Modification d'entrée** s'ouvre.
  4. Modifiez les données.
  5. Appuyez sur **Enregistrer** une fois les modifications terminées.

Le numéro sera modifié.

# SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

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

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

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

  1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone déployez le group **Contacts personnels**.
  2. Cliquez sur **Liste des contacts**.

     L'écran **Liste des contacts** apparaît.
  3. Choisissez le numéro à supprimer et dans le menu contextuel, sélectionnez **Supprimer**.
- *Pour purger la Liste de contacts, procédez comme suit :*

  1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone déployez le group **Contacts personnels**.
  2. Cliquez sur **Liste des contacts**.

     L'écran **Liste des contacts** apparaît.
  3. Sélectionnez dans le menu contextuel **Supprimer tout**.

     La fenêtre de confirmation s'ouvre.
  4. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

# 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.

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.

Les informations détaillées sur les bases des données antivirales utilisées sont disponibles dans le group **Anti-Virus** → **Avancé** dans le point **Lancer la mise à jour**.

# LANCEMENT MANUEL DE LA MISE A JOUR

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

*Pour lancer manuellement la mise à jour des bases manuellement, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Cliquez sur **Lancer de la mise à jour**.

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. 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 configurer la mise à jour automatique si vous vous trouvez dans la zone itinérante.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Anti-Virus**.
2. Cliquez sur **Avancé**.

   L'écran **Anti-Virus : avancé** s'ouvre.
3. Sélectionnez le point **Mise à jour automatique**.

   L'écran **Mise à jour automatique** s'ouvre.
4. Installez pour le paramètre **Mise à jour programmée**, l'une des tâches suivantes :
   - **Une fois/sem.** : les bases de l'application sont actualisées une fois par semaine. Sélectionnez l'une des valeurs pour les paramètres **Jour de lancem.** et **Heure de début**.
   - **Une fois**/j. : les bases de l'application sont actualisées quotidiennement. Saisissez la valeur pour le paramètre **Heure de début**.
   - **Désactivé** : ne pas mettre à jour les bases de l'application à la demande.

# CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

Les informations suivantes sur les possibilités additionnelles de Kaspersky Endpoint Security 8 for Smartphone sont disponibles : comment activer / désactiver les notifications sur le travail de l'application dans la barre d'état, notification sonore, affichage des conseils avant la configuration de chaque composant, comment configurer les paramètres du gadget de l'écran principal et comment modifier le code secret de l'application.

### DANS CETTE SECTION



## MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret de l'application défini après activation de l'application.

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

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez **Modification du code secret**.
3. Saisir le code secret actuel de l'application dans le champ **Saisissez le code secret** et cliquez sur **Suivant**.
4. Saisir le code secret actuel de l'application dans le champ **Saisissez le nouveau code secret** et cliquez sur **Suivant**.

   La robustesse du code saisi est vérifiée automatiquement.

   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**. Répétez la saisie du code secret de l'application.

5. Saisir ce code une nouvelle fois, dans le champ **Ressaisissez le nouveau code**.

   Le code secret sera changé.

## 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. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Exécutez les actions en fonction des tâches, comme suit :

   - Pour activer l'affichage des conseils, cochez la case **Astuces**.
   - Pour désactiver l'affichage des conseils, décochez la case **Astuces**.

# ADMINISTRATION DES NOTIFICATIONS SONORES

Après exécution de l'application, des événements surviennent, par exemple, un fichier infecté a été découvert, la validité de la licence a expiré. 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.

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

1. Développez le groupe **Avancé** sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone.

   L'écran **Avancé** s'ouvre.

2. Exécutez les actions en fonction des tâches, comme suit :

   - Pour activer la notification sonore, cochez la case **Son**.
   - Pour désactiver la notification sonore, décochez la case **Son**.

# NOTIFICATION DE L'ETAT

Kaspersky Endpoint Security 8 for Smartphone permet de recevoir des notifications pop-up dans la barre d'état concernant les événements de l'application, le lancement du programme, l'expiration de la validité de la licence ou la désactivation de la Protection. Vous pouvez activer / désactiver la réception des notifications sur les événements de l'application dans la barre d'état.

*Pour administrer les notifications pop-up dans l'application, procédez comme suit :*

1. Sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone, développez le groupe **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Exécutez les actions en fonction des tâches, comme suit :

   - Pour activer les pop-ups dans l'application, cochez la case **Notifications**.
   - Pour désactiver les pop-up, décochez la case **Notifications**.

Dans le cadre de l'utilisation de Kaspersky Endpoint Security 8 for Smartphone, vous avez accès au widget de l'écran principal (à la page 30). Le widget de l'écran principal vise à fournir des informations sur l'état de la licence de l'application, de la protection de l'appareil et du masquage des informations confidentielles.

Après l'installation de l'application, le gadget apparaît automatiquement sur l'écran principal de l'appareil. Vous pouvez ajouter un gadget sur l'écran principal ou le supprimer ainsi que configurer l'indication de masque informations confidentielles dans le gadget de l'écran principal (cf. section Masques des informations confidentielles à la page 67).

*Pour administrer l'affichage du gadget sur l'écran principal, procédez comme suit :*

1. Développez le groupe **Avancé** sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone.

   L'écran **Avancé** s'ouvre.

2. Choisissez le point **Gadget logiciel**.

   L'écran **Gadget de l'écran principal** s'ouvre (cf. ill. ci-après).

3. Exécutez les actions en fonction des tâches, comme suit :

   - Pour ajouter un gadget sur l'écran principal, cochez la case **Activer le gadget**.
   - Pour supprimer le gadget de l'écran principal, décochez la case **Activer le gadget**.

*Pour configurer l'indication de l'état des informations confidentielles sur le gadget de l'écran principal, procédez comme suit :*

1. Développez le groupe **Avancé** sur l'écran principal de Kaspersky Endpoint Security 8 for Smartphone.

   L'écran **Avancé** s'ouvre.

2. Choisissez le point **Gadget logiciel**.

   L'écran **Gadget de l'écran principal** s'ouvre.

3. Exécutez les actions en fonction des tâches, comme suit :

   - Pour afficher la modification du mode de masquage des informations confidentielles sur le gadget de la fenêtre principale, cochez la case **Afficher l'état des Contacts personnels**.
   - Pour masquer la modification du mode de masquage des informations confidentielles sur le gadget de la fenêtre principale, décochez la case **Afficher l'état des Contacts personnels**.

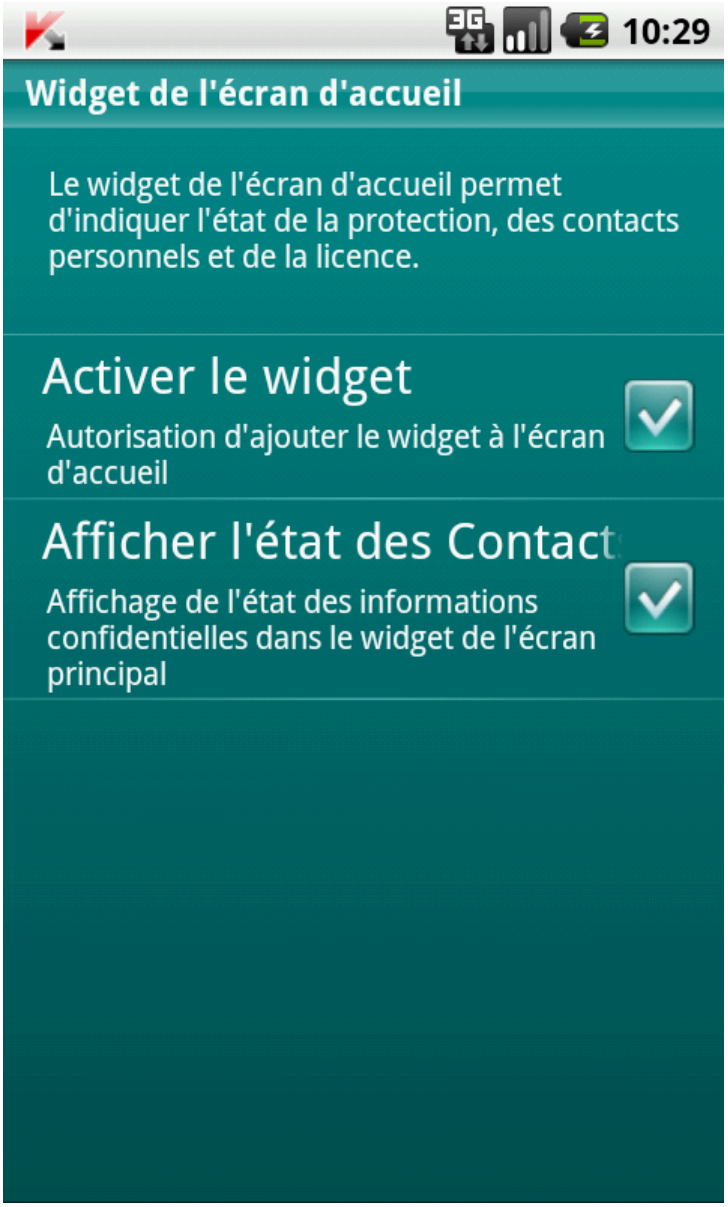


*Figure 33 : paramètres du gadget de l'écran principal*

# GLOSSAIRE

## A

### ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'utilisateur doit avoir une licence pour activer l'application.

### 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.

## 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 envoyer une instruction SMS depuis un autre appareil mobile pour activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Localisation, Contacts personnels.

## 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 DE 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.

## 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.

## S

### SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des 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. Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

# KASPERSKY LAB

Kaspersky Lab a vu le jour en 1997. 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 société 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<br>(envoi uniquement d'objets suspects sous forme d'archive)<br>http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr<br>(pour les questions aux experts antivirus) |

# INFORMATIONS SUR LE CODE TIERS

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

### DANS CETTE SECTION



## CODE DE PROGRAMMATION DIFFUSE

Le programme contient un code de programmation indépendant appartenant à d'autres éditeurs au format source ou binaire sans modification.

### DANS CETTE SECTION



## ADB

**Copyright (C) 2005-2008, The Android Open Source Project**

---

Distributed under the terms of the Apache License, version 2.0 of the License

## ADBWINAPI.DLL

**Copyright (C) 2005-2008, The Android Open Source Project**

---

Distributed under the terms of the Apache License, version 2.0 of the License

## ADBWINUSBAPI.DLL

**Copyright (C) 2005-2008, The Android Open Source Project**

---

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any

additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

# AUTRES INFORMATIONS

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique dans Kaspersky Endpoint Security 8 for Smartphone.

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

# INDEX

## A



## C



## D

## V