

Kaspersky Endpoint Security 8 for Smartphone

pour BlackBerry® OS

KASPERSKY **lab**

Guide de l'utilisateur

VERSION DE L'APPLICATION : 8.0

Cher utilisateur,

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

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

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

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

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

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

Date d'édition : 09/02/12

© 2012 Kaspersky Lab ZAO. Tous droits réservés.

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

TABLE DES MATIERES

A PROPOS DE CE MANUEL.....	5
SOURCES D'INFORMATIONS COMPLEMENTAIRES	6
Sources de données pour des consultations indépendantes	6
Publier des messages sur le forum de Kaspersky Lab	7
Contacter l'Equipe de rédaction de la documentation.....	7
KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE	8
CONFIGURATION LOGICIELLE ET MATERIELLE	9
INSTALLATION DE KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE	10
Sur l'installation de l'application via le poste de travail	10
Installation de l'application via le poste de travail	11
Sur l'installation de l'application après la réception d'un message électronique	13
Installation de l'application après la réception d'un message électronique.....	13
ADMINISTRATION DES PARAMETRES DE L'APPLICATION	16
SUPPRESSION DE L'APPLICATION	17
GESTION DE LA LICENCE	18
Présentation des licences de Kaspersky Endpoint Security 8 for Smartphone.....	18
Installation d'une licence.....	19
Affichage des informations de licence	19
SYNCHRONISATION DE L'APPAREIL AVEC LE SYSTEME D'ADMINISTRATION DISTANTE.....	20
Lancement de la synchronisation à la main.....	21
Modification des paramètres de synchronisation.....	22
PREMIERS PAS	24
Démarrage du logiciel.....	24
Saisie du code secret	25
Informations sur le programme.....	25
INTERFACE DE L'APPLICATION.....	26
Onglets de l'application.....	26
Fenêtre d'état de la protection	27
FILTRAGE DES APPELS ET DES SMS ENTRANTS	29
Présentation du Filtre des appels et des SMS	29
Présentation des modes du Filtre des appels et des SMS	30
Modification du mode du Filtre des appels et des SMS	31
Composition de la liste noire.....	31
Ajout d'un enregistrement à la liste noire	32
Modification d'un enregistrement de la liste noire	33
Suppression d'un enregistrement de la liste blanche.....	34
Composition de la liste blanche	35
Ajout d'un enregistrement à la liste blanche.....	36
Modification d'un enregistrement de la liste blanche.....	37
Suppression d'un enregistrement de la liste blanche.....	38
Réaction aux SMS et appels de contacts qui ne figurent pas dans le répertoire téléphonique	39

Réaction aux SMS en provenance de numéros sans chiffres	40
Sélection de l'action à appliquer sur les SMS entrants	42
Sélection de l'action à appliquer sur des appels entrants	43
PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL	44
A propos du module Antivol	44
Verrouillage de l'appareil	45
Suppression de données personnelles.....	47
Composition de la liste des dossiers à supprimer.....	49
Contrôle du remplacement de la carte SIM sur l'appareil	50
Détermination des coordonnées géographiques de l'appareil	51
Lancement à distance de la fonction Antivol.....	53
JOURNAUX DU LOGICIEL.....	55
À propos des journaux.....	55
Affichage des événements du journal.....	55
Suppression des enregistrements du journal.....	55
CONFIGURATION DES PARAMETRES COMPLEMENTAIRES	56
Modification du code secret	56
Affichage des astuces	57
GLOSSAIRE	58
KASPERSKY LAB ZAO	60
INFORMATIONS SUR LE CODE TIERS	62
NOTIFICATIONS SUR LES MARQUES DE COMMERCE	63
INDEX	64

A PROPOS DE CE MANUEL

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

Buts du document :

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

SOURCES D'INFORMATIONS COMPLEMENTAIRES

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

DANS CETTE SECTION

Sources de données pour des consultations indépendantes	6
Publier des messages sur le forum de Kaspersky Lab	7
Contacteur l'Equipe de rédaction de la documentation	7

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

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

Page sur le site Web de Kaspersky Lab

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

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

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

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

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

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de

Kaspersky Endpoint Security 8 for Smartphone. Ces articles sont regroupés par sujet, par exemple "Utilisation des fichiers de licence", "Mise à jour des bases" ou "Élimination des échecs". Les articles répondent non seulement à des questions sur Kaspersky Endpoint Security 8 for Smartphone, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

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

PUBLIER DES MESSAGES SUR LE FORUM DE KASPERSKY LAB

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

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

CONTACTER L'ÉQUIPE DE RÉDACTION DE LA DOCUMENTATION

Si vous avez des questions concernant la documentation, ou vous y avez trouvé une erreur, ou vous voulez laisser un commentaire sur nos documents, vous pouvez contacter les spécialistes du Groupe de rédaction de la documentation pour les utilisateurs. Pour contacter l'Équipe de rédaction de la documentation, envoyez un message à docfeedback@kaspersky.com. Dans le champ d'objet, saisissez "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 tournant sous SE BlackBerry®. L'application permet de contrôler des messages SMS et des appels entrants, et protéger les informations de l'appareil en cas de perte ou de vol. Chaque type de menace est traité par un module distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier. L'installation de l'application, la configuration et la mise à jour des paramètres sont effectuées par l'administrateur via les systèmes d'administration distante.

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

- **Filtre des appels et des SMS.** Analyse tous les SMS et appels entrants à la recherche de spam. Le module permet de configurer en souplesse la fonction de blocage des SMS et des appels considérés comme indésirables.
- **Antivol** Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol tout en facilitant sa recherche. Antivol permet de verrouiller l'appareil à distance à l'aide des SMS, de supprimer les données qu'il contient et de déterminer ses coordonnées géographiques (si l'appareil mobile est doté d'un récepteur GPS). De plus, Antivol permet également de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.

De plus, l'application propose diverses fonctions de service. Elles permettent d'améliorer les fonctionnalités de l'application, ainsi que de guider les activités utilisateur :

- **État de la protection.** Les états des modules de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection des données stockées sur l'appareil.
- **Journal des événements.** Les informations sur le fonctionnement de chacun des modules (par exemple, lancement à distance de la fonction Antivol, message sur la durée de validité de la licence de l'application). Les rapports sur le fonctionnement des modules sont envoyés et stockés dans le système d'administration distante.
- **Suppression de l'application.** Pour empêcher l'accès aux informations protégées, la suppression de Kaspersky Endpoint Security 8 for Smartphone ne peut être effectuée que depuis l'interface de l'application.

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

CONFIGURATION LOGICIELLE ET MATERIELLE

Kaspersky Endpoint Security 8 for Smartphone peut être installé sur des appareils mobiles tournant sous BlackBerry 4.5, 4.6, 4.7, 5.0 et 6.0.

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. L'installation de l'application nécessite une intervention de l'utilisateur.

Pour installer l'application, 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 et décrit les types d'installation de l'application sur l'appareil mobile.

DANS CETTE SECTION

Sur l'installation de l'application via le poste de travail	10
Installation de l'application via le poste de travail	11
Sur l'installation de l'application après la réception d'un message électronique	13
Installation de l'application après la réception d'un message électronique	13

SUR L'INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

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

Pour une installation réussie, l'application BlackBerry Desktop Manager doit être installée sur le poste de travail.

INSTALLATION DE L'APPLICATION VIA LE POSTE DE TRAVAIL

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

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

► Pour installer l'application sur l'appareil mobile depuis le poste de travail, procédez comme suit :

1. Connectez l'appareil mobile au poste de travail à l'aide de BlackBerry Desktop Manager.

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

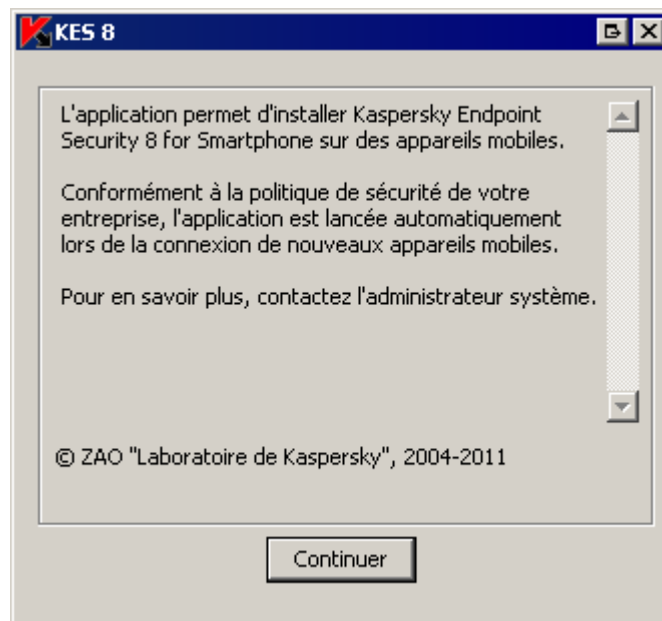


Figure 1: programme d'installation de Kaspersky Endpoint Security 8 for Smartphone

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

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

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

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

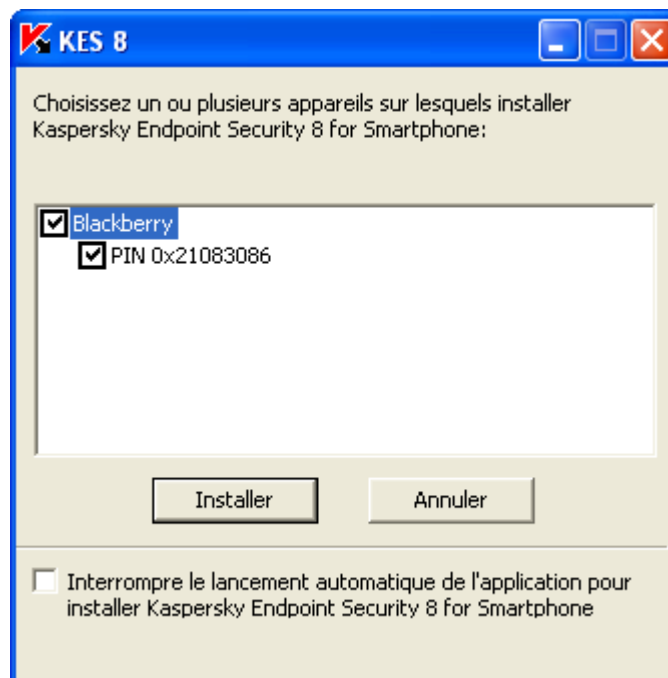


Figure 2: sélection des appareils pour installer Kaspersky Endpoint Security 8 for Smartphone

4. Cliquez sur **Installer**.

La fenêtre **Assistant de téléchargement de l'application** s'affiche. Après la transmission de la distribution, l'installation de l'application sur les appareils mobiles sélectionnés sera lancée automatiquement. Une fois l'installation terminée, cliquez dans la fenêtre **Assistant de téléchargement de l'application** sur **Fermer**.

L'état de la transmission sera affiché dans la fenêtre **KES 8.0** du poste de travail.

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**.

SUR 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

Si vous avez reçu un message électronique avec les paramètres d'installation, vous ne pouvez installer l'application que depuis l'appareil mobile. Dans ce cas, l'installation de Kaspersky Endpoint Security 8 for Smartphone depuis le poste de travail n'est pas prise en charge.

➤ 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.
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.

L'installation de l'application sera effectuée automatiquement et l'application sera installée sur l'appareil.
3. Lancez l'application (cf. la rubrique "Lancement de l'application" à la page [24](#)). Pour ce faire, sélectionnez **Menu** → **Téléchargement** → **KES 8** et lancez l'application avec la barre de défilement ou en sélectionnant **Menu** → **Ouvrir**.

4. Saisissez le code secret de l'application (cf. la rubrique "Saisie du code secret" à la page [24](#)). Pour ce faire, remplissez le champ **Saisissez le nouveau code**, puis le champ **Confirmation du code** et cliquez sur la touche **ENTRÉE**.

L'écran **Paramètres de synchronisation** s'ouvre.



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 **Votre adresse élec.** et cliquez sur **OK**.

L'adresse électronique est utilisée pour enregistrer l'appareil dans le système d'administration distante. N'oubliez pas qu'il est impossible de modifier l'adresse indiquée au moment de l'installation de l'application.

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

ADMINISTRATION DES PARAMETRES DE L'APPLICATION

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

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

Si en haut de l'écran de configuration du module un verrou et un message d'avertissement s'affichent, les paramètres de l'application 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 la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique "Lancement de la synchronisation à la main" à la page [20](#)).

SUPPRESSION DE L'APPLICATION

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

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

1. Sous l'onglet **Avancé**, sélectionnez l'option **Suppression de l'application** (cf. ill. ci-après).

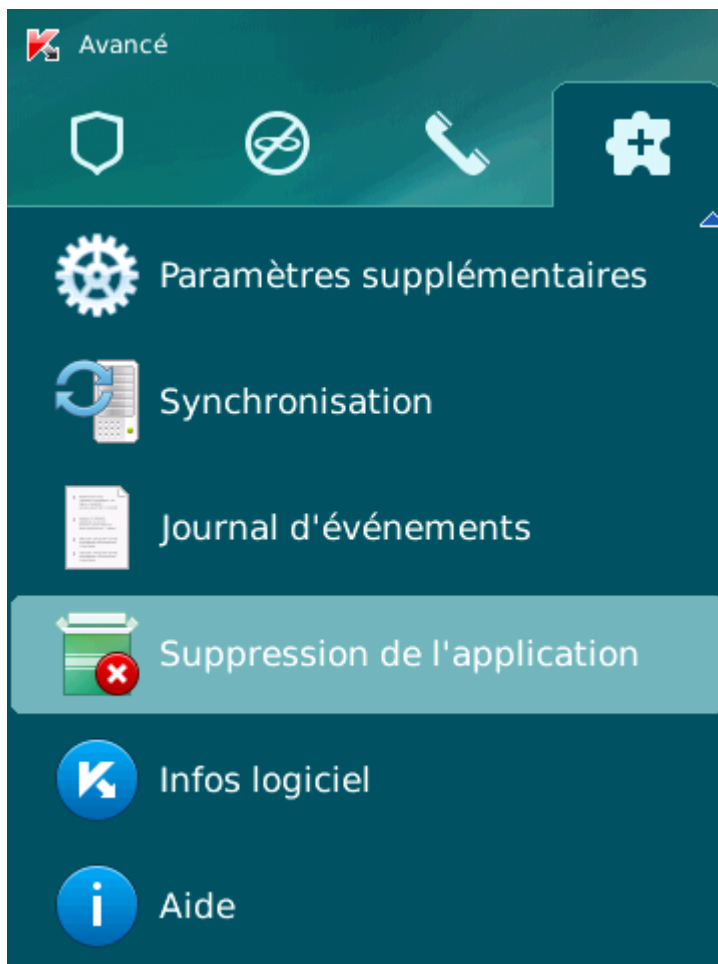


Figure 4: suppression de l'application

Une fenêtre de confirmation de la suppression de l'application s'affichera.

2. Confirmer la suppression de Kaspersky Endpoint Security 8 for Smartphone en cliquant sur **Oui**.

La suppression de l'application va commencer.

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

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

Présentation des licences de Kaspersky Endpoint Security 8 for Smartphone	18
Installation d'une licence	19
Affichage des informations de licence.....	19

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.

Durée de validité de la licence : période pendant laquelle vous pouvez bénéficier de l'assistance technique.

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 :

- 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. Dans ce mode vous pouvez :

- désactiver le module Antivol
- consulter le système d'aide ;
- synchronisation avec le système d'administration distante.

INSTALLATION D'UNE LICENCE

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

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

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

- désactiver tous les modules ;
- consulter le système d'aide.

Si la licence n'a pas été installée dans les trois jours qui suivent l'installation de l'application, pour installer la licence, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique "Lancement de la synchronisation à la main" à la page [20](#)).

AFFICHAGE DES INFORMATIONS DE LICENCE

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

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

1. Sélectionnez l'onglet **Avancé**.
2. Sélectionnez **Informations** dans l'onglet.

L'écran **Infos licence** s'ouvre.

SYNCHRONISATION DE L'APPAREIL AVEC LE SYSTEME D'ADMINISTRATION DISTANTE

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

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

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

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

En fonction du type de système d'administration distante, sélectionné par l'administrateur pour la gestion de l'application, l'utilisateur peut être invité à saisir les paramètres de connexion au système d'administration distante pendant l'installation de l'application. Dans ce cas, les valeurs que l'utilisateur a saisi à la main peuvent être modifiées depuis l'application (cf. la rubrique "Modification des paramètres de synchronisation" à la page [21](#)).

DANS CETTE SECTION

Lancement de la synchronisation à la main	20
Modification des paramètres de synchronisation	21

LANCEMENT DE LA SYNCHRONISATION A LA MAIN

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

1. Sélectionnez l'onglet **Avancé**.
2. Sélectionnez **Synchronisation** (cf. ill. ci-après).

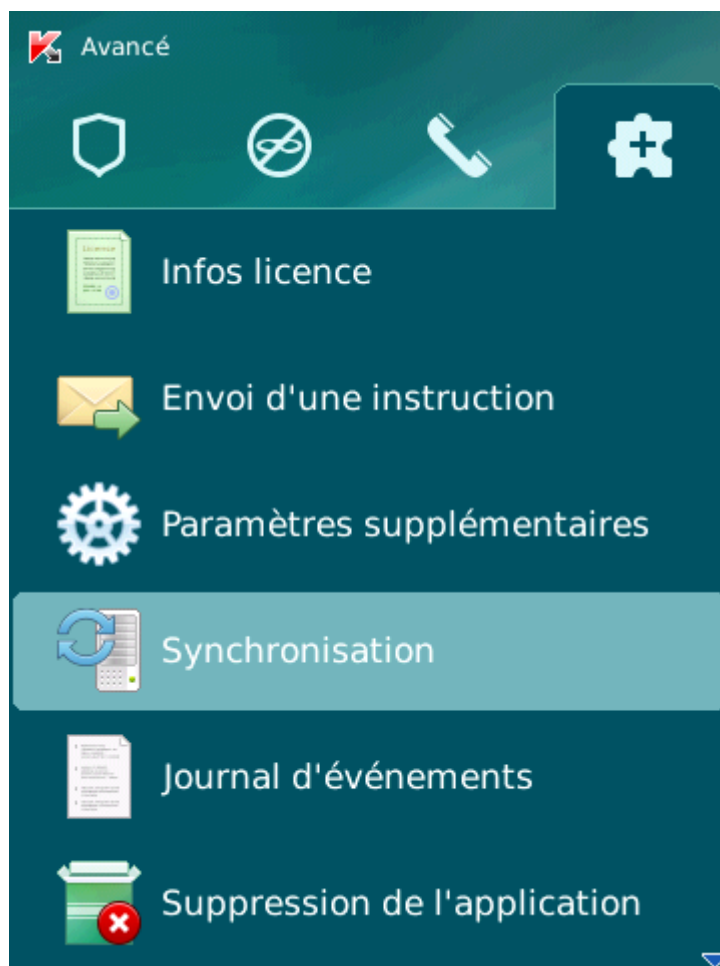


Figure 5: synchronisation à la main

Si l'utilisateur n'a pas été invité à saisir les paramètres de connexion au système d'administration distante, une fenêtre de confirmation de la connexion à Internet s'ouvrira sur l'écran. Pour autoriser la connexion, cliquer sur **Oui**. La connexion au système d'administration distante sera établie.

Si l'utilisateur a été invité à saisir les paramètres de connexion au système d'administration distante, le système affichera l'écran **Synchronisation**. Sélectionnez l'option **Lancement de la synchronisation**. La connexion au système d'administration distante sera établie.

MODIFICATION DES PARAMETRES DE SYNCHRONISATION

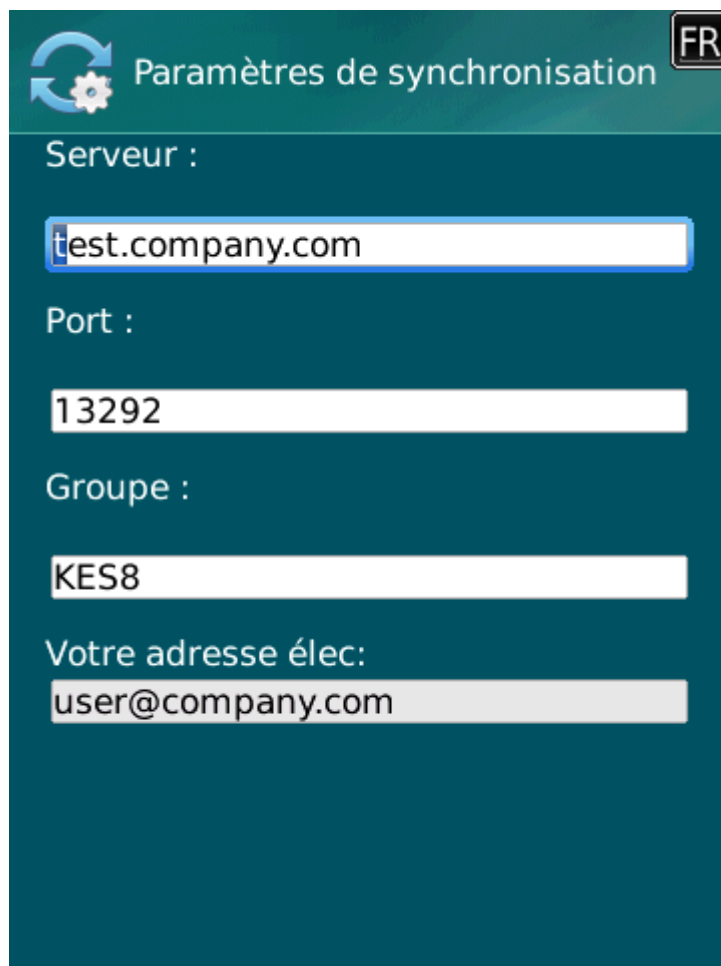
Il est déconseillé de modifier les paramètres de connexion au système d'administration distante sans être guidé par l'administrateur.

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

1. Sélectionnez l'onglet **Avancé**.
2. Sélectionnez l'option **Synchronisation**.

L'écran **Synchronisation** s'ouvre.

3. Sélectionnez l'option **Paramètres de synchronisation**.
4. Modifiez les valeurs aux paramètres suivants (cf. ill. ci-après) :
 - **Serveur** ;
 - **Port** ;
 - **Groupe**.



Paramètres de synchronisation FR

Serveur :

test.company.com

Port :

13292

Groupe :

KES8

Votre adresse élec:

user@company.com

Figure 6: modification des paramètres de synchronisation

5. Sélectionnez **Menu** → **Enregistrer**.

PREMIERS PAS

Cette section reprend les informations sur la première utilisation de Kaspersky Endpoint Security 8 for Smartphone : la saisie du code secret de l'application, le lancement de l'application et la consultation des informations qui la concernent.

DANS CETTE SECTION

Démarrage du logiciel	24
Saisie du code secret	24
Informations sur le programme	25

DEMARRAGE DU LOGICIEL

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

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

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

3. Lancez l'application. Pour ce faire, utilisez la barre de défilement ou sélectionnez **Menu** → **Ouvrir**.
4. Saisissez le code secret de l'application (cf. rubrique "Saisie du code secret" à la page [24](#)) et cliquez sur la touche **ENTRÉE**.

Le procédé de confirmation de la saisie du code secret peut se différencier en fonction du modèle d'appareil mobile.

La fenêtre d'état de la protection de Kaspersky Endpoint Security 8 for Smartphone (cf. rubrique "Fenêtre d'état de la protection" à la page [26](#)) apparaît à l'écran.

SAISIE DU CODE SECRET

Après le lancement de l'application, vous serez invité à saisir le code secret de l'application. 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.

Il faut saisir le code secret de l'application dans les cas suivants :

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

Mémoisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Endpoint Security 8 for Smartphone, ni supprimer l'application.

Le code secret de l'application est composé de chiffres. Il doit être composé d'au moins 4 chiffres.

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

1. Confirmez la saisie du code secret de l'application. Pour ce faire, à la première exécution de l'application cliquez sur **OK** dans la fenêtre de notification.

L'écran de saisie du code secret de l'application s'affiche.

2. Saisissez les chiffres qui constituent votre code dans le champ **Saisissez le nouveau code**.
3. Tapez de nouveau ce code dans la zone **Confirmer**.
4. Cliquez sur la touche **ENTER**.

La robustesse du code saisi est vérifiée automatiquement.

Si le code secret que vous avez saisi est fiable, l'écran de l'état de la protection s'affichera.

Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche et l'application demande une confirmation. Pour utiliser le code actuel, cliquez sur **Oui**.

Pour définir un nouveau code, cliquez sur **Non**. Les champs **Saisissez le nouveau code** et **Confirmation du code** seront vides. Ressaisissez le code secret de l'application.

INFORMATIONS SUR LE PROGRAMME

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

➤ *Pour consulter les informations relatives à l'application,*

sous l'onglet **Avancé**, choisissez l'option **Infos logiciel**.

INTERFACE DE L'APPLICATION

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

DANS CETTE SECTION

Onglets de l'application	26
Fenêtre d'état de la protection.....	26

ONGLETS DE L'APPLICATION

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

Kaspersky Endpoint Security 8 for Smartphone propose les onglets suivants :

- **État de protection** : affiche l'état de tous les modules de l'application.
- **Antivol** : protège des données stockées sur l'appareil en cas de perte ou de vol.
- **Filtre des appels et des SMS** : filtre les appels et les SMS entrants non sollicités.
- **Avancé** : paramètres généraux de l'application, lancement de la synchronisation de l'appareil avec le système d'administration distante, suppression de l'application, informations sur l'application et sur la licence.

Vous pouvez naviguer entre les onglets à l'aide de la barre de défilement.

FENETRE D'ETAT DE LA PROTECTION

L'état des modules principaux de l'application s'affiche dans la fenêtre de l'état de la protection (cf. ill. ci-après).

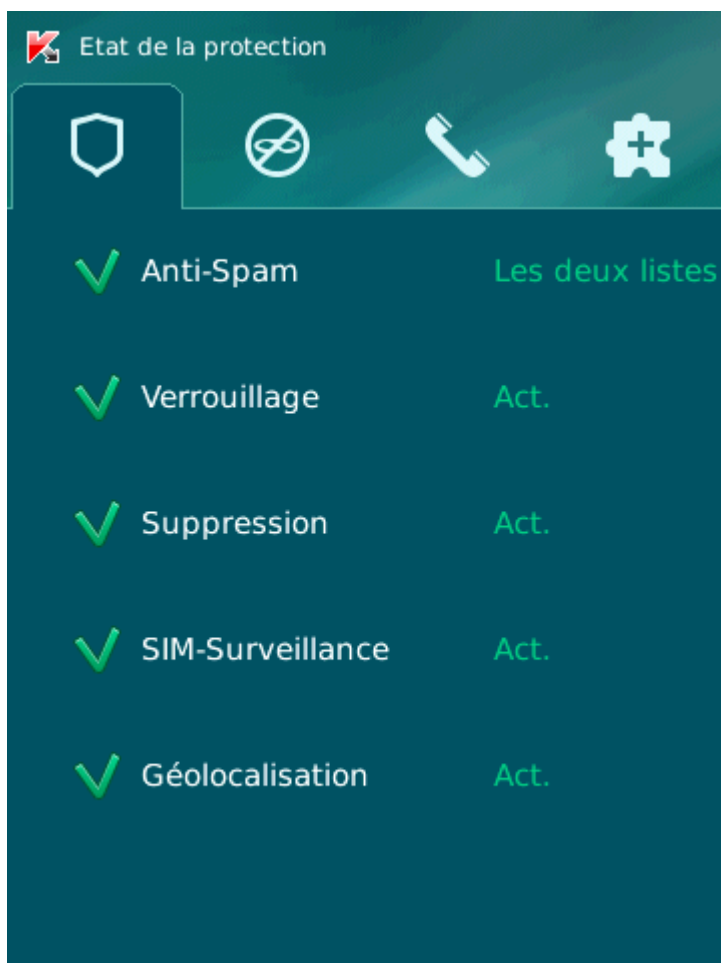


Figure 7: Fenêtre de l'état de la protection

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

- **Anti-Spam** : mode de filtrage des appels et des SMS (cf. rubrique "Filtrage des appels et des SMS entrants" à la page [29](#)).
- **Verrouillage, Suppression, SIM Surveillance, Localisation** : états des fonctions d'Antivol (cf. section "Protection des données en cas de perte ou de vol de l'appareil" à la page [44](#)).

L'état **Activée** signifie que la fonction Antivol est activée. L'état **Désactivée** signifie que la fonction Antivol est désactivée.

La fenêtre d'état de la protection s'affiche après le lancement de l'application. Vous pouvez également ouvrir la fenêtre d'état de la protection en sélectionnant l'onglet **État de la protection**.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

Cette section présente les informations sur le Filtre des appels et des SMS 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 du Filtre des appels et des SMS 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

Présentation du Filtre des appels et des SMS	29
Présentation des modes du Filtre des appels et des SMS	30
Modification du mode du Filtre des appels et des SMS	31
Composition de la liste noire	31
Composition de la liste blanche.....	35
Réaction aux SMS et appels de contacts qui ne figurent pas dans le répertoire téléphonique	39
Réaction aux SMS en provenance de numéros sans chiffres	40
Sélection de l'action à appliquer sur les SMS entrants.....	41
Sélection de l'action à appliquer sur des appels entrants.....	42

PRESENTATION DU FILTRE DES APPELS ET DES SMS

Le Filtre des appels et des SMS 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 le Filtre des appels et des SMS refuse pour la liste noire et accepte pour la liste blanche.
- Type d'événement que le Filtre des appels et des SMS 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 au Filtre des appels et des SMS d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, le Filtre des appels et des SMS 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, le Filtre des appels et des SMS va accepter les SMS avec cette expression clé et refuser les SMS sans cette expression clé.

Le Filtre des appels et des SMS filtre les appels et les SMS entrants selon le mode sélectionné (cf. la rubrique "Présentation des modes du Filtre des appels et des SMS " à la page [30](#)). Le Filtre des appels et des SMS 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 le Filtre des appels et des SMS a attribué l'état de sollicité ou non au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section "Journaux du logiciel" à la page [55](#)).

PRESENTATION DES MODES DU FILTRE DES APPELS ET DES SMS

Le mode détermine les règles utilisées par le Filtre des appels et des SMS pour filtrer les appels et les SMS entrants.

Les modes de fonctionnement du Filtre des appels et des SMS 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, le Filtre des appels et des SMS vous invitera à ajouter ce numéro sur une des listes.

Vous pouvez modifier le mode du Filtre des appels et des SMS (cf. rubrique "Modification du mode du Filtre des appels et des SMS" à la page [31](#)). Le mode actuel du Filtre des appels et des SMS s'affiche sous l'onglet **Filtre des appels et des SMS** à côté de l'option **Mode**.

MODIFICATION DU MODE DU FILTRE DES APPELS ET DES SMS.

➔ Pour modifier le mode du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS**, sélectionnez l'option **Mode**.

L'écran **Filtre des appels et des SMS** s'ouvre.

2. Sélectionnez une valeur pour le paramètre **Mode du Filtre des appels et des SMS** (cf. ill. ci-dessous).

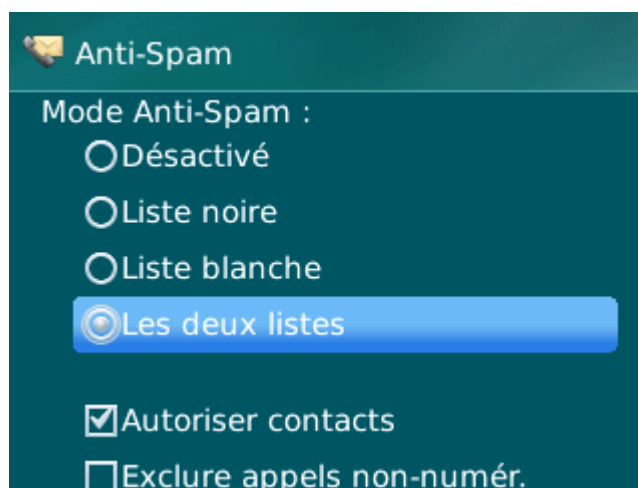


Figure 8: modification du mode du Filtre des appels et des SMS.

3. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

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

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

Le Filtre des appels et des SMS uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste noire. Le Filtre des appels et des SMS acceptera les appels et les SMS qui ne satisfont pas à un ou plusieurs critères de l'enregistrement de la liste noire.

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

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section "Journaux du logiciel" à la page [55](#)).

DANS CETTE SECTION

Ajout d'un enregistrement à la liste noire	32
Modification d'un enregistrement de la liste noire.....	33
Suppression d'un enregistrement de la liste blanche	34

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 du Filtre des appels et des SMS. 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 du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Menu** → **Ajouter**.

L'écran **Nouvel enregistrement** s'ouvre.

3. Attribuez des valeurs aux paramètres suivants (cf. ill. ci-après) :

- **Bloquer tout** : type d'événements en provenance du numéro de téléphone que le Filtre des appels et des SMS refusera pour les numéros de la liste noire :
 - **Appels et SMS** : bloque les appels et les SMS entrants.
 - **Appels seulement** : bloque uniquement les appels entrants.
 - **SMS seulement** : bloque uniquement les SMS entrants.

- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par le Filtre des appels et des SMS. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la Liste noire. Le Filtre des appels et des SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
- **Contenants le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Le Filtre des appels et des SMS refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS.

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

Figure 9 : paramètres d'une entrée de la liste noire

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

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

➔ Pour modifier un enregistrement de la liste noire du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

2. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

L'écran **Modification d'entrée** s'ouvre.

3. Modifiez les paramètres requis.

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

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

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer ce numéro de la liste noire. De plus, vous pouvez purger la liste noire du Filtre des appels et des SMS en supprimant tous les enregistrements qu'elle contient.

➤ Pour supprimer un enregistrement de la liste noire du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'entrée qu'il faut supprimer, puis sélectionnez **Menu** → **Supprimer**.

La fenêtre de confirmation s'affichera à l'écran.

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

➤ Pour purger la liste noire du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

2. Sélectionnez l'option **Menu** → **Supprimer tout**.

La fenêtre de confirmation s'affichera à l'écran.

3. 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 le Filtre des appels et des SMS. Chacun de ces enregistrements contient les informations suivantes :

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

Le Filtre des appels et des SMS accepte uniquement les appels et les SMS qui satisfont à tous les critères d'un enregistrement de la liste blanche. Le Filtre des appels et des SMS 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 à la liste blanche	35
Modification d'un enregistrement de la liste blanche	37
Suppression d'un enregistrement de la liste blanche	38

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 du Filtre des appels et des SMS. 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 une entrée dans la liste blanche du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste blanche**.

L'écran **Liste blanche** s'ouvre.

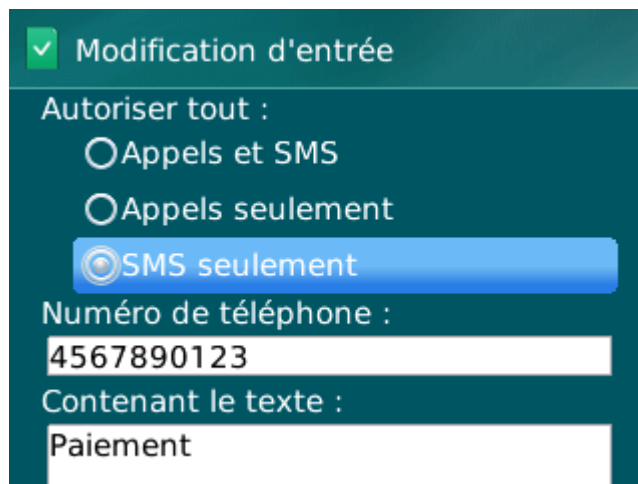
2. Sélectionnez **Menu** → **Ajouter**.

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

- **Autoriser tout** : type d'événements en provenance du numéro de téléphone que le Filtre des appels et des SMS refusera pour les numéros de la liste blanche :
 - **Appels et SMS** : autorise les appels et les SMS entrants.
 - **Appels seulement** : autorise uniquement les appels entrants.
 - **SMS seulement** : autorise les messages SMS entrants uniquement.
- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par le Filtre des appels et des SMS. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Le Filtre des appels et des SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

- **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, le Filtre des appels et des SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

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



Modification d'entrée
 Autoriser tout :
 Appels et SMS
 Appels seulement
 SMS seulement
 Numéro de téléphone :
 4567890123
 Contenant le texte :
 Paiement

Figure 10 : paramètres d'une entrée de la liste blanche

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

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

➔ Pour modifier un enregistrement de la liste blanche du Filtre des appels et des SMS, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste blanche**.

L'écran **Liste blanche** s'ouvre.

2. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

L'écran **Modification d'entrée** s'ouvre.

3. Modifiez les paramètres requis.

- **Autoriser tout** : type d'événements en provenance du numéro de téléphone que le Filtre des appels et des SMS refusera pour les numéros de la liste blanche :
 - **Appels et SMS** : autorise les appels et les SMS entrants.
 - **Appels seulement** : autorise uniquement les appels entrants.
 - **SMS seulement** : autorise les messages SMS entrants uniquement.
- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par le Filtre des appels et des SMS. Le numéro peut commencer par un chiffre, une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. En tant que le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Le Filtre des appels et des SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
- **Contenant le texte** : expression clé qui indique que le SMS reçu est sollicité. S'il s'agit des numéros de la liste blanche, le Filtre des appels et des SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

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

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

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

➔ *Pour supprimer un enregistrement de la liste blanche du Filtre des appels et des SMS, procédez comme suit :*

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste blanche**.

L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'entrée qu'il faut supprimer, puis sélectionnez **Menu** → **Supprimer**.

La fenêtre de confirmation s'affichera à l'écran.

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

➤ *Pour purger la liste blanche du Filtre des appels et des SMS, procédez comme suit :*

1. Sous l'onglet **Filtre des appels et des SMS** sélectionnez l'option **Liste blanche**.

L'écran **Liste blanche** s'ouvre.

2. Appuyez sur **Menu** → **Supprimer tout**.

La fenêtre de confirmation s'affichera à l'écran.

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

La liste blanche sera vide.

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

Si le mode du Filtre des appels et des SMS **Les deux listes** ou **Liste blanche** (cf. la rubrique "**Présentation des modes du Filtre des appels et des SMS**" à la page [30](#)) est sélectionné, vous pouvez également définir la réaction du Filtre des appels et des SMS aux SMS ou aux appels dont les numéros ne figurent pas dans les Contacts. Le Filtre des appels et des SMS permet d'élargir la liste blanche en y introduisant les numéros des contacts.

➤ *Pour définir la réaction du Filtre des appels et des SMS face aux numéros ne figurant pas dans le répertoire téléphonique de l'appareil, procédez comme suit :*

1. Sous l'onglet **Filtre des appels et des SMS**, sélectionnez l'option **Mode**.

L'écran **Filtre des appels et des SMS** s'ouvre.

2. Choisissez la valeur de paramètre **Autoriser contacts** (cf. ill. ci-après) :
 - Pour que le Filtre des appels et des SMS 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 le Filtre des appels et des SMS filtre les SMS et les appels uniquement sur la base du régime défini du Filtre des appels et des SMS, décochez la case **Autoriser contacts**.

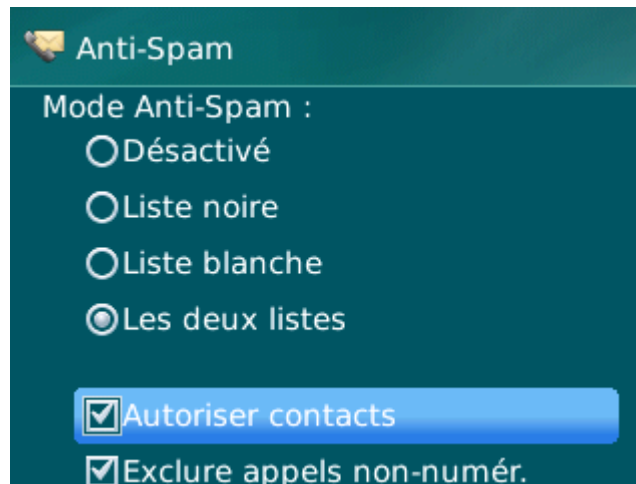


Figure 11: réaction du Filtre des appels et des SMS face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

3. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode choisi pour le Filtre des appels et des SMS est **Les deux listes** ou **Liste noire** (cf. la rubrique "**Présentation des modes du Filtre des appels et des SMS**" à la page [30](#)), vous pouvez enrichir la liste noire en y ajoutant tous les numéros sans chiffres (composés de lettres). Si cette case est cochée, le Filtre des appels et des SMS traite les SMS en provenance des numéros sans chiffres comme s'il s'agissait des numéros de la liste noire.

➤ Afin de définir les réactions du Filtre des appels et des SMS face aux SMS en provenance de numéros sans chiffres, procédez comme suit :

1. Sous l'onglet **Filtre des appels et des SMS**, sélectionnez l'option **Mode**.

L'écran **Filtre des appels et des SMS** s'ouvre.

2. Choisissez une valeur pour le paramètre **Exclure appels non-numériques** (cf. ill. ci-après) :
 - afin que le Filtre des appels et des SMS bloque les messages en provenance de numéros sans chiffres, cochez la case **Exclure numéros sans chiffres** ;
 - afin que le Filtre des appels et des SMS filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour le Filtre des appels et des SMS, décochez la case **Exclure numéros sans chiffres**.

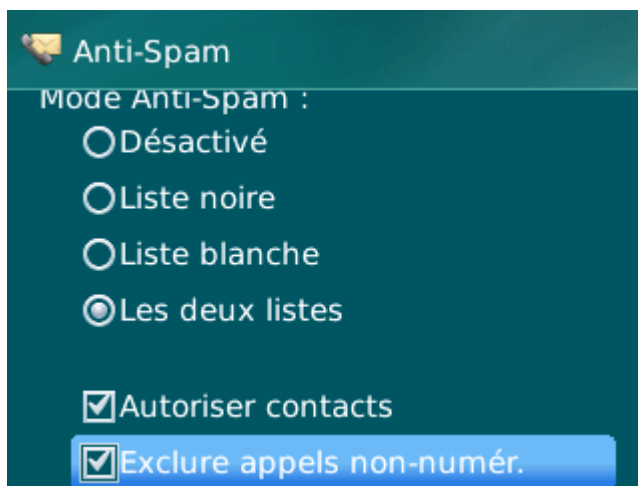


Figure 12: Sélection des actions exécutées par le Filtre des appels et des SMS en cas de réception de SMS depuis un numéro sans chiffres

3. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Si le mode choisi est **Les deux listes** (cf. la rubrique "**Présentation des modes du Filtre des appels et des SMS**" à la page [30](#)), le Filtre des appels et des SMS analyse les SMS entrants sur la base des listes blanche et noire.

Après la réception d'un SMS en provenance du numéro qui ne figure sur aucune des listes, le Filtre des appels et des SMS 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**.

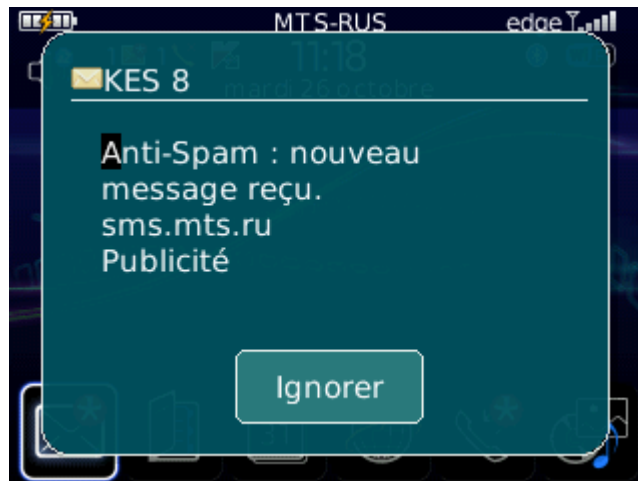


Figure 13: notification du Filtre des appels et des SMS sur le SMS reçu

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page [55](#)).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Si le mode choisi est **Les deux listes** (cf. la rubrique "**Présentation des modes du Filtre des appels et des SMS**" à la page [30](#)), le Filtre des appels et des SMS analyse les SMS entrants sur la base des listes blanche et noire. Après la réception d'un appel en provenance du numéro qui ne figure sur aucune des listes, le Filtre des appels et des SMS 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.



Figure 14: notification du Filtre des appels et des SMS sur le SMS reçu

Les informations relatives aux appels interdits sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page [55](#)).

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

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

Elle explique également comment activer/désactiver les fonctions d'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 module Antivol	44
Verrouillage de l'appareil.....	45
Suppression de données personnelles	46
Composition de la liste des dossiers à supprimer	49
Contrôle du remplacement de la carte SIM sur l'appareil.....	50
Détermination des coordonnées géographiques de l'appareil.....	51
Lancement à distance de la fonction Antivol	53

A PROPOS DU MODULE ANTIVOL

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

Antivol dispose des fonctions suivantes :

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

- **Géolocalisation** : permet de déterminer les coordonnées de l'appareil. Le message avec les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis le SMS spécial, ainsi que à l'adresse de la messagerie électronique.

Kaspersky Endpoint Security 8 for Smartphone permet de lancer à distance la fonction Antivol via l'envoi d'une instruction SMS (cf. la rubrique "Lancement à distance de la fonction Antivol" à la page [53](#)) depuis un autre appareil mobile.

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

L'état actuel de chaque fonction apparaît dans l'écran **Antivol** à côté du nom de l'application.

Les informations relatives au fonctionnement du module sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page [55](#)).

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 activer la fonction de verrouillage, procédez comme suit :

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

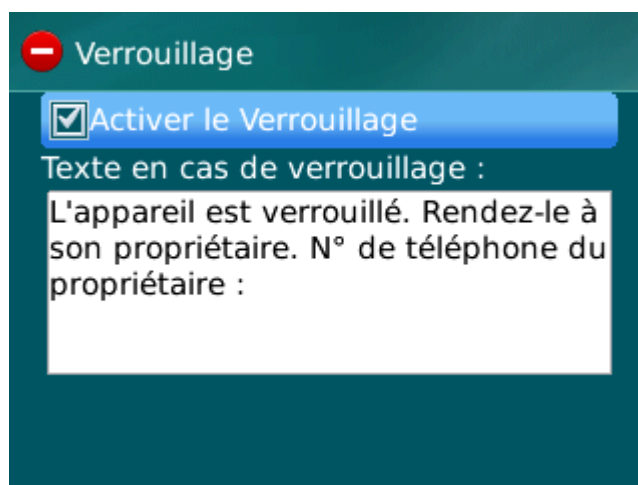


Figure 15: paramètres de la fonction Verrouillage

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

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

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

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

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

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

1. Sous l'onglet **Avancé** sélectionnez l'option **Envoi d'une instruction**.

L'écran **Envoi d'une instruction** s'ouvre.

2. Sélectionnez pour le paramètre **Sélectionnez l'instruction SMS** la valeur **Verrouillage**.
3. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
4. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'application, spécifié sur l'appareil destinataire de l'instruction SMS.
5. Sélectionnez **Menu** → **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 DONNÉES PERSONNELLES

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

- données personnelles de l'utilisateur (entrées des Contacts, calendrier, messages électroniques, journal des appels) ;
- données sur la carte mémoire ;
- fichiers de la liste des dossiers à supprimer (cf. section Création de la liste des dossiers à supprimer à la page [49](#)).

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. Sous l'onglet **Antivol**, choisissez l'option **Suppression**.
L'écran **Suppression de données** s'ouvre.
2. Sélectionnez l'option **Mode**.
L'écran **Suppression de données** s'ouvre.
3. Cochez la case **Activer la suppression de données**.
4. Sélectionnez les informations à supprimer. Pour ce faire, dans le groupe **Supprimer**, 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 des dossiers de la carte mémoire et ceux de la liste des dossiers à supprimer, cochez la case **Dossiers à choisir**.

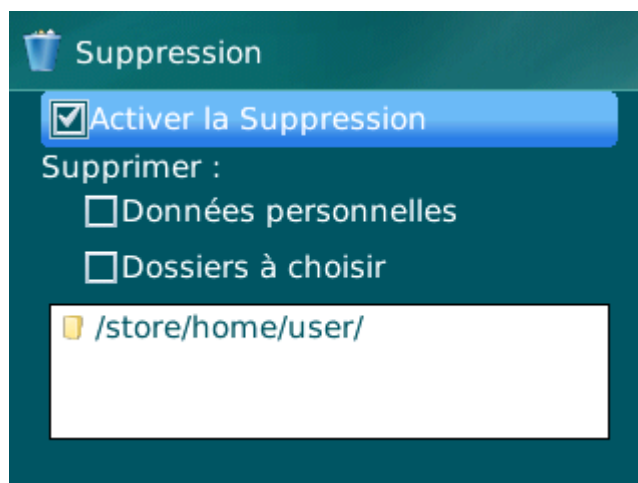


Figure 16: paramètres de la fonction de suppression de données

5. Fichiers de la liste des dossiers à supprimer (cf. section Création de la liste des dossiers à supprimer à la page [49](#)).
6. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

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

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

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

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

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

1. Sous l'onglet **Avancé**, sélectionnez l'option **Envoi d'une instruction**.

L'écran **Envoi d'une instruction** s'ouvre.

2. Sélectionnez pour le paramètre **Sélectionnez l'instruction SMS** la valeur **Suppression**.
3. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
4. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'application, spécifié sur l'appareil destinataire de l'instruction SMS.
5. Sélectionnez **Menu** → **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.

Pour qu'Antivol supprime les dossiers de la liste après la réception de l'instruction SMS spéciale, assurez-vous que sous l'onglet **Antivol** → **Suppression** la case **Dossiers à choisir** est cochée.

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

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

1. Sous l'onglet **Antivol**, choisissez l'option **Suppression**.

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

2. Ouvrez la liste des dossiers à supprimer.
3. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

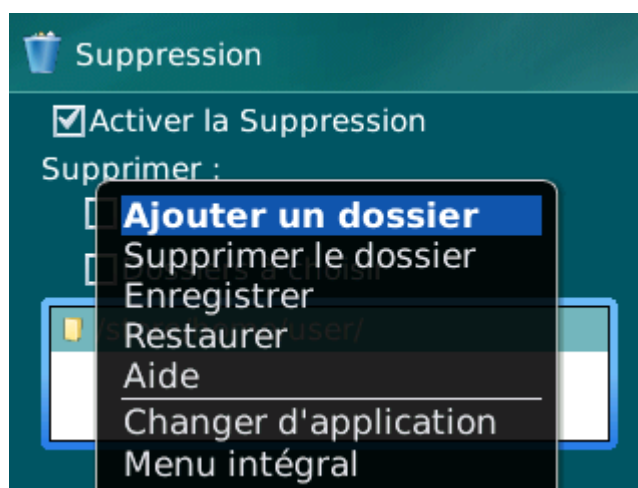


Figure 17: ajout d'un dossier

4. Sélectionnez le dossier requis dans l'arborescence, puis sélectionnez **Menu** → **Sélectionner**.

Le dossier sera ajouté à la liste **Dossiers à choisir**.

5. Sélectionnez **Menu** → **Enregistrer**.

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

1. Sous l'onglet **Antivol**, choisissez l'option **Suppression**.

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

2. Ouvrez la liste des dossiers à supprimer.

3. Marquez un dossier de la liste, puis sélectionnez **Menu** → **Supprimer le dossier**.
La fenêtre de confirmation s'affichera à l'écran.
4. Pour confirmer la suppression du dossier, cliquez sur **Oui**.
Le dossier sera supprimé de la liste **Dossiers à choisir**.
5. Sélectionnez **Menu** → **Enregistrer**.

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. Sous l'onglet **Antivol**, sélectionnez l'option **SIM-Surveillance**.
L'écran **SIM-Surveillance** s'ouvre.
2. Cochez la case **Activer SIM-Surveillance**.
3. Pour contrôler le remplacement de la carte SIM sur l'appareil, configurez les paramètres suivants (cf. ill. ci-dessous) :
 - Pour recevoir automatiquement un SMS indiquant le nouveau numéro de téléphone de votre appareil, saisissez dans le groupe **Envoyer le nouveau numéro de la carte SIM** dans le champ **SMS au numéro de téléphone** le numéro de téléphone vers lequel le SMS sera envoyé.

Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres.
 - Pour recevoir un message électronique indiquant le nouveau numéro de téléphone de votre appareil, saisissez dans le groupe **Envoyer le nouveau numéro de la carte SIM** dans le champ **Mess. à l'adresse de courrier élec.** une adresse électronique.
 - Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, cochez dans le groupe **Avancé** la case **Verrouiller l'appareil**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret de l'application.

- Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Texte en cas de verrouillage**. Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

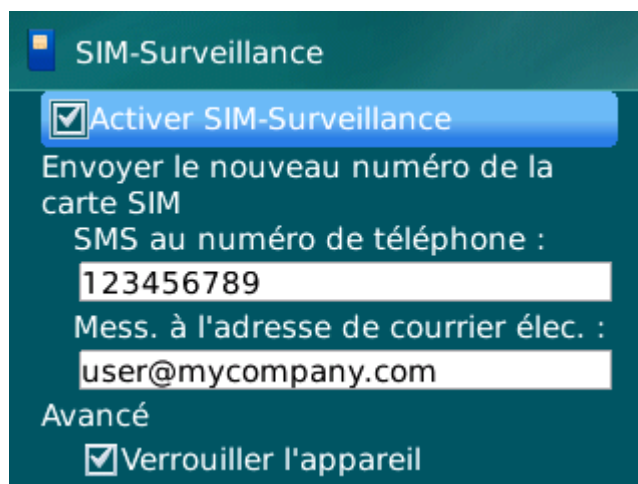


Figure 18: paramètres de la fonction SIM-Surveillance

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

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

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

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

◆ *Pour activer la fonction Géolocalisation, procédez comme suit :*

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

L'écran **Géolocalisation** s'ouvre.

2. Cochez la case **Activer la Géolocalisation**.

Après la réception d'une instruction SMS spéciale, Kaspersky Endpoint Security 8 for Smartphone renvoie les coordonnées de l'appareil par SMS.

3. Pour recevoir également les coordonnées par courrier électronique, saisissez dans le groupe **Envoyer les coordonnées de l'appareil** pour le paramètre **Message à l'adresse électronique** l'adresse électronique (cf. ill. ci-après).

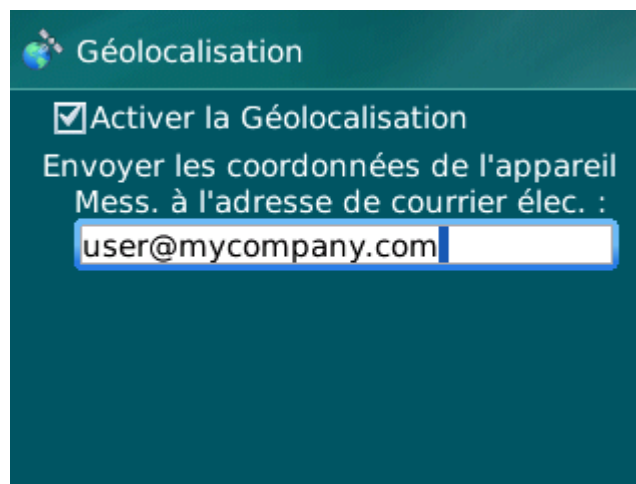


Figure 19: paramètres de la fonction Géolocalisation

4. Sélectionnez **Menu** → **Enregistrer** pour enregistrer les modifications.

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

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

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

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

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

1. Sous l'onglet **Avancé** sélectionnez l'option **Envoi d'une instruction**.

L'écran **Envoi d'une instruction** s'ouvre.

2. Attribuez au paramètre **Instruction SMS** la valeur **Géolocalisation**.
3. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

4. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'application, spécifié sur l'appareil destinataire de l'instruction SMS.
5. Sélectionnez **Menu** → **Envoyer**.

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

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

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

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

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

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

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

1. Sous l'onglet **Avancé**, sélectionnez l'option **Envoi d'une instruction**.

L'écran **Envoi d'une instruction** s'ouvre.

2. Sélectionnez la fonction à exécuter à distance depuis un autre appareil mobile. Pour ce faire, sélectionnez une des valeurs proposées du paramètre **Choisissez l'instruction SMS** (cf. ill. ci-après) :
 - Verrouillage de l'appareil (à la page [45](#)).
 - Suppression des données (cf. la rubrique Suppression de données personnelles à la page [46](#)) ;

- Localisation de l'appareil (cf. la rubrique Détermination des coordonnées géographiques de l'appareil à la page [51](#)).
- Contacts personnels.

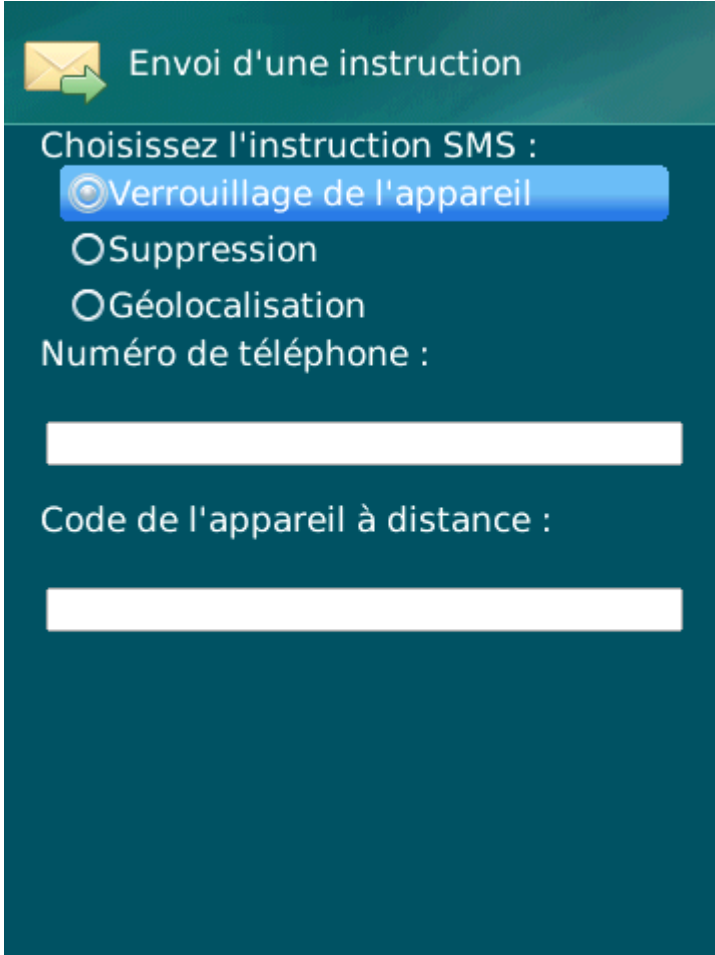


Figure 20: Lancement des fonctions Antivol à distance

3. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
4. Dans le champ **Code de l'appareil à distance**, saisissez le code secret de l'application, spécifié sur l'appareil destinataire de l'instruction SMS.
5. Sélectionnez **Menu** → **Envoyer**.

JOURNAUX DU LOGICIEL

La section présente les informations sur les journaux où sont consignés les détails du fonctionnement de chaque module ainsi que les détails de l'exécution de chaque tâche (par exemple, synchronisation avec le système d'administration distante, réception de l'instruction SMS depuis un autre appareil).

DANS CETTE SECTION

À propos des journaux	55
Affichage des événements du journal	55
Suppression des enregistrements du journal	55

À PROPOS DES JOURNAUX

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

AFFICHAGE DES EVENEMENTS DU JOURNAL

- *Pour consulter les enregistrements dans le journal du module,*
sous l'onglet du module nécessaire, choisissez l'option **Journal des événements**.

Le journal du module sélectionné s'ouvre.

Naviguez dans le journal à l'aide de la barre de défilement.

- *Pour afficher des informations détaillées sur les enregistrements du journal,*
sélectionnez l'enregistrement nécessaire et cliquez sur la touche **ENTRÉE**.

SUPPRESSION DES ENREGISTREMENTS DU JOURNAL

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

- *Pour purger tous les journaux, procédez comme suit :*
 1. Sous l'onglet de n'importe quel module, choisissez l'option **Journal des événements**.
L'écran **Journal d'événements** s'ouvre.
 2. Sélectionnez **Menu** → **Effacer le journal**.
 3. Pour confirmer la suppression, cliquez sur **Oui**.

Tous les enregistrements du journal de chaque module seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section offre des informations sur les possibilités complémentaires de Kaspersky Endpoint Security 8 for Smartphone : comment modifier le code secret et comment activer/désactiver l'affichage des astuces avant l'installation des paramètres de chaque module.

DANS CETTE SECTION

Modification du code secret.....	56
Affichage des astuces	57

MODIFICATION DU CODE SECRET

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

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

1. Sous l'onglet **Avancé**, sélectionnez l'option **Paramètres supplémentaires**.
L'écran **Paramètres supplémentaires** apparaît.
2. Choisissez l'option **Modification du code**.
3. Saisissez le code secret actuel de l'application dans la zone **Saisissez le code secret**.
4. Saisissez le nouveau code secret de l'application dans les champs **Saisissez le nouveau code** et **Confirmation du code**.

La robustesse du code saisi est vérifiée automatiquement.

Si le code secret que vous avez saisi est fiable, il sera enregistré.

Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche sur l'écran et l'application demande une confirmation. Pour utiliser le code actuel, cliquez sur **Oui**.

Pour définir un nouveau code, cliquez sur **Non**. Les champs **Saisissez le nouveau code** et **Confirmation du code** seront vides. Ressaisissez le code secret de l'application.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des modules, 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. Sous l'onglet **Avancé**, sélectionnez l'option **Paramètres supplémentaires**.

L'écran **Paramètres supplémentaires** apparaît.

2. Activez / désactivez l'affichage des astuces. Pour ce faire, sélectionnez l'option **Astuces**.

L'état d'affichage des astuces sera affiché à côté de l'option **Astuces**. L'icône de basculement à droite changera en fonction de l'état d'affichage des astuces.

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'activation est effectuée par l'utilisateur pendant et après l'installation de l'application. L'utilisateur doit avoir le code d'activation et le fichier de licence pour activer l'application.

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 afin d'activer à distance les fonctions suivantes : Verrouillage, Suppression, SIM-Surveillance, Localisation et Contacts personnels.

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 le Filtre des appels et des SMS.
- Type d'événement en provenance de ce numéro que le Filtre des appels et des SMS accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.
- Expression clé qui permet au Filtre des appels et des SMS d'identifier des SMS sollicités (qui ne sont pas du spam). Le Filtre des appels et des SMS 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 le Filtre des appels et des SMS.
- Type d'événement en provenance de ce numéro que le Filtre des appels et des SMS bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.

- Expression clé qui permet au Filtre des appels et des SMS d'identifier des SMS non sollicités (spam). Le Filtre des appels et des SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

MASQUE DU NUMERO DE TELEPHONE

Présentation du numéro de téléphone dans la liste noire ou blanche par les caractères communs. Les deux caractères génériques de base utilisés dans les masques de numéro de téléphone sont "*" et "?" (où * représente une suite de caractères quelconques et ? un seul caractère). Il s'agit, par exemple, du numéro *1234 ? de la Liste noire. Le Filtre des appels et des SMS 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.

S

SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des messages SMS clairement indésirables.

SYNCHRONISATION

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

SYSTEME D'ADMINISTRATION DISTANTE

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

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures, tandis que les bases antispam sont actualisées toutes les 5 minutes.*

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U),

ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

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

L'Encyclopédie des virus: <http://www.securelist.com/fr>

Laboratoire antivirus : newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>

(pour les questions aux experts antivirus)

Forum Internet de Kaspersky Lab : <http://forum.kaspersky.fr>

INFORMATIONS SUR LE CODE TIERS

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

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

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

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques enregistrées et les marques de services appartiennent à leurs propriétaires respectifs.

La marque de commerce Blackberry appartient à Research In Motion Limited, elle est déposée aux Etats-Unis et peut être déposée ou est déposée dans d'autres pays.

INDEX

A

Activer	
Filtre des appels et des SMS	31
Afficher	
Etat de la protection.....	27
Ajout	
liste blanche du Filtre des appels et des SMS	36
liste noire du Filtre des appels et des SMS.....	32
Antivol	44
Géolocalisation	51
SIM-Surveillance	50
suppression de données.....	47, 49
verrouillage.....	45
Astuces de l'application.....	57
Autoriser	
appels entrants.....	36
SMS entrants.....	36

C

Clé	
installation.....	19
Code	
code secret de l'application	25
Code secret de l'application	25, 56
CONFIGURATION MATERIELLE	9
Coordonnées de l'appareil	51

D

Désactiver	
Filtre des appels et des SMS.....	30, 31
Données	
suppression à distance.....	47

E

Enregistrement	
liste blanche du Filtre des appels et des SMS	36
liste noire du Filtre des appels et des SMS.....	32
Etat de la protection	27
Exécuter	
programme	24

F

FILTRAGE	
APPELS ENTRANTS	29
SMS ENTRANTS	29
Filtre des appels et des SMS	29
Filtre des appels et des SMS	
modes.....	30
Filtre des appels et des SMS	
liste noire	31
Filtre des appels et des SMS	
liste blanche.....	35
Filtre des appels et des SMS	

numéros qui ne figurent pas dans les Contacts	39
Filtre des appels et des SMS	
numéros sans chiffres	40
Filtre des appels et des SMS	
action à appliquer sur les SMS	42
Filtre des appels et des SMS	
action à appliquer sur un appel.....	43
I	
INSTALLATION DE L'APPLICATION	10
Interdire	
appels entrants	31, 35
SMS entrants	31
INTERFACE DE L'APPLICATION.....	26
J	
Journal des événements	
consultation des enregistrements	55
Journaux des événements	
suppression des enregistrements	55
K	
Kaspersky Lab	60
KASPERSKY LAB.....	60
L	
L'envoi d'une instruction SMS	53
Licence	
informations	19
Liste noire	
Filtre des appels et des SMS	31
Lite blanche	
Filtre des appels et des SMS	35
M	
Modes	
Filtre des appels et des SMS	30, 31
Modification	
liste blanche du Filtre des appels et des SMS	37
liste noire du Filtre des appels et des SMS.....	33
O	
Onglets de l'application	26
S	
Suppression	
informations stockées sur l'appareil.....	47
liste blanche du Filtre des appels et des SMS	38
liste noire du Filtre des appels et des SMS.....	34
SUPPRESSION	
APPLICATION.....	17
Supprimer	
événements des journaux.....	55
V	
Verrouiller	
appareil.....	45