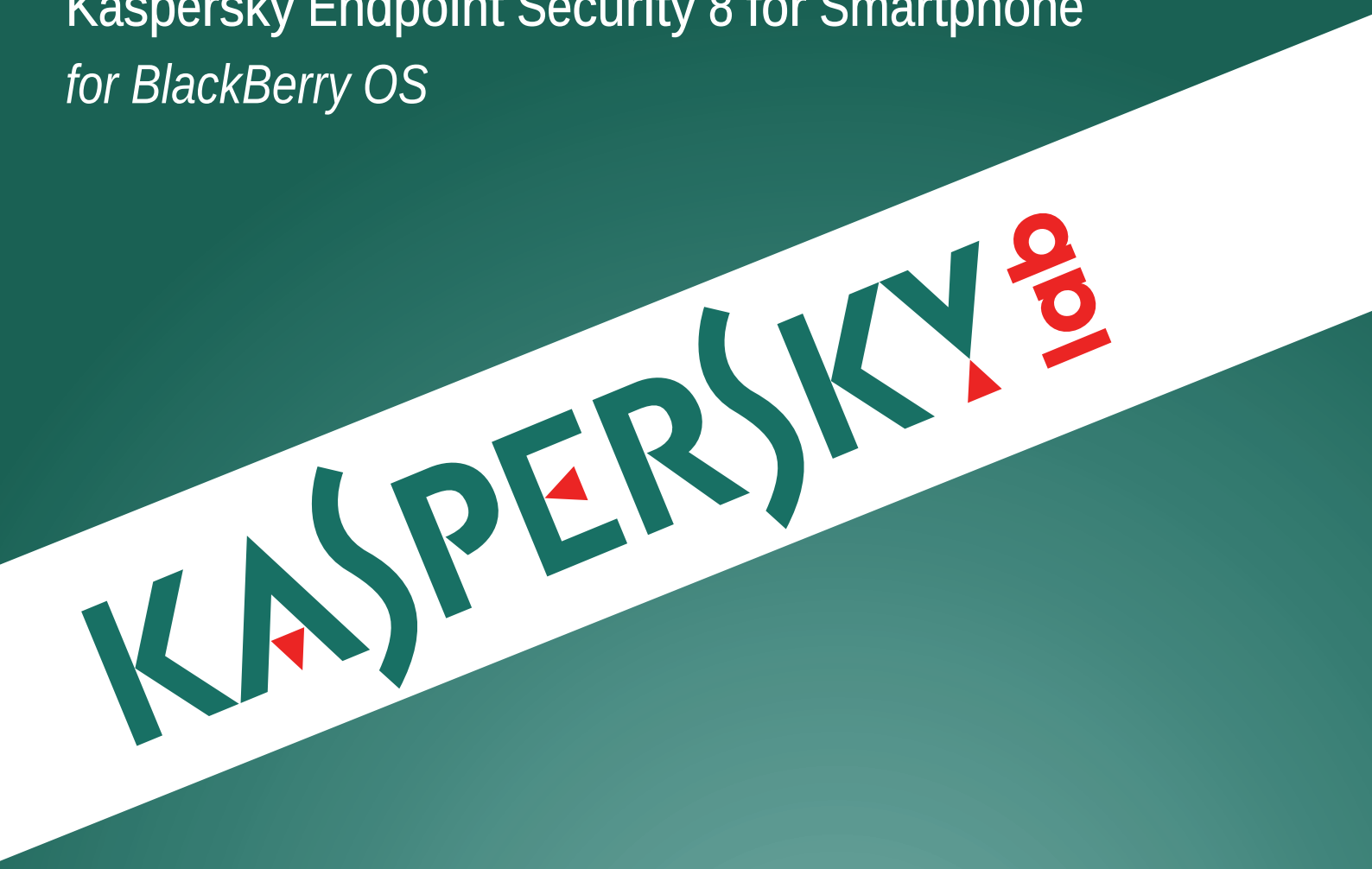
Kaspersky Endpoint Security 8 for Smartphone

for BlackBerry OS



Guide de l'utilisateur

VERSION DE L'APPLICATION: 8.0

Cher utilisateur,

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

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.

Date d'édition : 20/10/2010

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

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

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

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

SI UN CONTRAT DE LICENCE OU UN DOCUMENT SIMILAIRE ACCOMPAGNE LE LOGICIEL, LES CONDITIONS D'UTILISATION DU LOGICIEL DÉFINIES DANS CE DOCUMENT PRÉVALENT SUR LE PRÉSENT CONTRAT DE LICENCE D'UTILISATEUR FINAL.

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

1. Définitions

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

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *" Vous "* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *" entité ",* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patchs, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

2.1. Une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (" l'utilisation ") du Logiciel sur un nombre spécifié d'Ordinateurs vous est octroyée pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la " Licence "), et vous acceptez cette Licence :

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

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos

Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs précisé dans les licences que vous avez obtenues, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.

2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.

3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

4.1. L'assistance technique décrite dans la Clause 2.5 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).
Service d'assistance technique : http://support.kaspersky.com

4.2. Les données de l'utilisateur, spécifiées dans Personal Cabinet/My Kaspersky Account, ne peuvent être utilisées par les spécialistes de l'assistance technique que lors du traitement d'une requête de l'utilisateur.

5. Limitations

5.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou

toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

5.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie.

5.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits.

5.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

5.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

5.6. Votre fichier clé peut être bloqué en cas de non-respect de Votre part des conditions générales de ce Contrat.

5.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

6. Garantie limitée et avis de non-responsabilité

6.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

6.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adapté à Votre cas.

6.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

6.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.5 de ce Contrat.

6.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

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

7. Exclusion et Limitation de responsabilité

7.1. DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE

SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET/OU DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS ET/OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

8. Licence GNU et autres licences de tierces parties

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

9. Droits de propriété intellectuelle

9.1. Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des États-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis

d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

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

10. Droit applicable ; arbitrage

10.1. Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations-Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 10 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

11. Délai de recours.

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

12. Intégralité de l'accord ; divisibilité ; absence de renoncement.

12.1. Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en équité de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

13. Informations de contact du Titulaire des droits

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

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com

TABLE DES MATIERES

A PROPOS DE CE MANUEL

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

Buts du document :

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

SOURCES D'INFORMATIONS COMPLEMENTAIRES

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

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

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

Page sur le site Web de Kaspersky Lab

http://www.kaspersky.com/fr/kaspersky-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 (Knowledge Base)

http://support.kaspersky.com/kes8mobile

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

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Endpoint Security 8 for Smartphone. Ces articles sont regroupés par sujet, par exemple " Utilisation des fichiers de licence ", " Mise à jour des bases " ou " Elimination des échecs ". Les articles répondent non seulement à des questions sur Kaspersky Endpoint Security 8 for Smartphone, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

Système d'aide en ligne

En cas de problème concernant un écran ou un onglet spécifiques de Kaspersky Endpoint Security 8 for Smartphone, vous disposez de l'aide contextuelle.

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

Documentation

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

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

Si votre question n'est pas urgente, vous pouvez en discuter avec les spécialistes de Kaspersky Lab et d'autres utilisateurs sur notre forum au 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'EQUIPE DE REDACTION DE LA DOCUMENTATION

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

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protège les appareils mobiles tournant sous BlackBerry OS. L'application permet de contrôler les SMS et les appels entrants, de protéger les données stockées sur l'appareil en cas de perte ou de vol, et de masquer les informations liées aux contacts confidentiels. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier. 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 composants de protection suivants :

- **Anti-Spam**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant permet de configurer en souplesse la fonction de blocage des SMS et des appels considérés comme indésirables.

- **Antivol** Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol tout en facilitant sa recherche. L'Antivol permet de verrouiller l'appareil à distance à l'aide des SMS, de supprimer les données qu'il contient et de déterminer ses coordonnées géographiques (si l'appareil mobile est doté d'un récepteur GPS). De plus, Antivol permet également de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.

- **Contacts personnels**. Masque les informations liées aux numéros confidentiels de la Liste des contacts que vous avez créée. Les Contacts personnels masquent les entrées des Contacts, les entrées dans le journal des appels et les appels entrants pour ce type de numéros.

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 composants 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 composants (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 composants 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 OS 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, décrit les types d'installation de l'application sur l'appareil mobile et les actions de l'utilisateur pour chacun d'eux.

DANS CETTE SECTION

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).

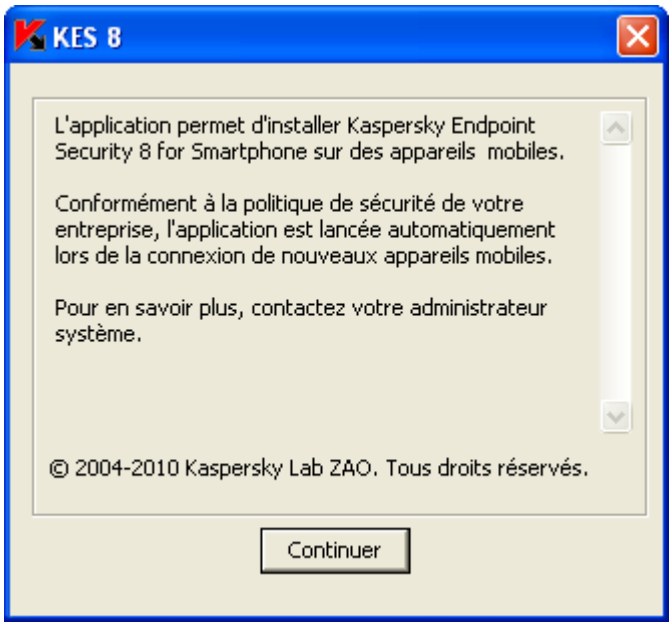


Figure 1: programme d'installation de Kaspersky Endpoint Security 8 for Smartphone

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).

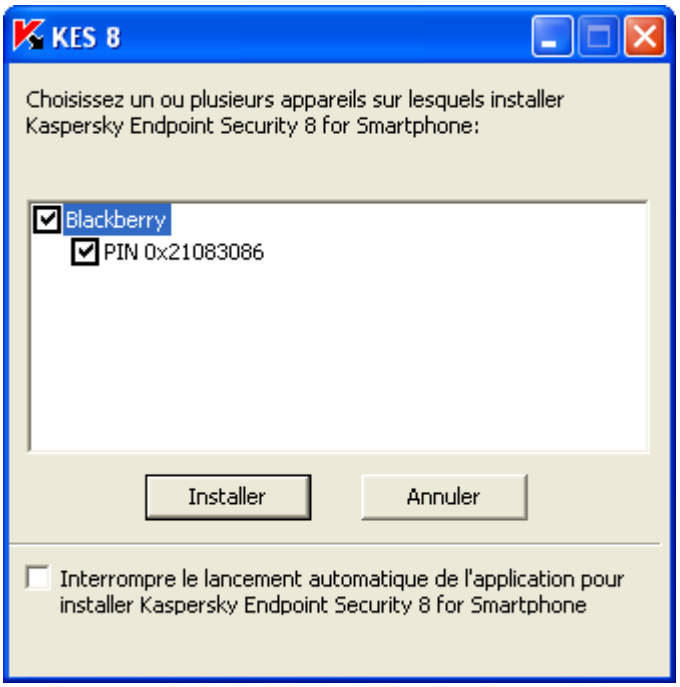


Figure 2: sélection des appareils pour installer Kaspersky Endpoint Security 8 for Smartphone

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 de la distribution de l'application vers l'appareil sera également affiché dans la fenêtre **Kaspersky Endpoint Security 8 for Smartphone** 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 23). 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.

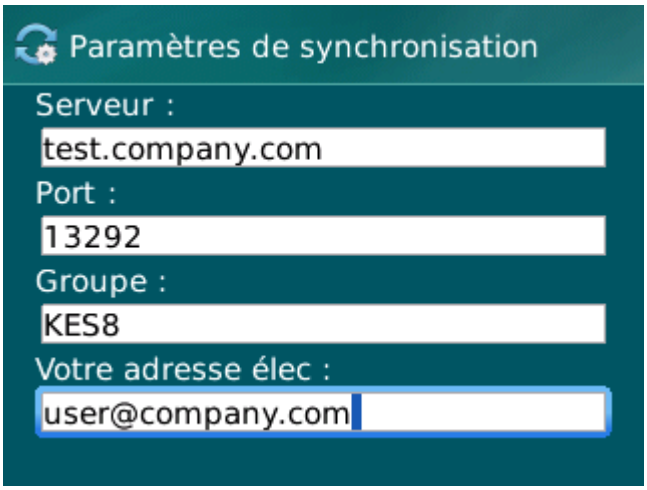


Figure 3: paramètres de synchronisation

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 suivants :

   - **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**.

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

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

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 composant 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 21).

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

SUPPRESSION DE L'APPLICATION

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

La suppression de l'application est possible uniquement si la dissimulation des informations confidentielles est désactivée. Pendant la suppression de l'application l'utilisateur doit s'assurer que cette condition est satisfaite.

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

1. Désactivez la dissimulation des informations confidentielles (cf. la rubrique "Activation/désactivation du composant Contacts personnels" à la page 47).

2. Désinstallation de Kaspersky Endpoint Security 8 for Smartphone Pour ce faire, sous l'onglet **Avancé** sélectionnez l'option **Suppression de l'application** (cf. ill. ci-après).

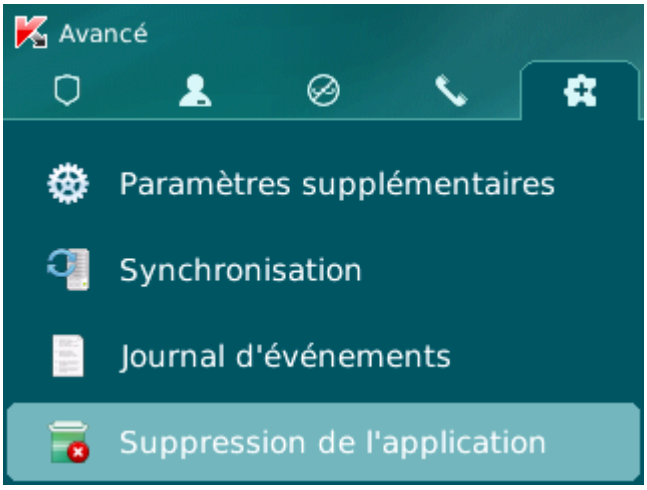


Figure 4: suppression de l'application

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

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

   La suppression de l'application va commencer.

4. 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

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 :

  - désactiver le composant Contacts personnels ;
  - 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 des composants Antivol et Contacts personnels ;
  - désactiver de la dissimulation des informations confidentielles ;
  - consulter le système d'aide ;
  - synchronisation avec le système d'administration distante.

INSTALLATION D'UNE LICENCE

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

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

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

- désactiver tous les composants ;
- désactiver la dissimulation des données confidentielles ;
- consulter le système d'aide.

Si la licence n'a pas été installée dans les trois jours qui suivent l'installation de l'application, pour installer la licence, utilisez la fonction de la synchronisation de l'appareil avec le système d'administration distante (cf. la rubrique "Lancement de la synchronisation à la main" à la page 21).

AFFICHAGE DES INFORMATIONS DE LICENCE

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

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

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

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

Il faut effectuer la synchronisation à la main dans les cas suivants :

- si dans les trois jours qui suivent l'installation de l'application la licence n'a pas été installée ;
- si l'appareil n'a pas reçu les paramètres de l'application, définis par l'administrateur.

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 22).

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).

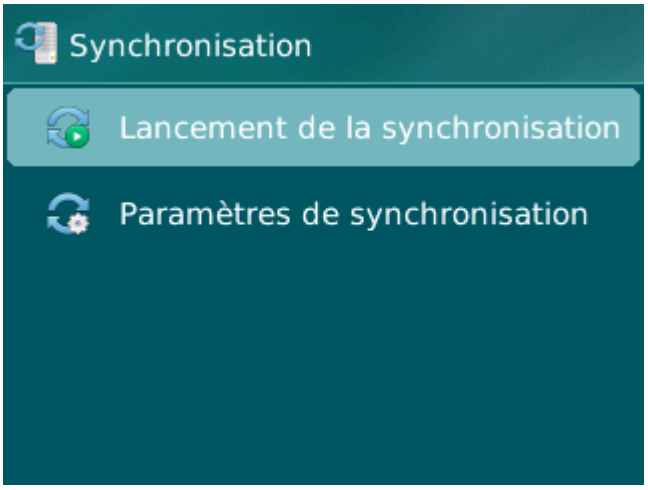


Figure 5: synchronisation à la main

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**. Pour autoriser la connexion à Internet, cliquer sur **Oui**. La connexion au système d'administration distante sera établie.

MODIFICATION DES PARAMETRES DE SYNCHRONISATION

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

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

1. 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**.

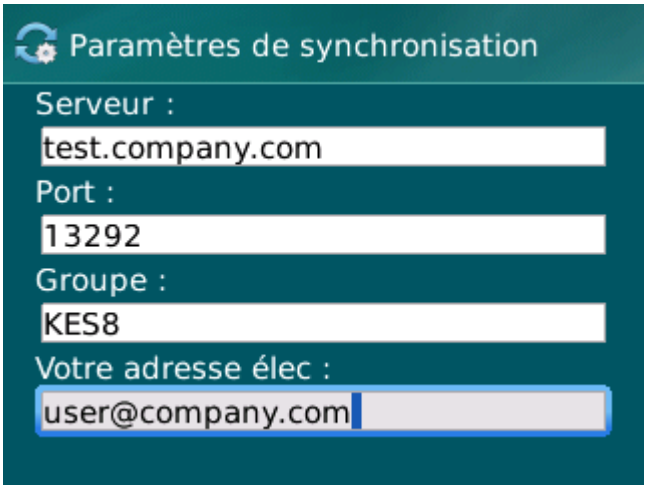


Figure 6: modification des paramètres de synchronisation

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

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** → **KMS 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**.

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 25) 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.

Mémorisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Endpoint Security 8 for Smartphone, ni 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 champs **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 ce code, cliquez sur **Oui**.

   Pour saisir 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

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

DANS CETTE SECTION

MENU DE L'APPLICATION

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

Kaspersky Endpoint Security 8 for Smartphone propose les onglets suivants :

- **État de protection** : affiche l'état de tous les composants de l'application.
- **Contacts personnels** : masque les informations confidentielles sur l'appareil.
- **Antivol** : protège des données stockées sur l'appareil en cas de perte ou de vol.
- **Anti-Spam** : filtrage des SMS et des appels 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 composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection (cf. ill. ci-après).

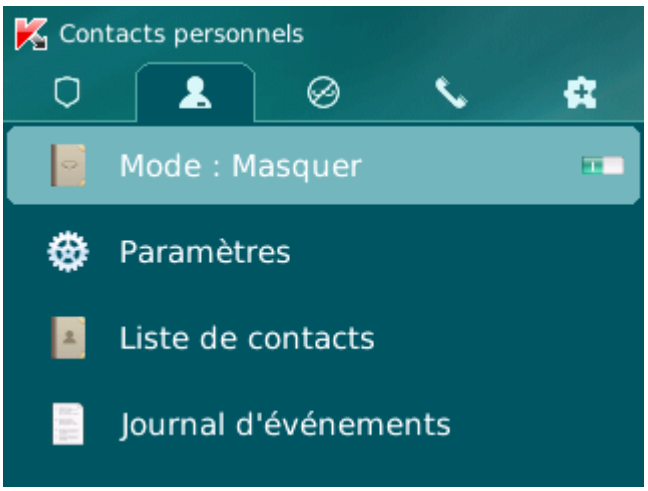


Figure 7: Fenêtre de l'état de la protection

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

- **Contacts personnels** : état de la dissimulation des informations confidentielles (cf. la rubrique "Dissimulation des informations confidentielles" à la page 46).

L'état **Afficher** signifie que la fonction de la dissimulation des informations confidentielles est désactivée. L'état **Masquer** signifie que la fonction de la dissimulation des informations confidentielles est activée.

- **Anti-Spam** : mode de filtrage des appels et des SMS (cf. rubrique "Filtrage des appels et des SMS entrants" à la page 26).

- **Verrouillage**, **Suppression**, **SIM-Surveillance**, **Géolocalisation** : états de la fonction Antivol (cf. rubrique "Protection des données en cas de perte ou de vol de l'appareil" à la page 37).

  L'état **Activée** signifie que la fonction Antivol est activée. L'état **Désactivé** 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 Anti-Spam qui interdit la réception d'appels et de SMS non sollicités sur la base des listes noire et blanche que vous avez créées. De plus, la section décrit comment sélectionner le mode de filtrage Anti-Spam des appels et des SMS entrants, comment configurer les paramètres avancés de filtrage pour les appels et les SMS entrants et comment créer la liste noire et la liste blanche.

DANS CETTE SECTION

A PROPOS DU COMPOSANT ANTI-SPAM

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

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

- Numéro de téléphone qu'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche.

- Type d'événement qu'Anti-Spam refuse pour la liste noire et accepte pour la liste blanche. Types d'informations représentés : appels et SMS, appels seuls, SMS seuls.

- Expression clé qui permet à Anti-Spam d'identifier si les SMS sont sollicités ou non. S'il s'agit de la liste noire, Anti-Spam va refuser les SMS avec cette expression clé et accepter les autres SMS sans cette expression clé. S'il s'agit de la liste blanche, Anti-Spam va accepter les SMS avec cette expression et refuser les SMS sans cette expression.

Anti-Spam filtre les SMS et les appels selon le mode sélectionné (cf. la rubrique "Présentation des modes d'Anti-Spam" à la page 27). Anti-Spam analyse selon le mode sélectionné chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non (spam). L'analyse se termine dès qu'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique "Journaux du logiciel" à la page 53).

PRESENTATION DES MODES D'ANTI-SPAM

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

Les modes de fonctionnement Anti-Spam disponibles :

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

Vous pouvez modifier le mode d'Anti-Spam (cf. la rubrique "Modification du mode d'Anti-Spam" à la page 27). Le mode actuel d'Anti-Spam s'affiche sous l'onglet **Anti-Spam** à côté de l'option **Mode**.

MODIFICATION DU MODE D'ANTI-SPAM

Pour sélectionner le mode d'Anti-Spam, procédez comme suit :

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

   L'écran **Anti-Spam** s'ouvre.

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

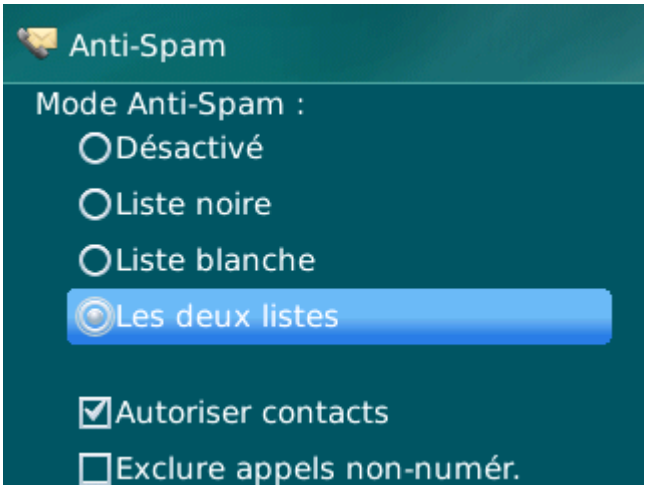


Figure 8: modification du mode de l'Anti-Spam

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 Anti-Spam. Chacun de ces enregistrements contient les informations suivantes :

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

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

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

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique "Journaux de l'application" à la page 53).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE "NOIRE"

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

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

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

   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 qu'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour 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. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS.

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

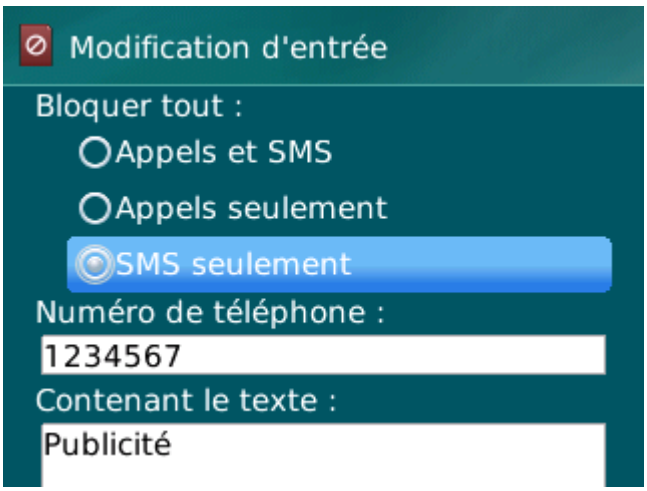


Figure 9: paramètres d'un enregistrement de la liste noire

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 laliste noire de l'Anti-Spam, exécutez les opérations suivantes :

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

   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 qu'Anti-Spam refusera pour les numéros de la liste noire :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seulement :** bloque uniquement les appels entrants.
     - **SMS seulement** : bloque uniquement les SMS entrants.
   - **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour 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. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
   - **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Anti-Spam refuse uniquement les SMS avec l'expression clé et accepte tous les autres SMS.

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

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

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

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

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

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

   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, appuyez sur le bouton **Oui**.

Pour purger laliste noire d'Anti-Spam, procédez comme suit :

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

   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, appuyez sur le bouton **Oui**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

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

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

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

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

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

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

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

   L'écran **Liste blanche** s'ouvre.

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

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

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

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

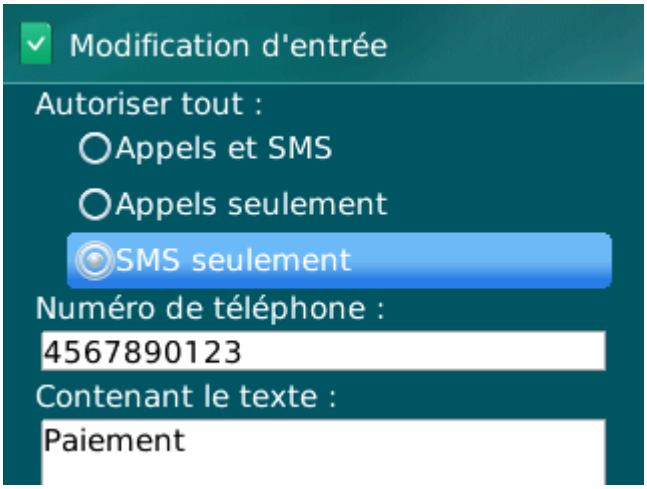


Figure 10: paramètres d'un enregistrement de la liste blanche

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 d'Anti-Spam, exécutez les opérations suivantes :

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

   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.

   - **Bloquer tout** : type d'événements en provenance du numéro de téléphone qu'Anti-Spam refusera pour les numéros de la liste noire :

     - **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 Anti-Spam. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques "*" et "?" (où "*" représente n'importe quel nombre de caractères et "?", n'importe quel caractère unique). Il s'agit, par exemple, du numéro *1234 ? de la liste blanche. Anti-Spam refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.

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

     Si vous souhaitez recevoir tous les SMS en provenance d'un numéro de la liste blanche, laisser le champ **Contenant le texte** de cet enregistrement 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 d'Anti-Spam, procédez comme suit :

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

   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 d'Anti-Spam, procédez comme suit :

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

   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 Anti-Spam **Les deux listes** ou **Liste blanche** (cf. la rubrique "**Présentation des modes d'Anti-Spam**" à la page 27) est sélectionné, vous pouvez également définir la réaction Anti-Spam aux SMS ou aux appels dont les numéros ne figurent pas dans les Contacts. Anti-Spam permet d'élargir la liste blanche en y introduisant les numéros des contacts.

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

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

   L'écran **Anti-Spam** s'ouvre.

2. Choisissez la valeur de paramètre **Autoriser contacts** (cf. ill. ci-après) :

   - Pour qu'Anti-Spam considère un numéro des contacts comme un ajout à la liste blanche et qu'il n'accepte pas les SMS et les appels en provenance de numéros qui ne figurent pas dans les Contacts, cochez la case **Autoriser contacts** ;

   - Pour qu'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini d'Anti-Spam, décochez la case **Autoriser contacts**.

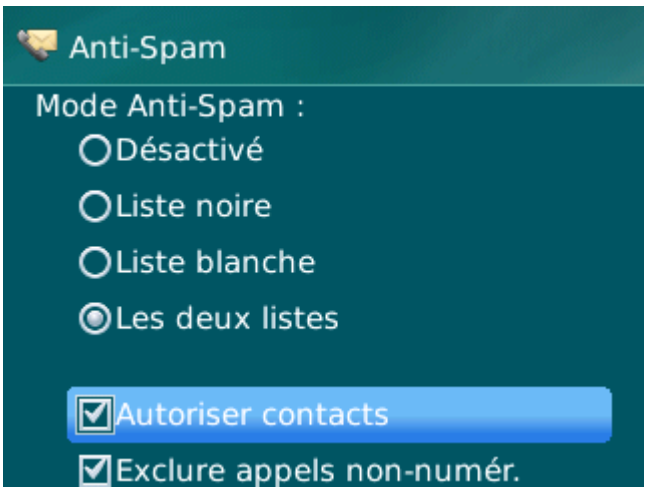


Figure 11: réaction d'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

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

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode choisi pour Anti-Spam est **Les deux listes** ou **Liste noire** (cf. la rubrique "**Présentation des modes d'Anti-Spam**" à la page 27), vous pouvez enrichir la liste noire en y ajoutant tous les numéros sans chiffres (composés de lettres). Si cette case est cochée, Anti-Spam traite les appels et les SMS en provenance des numéros sans chiffres comme s'il s'agit des numéros de la liste noire.

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

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

2. L'écran **Anti-Spam** s'ouvre.

3. Choisissez une valeur pour le paramètre **Exclure appels non-numériques** (cf. ill. ci-après) :

   - afin qu'Anti-Spam bloque les messages en provenance de numéros sans chiffres, cochez la case **Exclure appels non-numériques** ;

   - afin qu'Anti-Spam filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour Anti-Spam, décochez la case **Exclure appels non-numériques**.

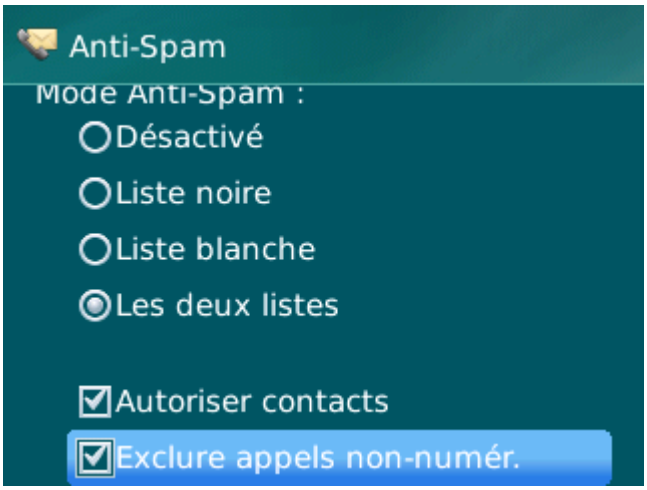


Figure 12: Sélection des actions exécutées par Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres

4. 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 d'Anti-Spam**" à la page 27), Anti-Spam 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, Anti-Spam vous invitera à ajouter ce numéro sur une des listes.

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 dans la liste noire**.

- Pour accepter le SMS et ajouter le numéro de téléphone de l'expéditeur à la liste blanche, cliquez sur **Ajouter dans la liste blanche**.

- Pour accepter le SMS sans ajouter le numéro de téléphone de l'expéditeur dans aucune des listes, cliquez sur **Ignorer**.

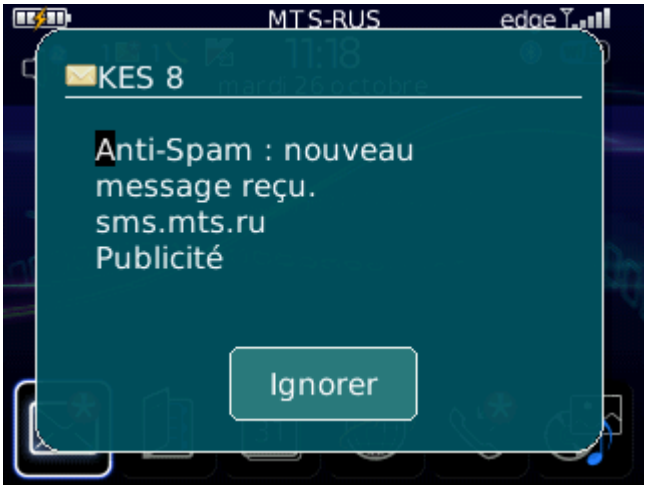


Figure 13: notification d'Anti-Spam sur le SMS reçu

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique "Journaux de l'application" à la page 53).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Si le mode choisi est **Les deux listes** (cf. la rubrique "**Présentation des modes d'Anti-Spam**" à la page 27), Anti-Spam 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, Anti-Spam vous invitera à ajouter ce numéro sur une des listes (cf. ill. ci-après).

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

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

Figure 14: notification d'Anti-Spam sur le SMS reçu

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique "Journaux de l'application" à la page 53).

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

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

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

DANS CETTE SECTION

À PROPOS DU COMPOSANT ANTIVOL

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

Antivol dispose des fonctions suivantes :

- **Verrouillage** permet de verrouiller l'appareil à distance et de définir le texte qui apparaîtra à l'écran de l'appareil bloqué.
- **Suppression** permet de supprimer à distance les données personnelles de l'utilisateur (entrées dans les Contacts, SMS, galerie, calendrier, journaux, paramètres de connexion à Internet), ainsi que les données de la carte mémoire et les dossiers de la liste à supprimer.
- **SIM-Surveillance** permet de garder le numéro de téléphone en cas de remplacement de la carte SIM et de verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte. Le message avec le nouveau numéro de téléphone est envoyé vers le numéro de téléphone et/ou l'adresse de la messagerie électronique que vous avez 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 depuis un autre appareil mobile (cf. la rubrique "Lancement à distance de la fonction Antivol" à la page 45).

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 sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique "Journaux de l'application" à la page 53).

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

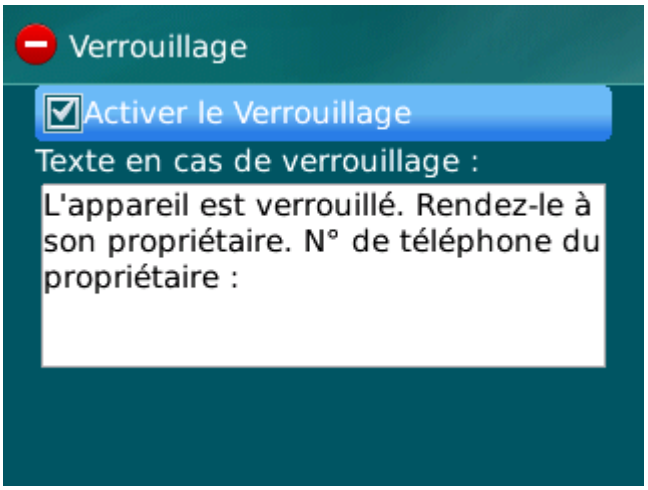


Figure 15: paramètres de la fonction Verrouillage

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

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

SUPPRESSION DE DONNEES PERSONNELLES

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

- données personnelles de l'utilisateur (entrées des Contacts, calendrier, messages électroniques, journal des appels) ;
- données sur la carte mémoire ;
- les fichiers de la liste des dossiers à supprimer (cf. rubrique "Composition de la liste des dossiers à supprimer" à la page 41).

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. Sélectionnez **Antivol**, choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Suppression** s'ouvre.

3. Cochez la case **Activer la Suppression**.

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**.

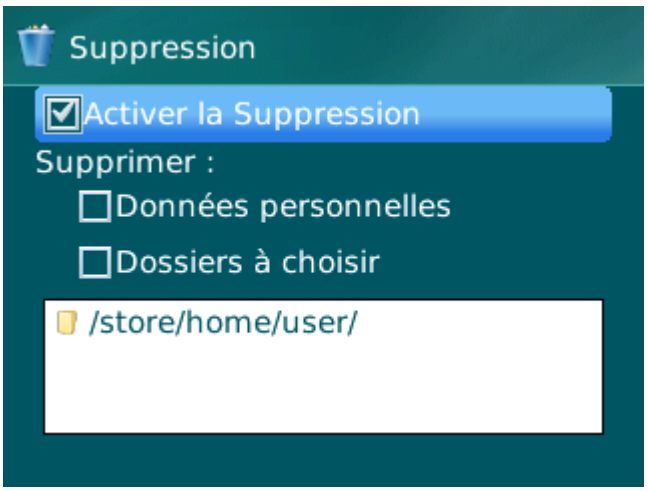


Figure 16: paramètres de la fonction de suppression de données

5. Procédez à la composition de la liste des dossiers à supprimer (cf. la rubrique "Composition de la liste des dossiers à supprimer" à la page 41).
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 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 l'autre appareil un message SMS, contenant le texte `wipe:<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.

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. Sélectionnez **Antivol**, choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

2. Ouvrez la liste des dossiers à supprimer.

3. Choisissez l'option **Menu** → **Ajouter un dossier** (cf. ill. ci-après).

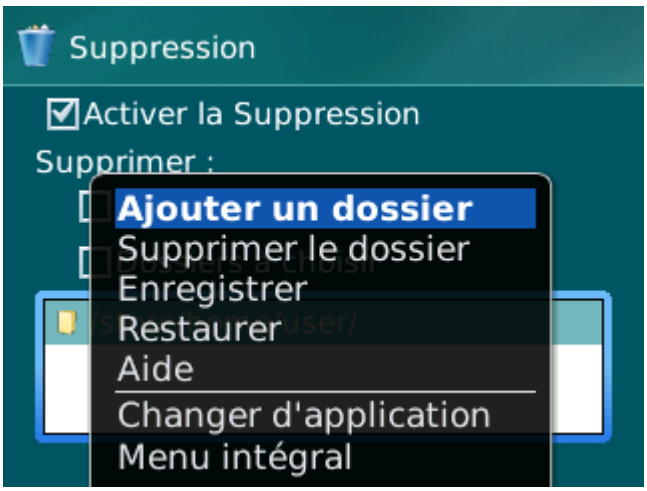


Figure 17: ajout d'un dossier

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. Sélectionnez **Antivol**, choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

2. Ouvrez la liste des dossiers à supprimer.

3. Sélectionnez un dossier dans 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. Sélectionnez **Antivol**, choisissez 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.

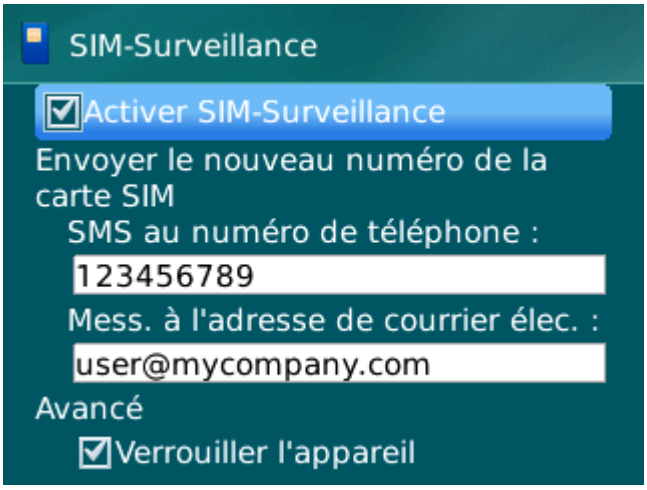


Figure 18: paramètres de la fonction SIM-Surveillance

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 Localisation 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 Localisation à intervalles réguliers.

Pour activer la fonction Localisation, procédez comme suit :

1. Sous l'onglet **Antivol**, sélectionnez l'option **Géolocalisation**.

   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 **Mess. à l'adresse de courrier élec.** l'adresse électronique (cf. ill. ci-après).

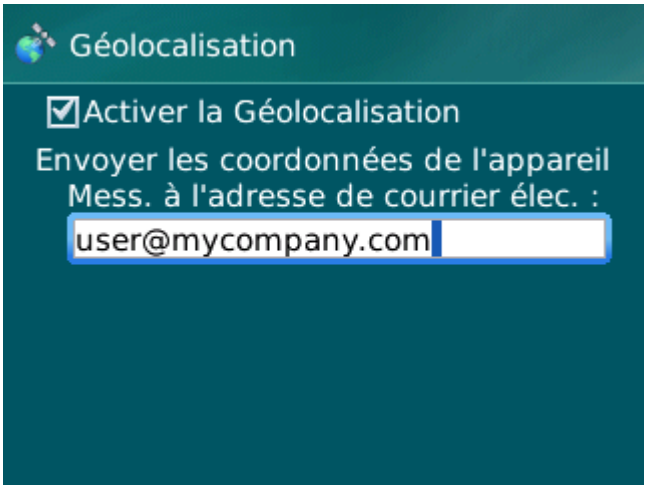


Figure 19: paramètres de la fonction Localisation

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

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

- Utilisez sur un autre appareil mobile l'application de Kaspersky Lab pour les appareils mobiles (par exemple, Kaspersky Endpoint Security 8) 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. Sélectionnez **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 composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone :

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

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

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

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

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

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

1. Sélectionnez **Avancé**, 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 38).
   - **Suppression** (cf. la rubrique "**Suppression de données personnelles**" à la page 39).
   - **Géolocalisation** (cf. la rubrique "**Détermination des coordonnées géographiques de l'appareil**" à la page 43)
   - **Contacts personnels** (cf. la rubrique "**Dissimulation des informations confidentielles**" à la page 46).

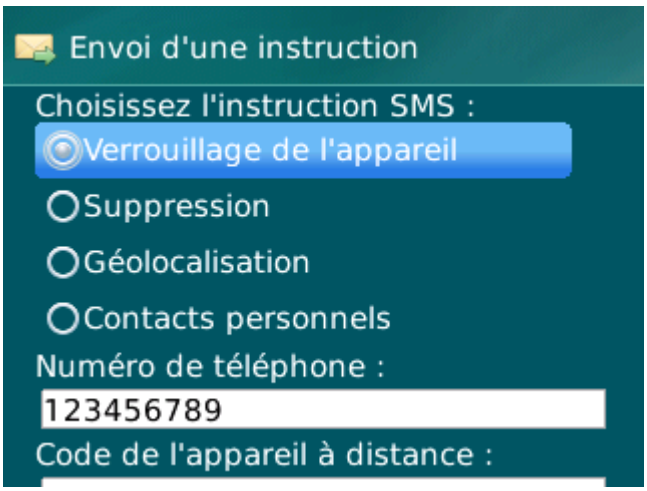


Figure 20: lancement à distance des fonctions Antivol et Contacts personnels

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**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

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

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

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

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

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. la rubrique "Journaux de l'application" à la page 53).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

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

Les modes suivants sont prévus pour Contacts personnels :

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

Vous pouvez configurer l'activation automatique (cf. rubrique "Activation automatique de Contacts personnels" à la page 47) de la dissimulation des données personnelles ou son activation à distance depuis un autre appareil (cf. rubrique "Activation de la dissimulation des informations confidentielles à distance" à la page 48).

L'état actuel de dissimulation des informations confidentielles est affiché sous l'onglet **Contacts personnels** à côté de l'option **Mode**.

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

ACTIVATION/DESACTIVATION DE CONTACTS PERSONNELS

Pour modifier le mode des contacts personnels,

sous l'onglet **Contacts personnels**, sélectionnez **Mode** (cf. ill. ci-après).

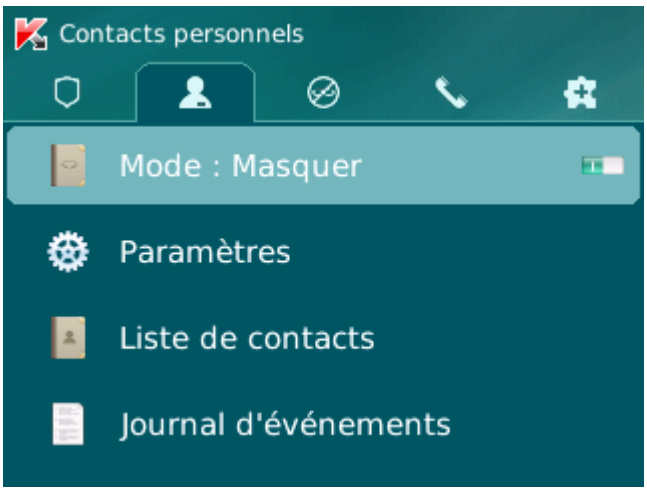


Figure 21: modification du mode de Contacts personnels

Le mode actuel des Contacts personnels s'affiche à côté de l'option **Mode**.

L'icône de basculement à droite de l'option **Mode** changera en fonction du mode sélectionné.

ACTIVATION AUTOMATIQUE DE CONTACTS PERSONNELS

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

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

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

1. Sélectionnez sous l'onglet **Contacts personnels** l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

2. Cochez la case **Masquer automatiq.** dans le groupe **Activ. automatique** (cf. ill. ci-après).

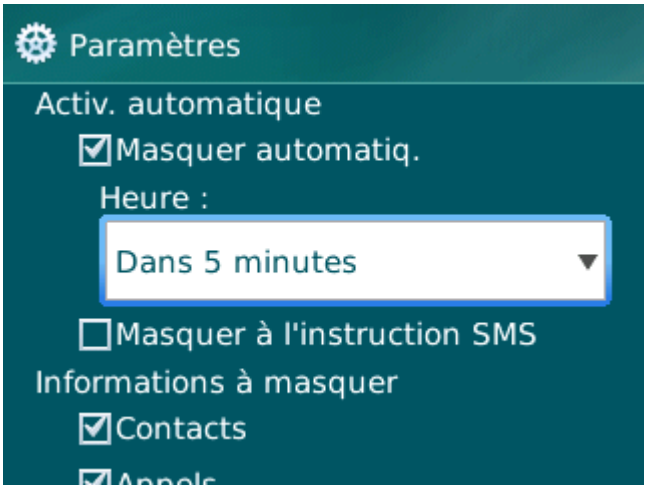


Figure 22: paramètres de lancement automatique de Contacts personnels

3. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, choisissez une des valeurs prédéfinies pour le paramètre **Heure** :

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

4. Sélectionnez **Menu** → **Enregistrer**.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

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

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

1. Sélectionnez sous l'onglet **Contacts personnels** l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

2. Cochez la case **Masquer à l'instruction SMS** (cf. ill. ci-après).

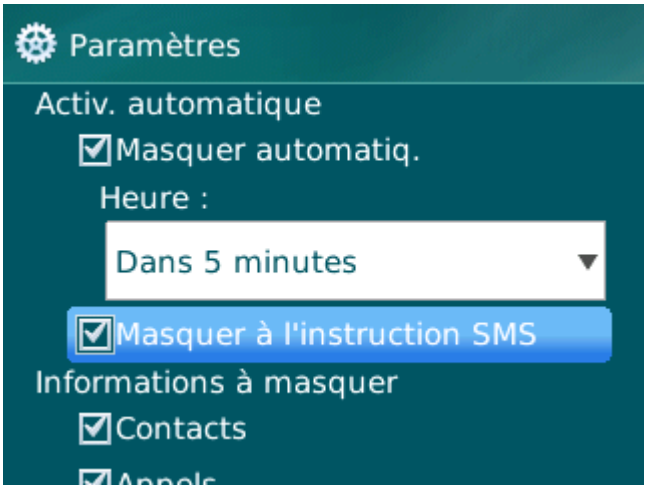


Figure 23 : paramètres d'activation à distance du composant Contacts personnels

3. Sélectionnez **Menu** → **Enregistrer**.

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

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

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra un SMS qui déclenchera la dissimulation des informations confidentielles.

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

Pour activer à distance depuis un autre appareil mobile la dissimulation des informations confidentielles à l'aide d'une instruction SMS spéciale, procédez comme suit :

1. Sélectionnez **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 **Contacts personnels**.

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**.

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

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

envoyez à l'appareil un SMS contenant le texte `hide:<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.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

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

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

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

1. Sous l'onglet **Contacts personnels**, sélectionnez l'option **Paramètres**.

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

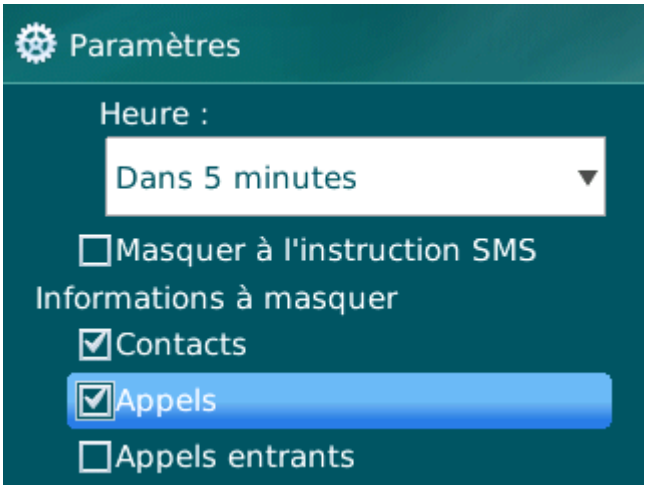


Figure 24: sélection des informations et des événements à dissimuler

2. Sélectionnez dans le groupe **Informations à masquer** les informations et les événements qui seront masqués pour les numéros confidentiels. Pour ce faire, cochez les cases des paramètres requis. Les paramètres suivants sont prévus:

   - **Contacts :** masque toutes les informations relatives aux numéros confidentiels.
   - **Appels** : accepte les appels en provenance des numéros confidentiels mais ne définit pas le numéro de l'appelant et n'affiche pas les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).
   - **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité "occupé"). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.

3. Sélectionnez **Menu** → **Enregistrer**.

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

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

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

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter à la Liste de contacts les numéros de téléphones en mode manuel ou les importer depuis les Contacts.

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

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

1. Sélectionnez **Contacts personnels**, choisissez l'option **Liste des contacts**.

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

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

   - Pour ajouter un numéro depuis les Contacts, sélectionnez **Menu** → **Ajouter le contact**. Sélectionnez dans l'écran **Choisir un contact** qui apparaît l'entrée requise des Contacts et sélectionnez **Menu** → **Sélectionner**.

   - Pour ajouter un numéro manuellement, sélectionnez **Menu** → **Ajouter le numéro**. Dans l'écran **Ajouter un numéro** qui apparaît, remplissez le champ **Numéro de téléphone**, puis sélectionnez **Menu** → **Sélectionner**.

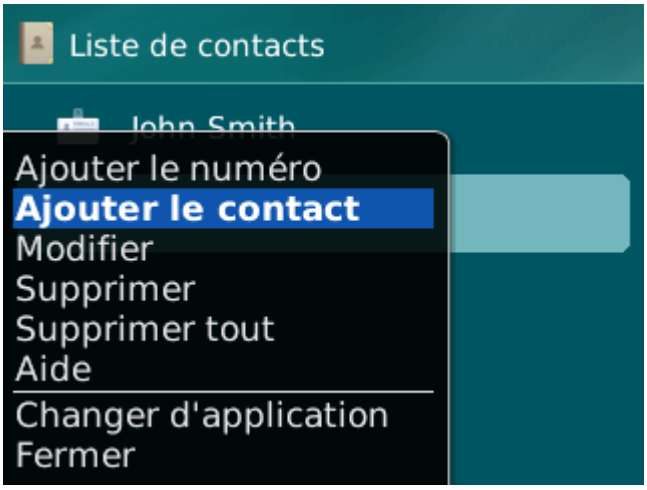


Figure 25: ajout d'un enregistrement à la liste des contacts confidentiels

Le numéro est alors ajouté à la liste des contacts.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

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

Seuls les numéros qui ont été saisis manuellement dans la Liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans les Contacts.

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

1. Sélectionnez **Contacts personnels**, choisissez l'option **Liste des contacts**.

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

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

   L'écran **Changer le numéro** apparaît.

3. Modifiez les données dans le champ **Numéro de téléphone**.

4. Une fois la modification terminée, sélectionnez **Menu** → **Enregistrer**.

Le numéro sera modifié

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

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

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

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

  1. Sélectionnez **Contacts personnels**, choisissez l'option **Liste des contacts**.

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

  2. Sélectionnez le numéro à supprimer, puis choisissez **Menu** → **Supprimer**.

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

  3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

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

  1. Sélectionnez **Contacts personnels**, choisissez l'option **Liste des contacts**.

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

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

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

  3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

JOURNAUX DU LOGICIEL

La section présente les informations sur les journaux où sont consignés les détails du fonctionnement de chaque composant 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

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

AFFICHAGE DES EVENEMENTS DU JOURNAL

- *Pour consulter les enregistrements dans le journal du composant,*

  sous l'onglet du composant nécessaire, choisissez l'option **Journal des événements**.

Le journal du composant 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 composants 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 composant, 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 composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section présente les fonctionnalités supplémentaires de Kaspersky Endpoint Security 8 for Smartphone : comment modifier le code secret de l'application, comment administrer les notifications sonores Anti-Spam et comment activer / désactiver l'affichage des astuces avant la configuration des paramètres de chaque composant.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

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

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

  1. 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**.

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

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

1. Sélectionnez **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 astuce 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'utilisateur doit avoir une 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, 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 Anti-Spam.

Type d'événements en provenance de ce numéro qu'Anti-Spam accepte. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.

Expression clé qui permet à Anti-Spam d'identifier des SMS sollicités (qui ne sont pas du spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

Liste noire

Les entrées de cette liste contiennent les informations suivantes :

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

Type d'événement en provenance de ce numéro qu'Anti-Spam bloque. Types d'événements représentés : appels et SMS, appels seuls, SMS seuls.

Expression clé qui permet à Anti-Spam d'identifier des SMS non sollicités (spam). Anti-Spam accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS.

M

Masque du numero de telephone

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

N

NON-NUMERIQUES

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

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

SYSTEME D'ADMINISTRATION DISTANTE

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

KASPERSKY LAB

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes senior de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections anti-virus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des premiers fabricants de logiciels antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-Virus : il assure une protection complète de tous les systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. La base anti-virus de Kaspersky Lab est mise à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

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

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

UTILISATION DE CODE TIERS

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

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

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

INDEX

A

C

D

E

F

I

J

K

L

M

O

S

V