

Kaspersky Mobile Security 9

for Microsoft Windows Mobile

The Kaspersky logo is displayed diagonally across a white diagonal band. The word "KASPERSKY" is in a dark teal, bold, sans-serif font. The letter "A" has a small red triangle pointing upwards inside it. The letter "S" has a small red triangle pointing downwards inside it. The letter "Y" has a small red triangle pointing downwards inside it. To the right of "KASPERSKY" is a red "lab" logo, where the letters "lab" are in a stylized, rounded font, with the "a" being a circle and the "l" and "b" having a unique shape.

Guide de l'utilisateur

VERSION DE L'APPLICATION : 9.0

Cher utilisateur,

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

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

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

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

Ce document peut être modifié sans préavis. La version la plus récente est disponible sur le site de Kaspersky Lab à l'adresse suivante <http://www.kaspersky.com/fr/docs>.

Kaspersky Lab ne peut être tenu responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. Kaspersky Lab n'assume pas non plus la responsabilité en cas de dommages liés à l'utilisation de ces textes.

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

Date d'édition : 25/01/2011

© 1997–2011 Kaspersky Lab ZAO. Tous droits réservés.

<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(E) 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.

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 patch, 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. Le Titulaire des droits convient par la présente de Vous accorder 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 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 spécifiés dans les licences que vous avez obtenues auprès du Titulaire des droits, *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 ou stipulé dans le contrat additionnel.

- 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 ou stipulé dans le contrat additionnel.
- 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 ou celle stipulée dans le contrat additionnel.
- 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 ou celle stipulée dans le contrat additionnel.
- 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 (7 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. Si le Titulaire des droits fixe une autre durée pour la période d'évaluation unique applicable, Vous serez informé(e) par notification.
- 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 d'utilisation du Logiciel 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.
- 3.10. Si vous avez acheté le logiciel avec un code d'activation valide pour la localisation de la langue parlée dans la région où il a été acquis auprès du détenteur des droits ou de ses partenaires, vous ne pouvez pas activer le logiciel avec le code d'activation prévu pour la localisation d'une autre langue.
- 3.11. Si vous avez acquis le logiciel prévu pour fonctionner avec un opérateur de télécommunications en particulier, ce logiciel n'est utilisable qu'en association avec l'opérateur indiqué au moment de l'acquisition.
- 3.12. En cas de restrictions précisées dans les clauses 3.10 et 3.11, vous trouverez des informations concernant ces restrictions sur l'emballage et/ou le site Web du détenteur et/ou de ses partenaires.

4. Assistance technique

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>

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 pièce 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 sauf aux conditions énoncées dans le contrat additionnel.
- 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, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans le contrat additionnel.
- 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. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.
- 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 déchargé 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 adaptés à Votre cas.
- 6.3. Vous reconnaissez, acceptez et convenez que le Titulaire des droits n'est pas responsable ou ne peut être tenu pour responsable de la suppression des données que vous autorisez. Les données mentionnées peuvent inclure des informations personnelles ou confidentielles.
- 6.4. 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.
- 6.5. 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.
- 6.6. 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.
- 6.7. 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 PAR LA LÉGISLATION EN VIGUEUR, LE « 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

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 DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS 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 SERA 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

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 être 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 que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.
- 9.3 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

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

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

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. Coordonnées 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

© 1997-2011 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et toute documentation l'accompagnant font l'objet de droits d'auteur et sont protégés par les lois sur la protection des droits d'auteur et les traités internationaux sur les droits d'auteur, ainsi que d'autres lois et traités sur la propriété intellectuelle.

TABLE DES MATIERES

A PROPOS DE CE MANUEL.....	13
Dans ce document.....	13
Conventions.....	16
SOURCES D'INFORMATIONS COMPLEMENTAIRES.....	17
Sources de données pour des consultations indépendantes	17
Contacter le Département commercial	18
Publier des messages sur le forum concernant les applications de Kaspersky Lab.....	18
Contacter l'Equipe de rédaction de la documentation.....	18
KASPERSKY MOBILE SECURITY 9.....	19
Nouveautés de Kaspersky Mobile Security 9	20
Kit de distribution	20
Spécifications matérielles et logicielles.....	20
INSTALLATION DE KASPERSKY MOBILE SECURITY 9.....	21
SUPPRESSION DE L'APPLICATION	22
MISE A JOUR DE L'APPLICATION	25
PREMIERS PAS	27
Activation du logiciel	27
Activation de la version commerciale	28
Activation de l'abonnement à Kaspersky Mobile Security 9	30
Achat du code d'activation en ligne.....	31
Activation de la version d'évaluation	31
Saisie du code secret	32
Activation de la fonction de restauration du code secret	33
Restauration du code secret.....	33
Démarrage du logiciel.....	34
Mise à jour des bases du programme	34
Recherche de virus sur l'appareil.....	35
Informations sur le programme.....	35
GESTION DE LA LICENCE	36
Présentation du contrat de licence	36
A propos des licences de Kaspersky Mobile Security 9	37
Affichage des informations de licence	38
Renouvellement de la licence.....	38
Renouvellement de la licence à l'aide du code d'activation	39
Renouvellement de la licence en ligne.....	40
Renouvellement de la licence à l'aide de l'activation de l'abonnement	41
Refus de l'abonnement	42
Renouvellement de l'abonnement.....	43
INTERFACE DE L'APPLICATION.....	44
Fenêtre d'état de la protection	44
Menu de l'application	46

PROTECTION DU SYSTEME DE FICHIERS	48
Présentation de la protection	48
Activation et désactivation de la protection	48
Sélection des actions à appliquer sur les objets identifiés	50
ANALYSE DE L'APPAREIL	52
À propos de l'analyse à la demande	52
Exécution manuelle d'une analyse	53
Exécution de l'analyse programmée	54
Sélection du type d'objet à analyser	55
Configuration de l'analyse des archives	56
Sélection des actions à appliquer sur les objets identifiés	57
QUARANTAINE DES OBJETS MALVEILLANTS	59
À propos de la quarantaine	59
Affichage des objets en quarantaine	59
Restauration d'objets de la quarantaine	60
Suppression d'objets de la quarantaine	61
FILTRAGE DES APPELS ET DES SMS ENTRANTS	62
A propos du Filtre des appels et SMS	62
A propos des Modes du Filtre des appels et SMS	63
Modification du mode Filtre des appels et SMS	63
Composition de la liste noire	64
Ajout d'une entrée à la liste noire	65
Modification d'un enregistrement de la liste noire	66
Suppression d'un enregistrement de la liste noire	67
Composition de la liste blanche	68
Ajout d'une entrée à la liste blanche	68
Modification d'un enregistrement de la liste blanche	69
Suppression d'un enregistrement de la liste blanche	70
Réaction aux SMS et appels de contacts qui ne figurent pas dans le répertoire téléphonique	71
Réaction aux SMS en provenance de numéros sans chiffres	72
Sélection de l'action à appliquer sur les SMS entrants	73
Sélection de l'action à appliquer sur des appels entrants	74
RESTRICTIONS SUR LES APPELS ET LES SMS SORTANTS. CONTROLE PARENTAL	75
À propos du Contrôle parental	75
Modes du Contrôle parental	75
Activation/désactivation du Contrôle parental	76
Composition de la liste noire	77
Ajout d'une entrée à la liste "noire"	77
Modification d'un enregistrement de la liste noire	78
Suppression d'un enregistrement de la liste noire	79
Composition de la liste blanche	79
Ajout d'une entrée à la liste blanche	80
Modification d'un enregistrement de la liste blanche	81
Suppression d'un enregistrement de la liste blanche	82
PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL	83
A propos du composant Antivol	83
Verrouillage de l'appareil	84

Suppression de données personnelles.....	86
Composition de la liste des dossiers à supprimer.....	88
Contrôle du remplacement de la carte SIM sur l'appareil	90
Détermination des coordonnées géographiques de l'appareil	91
Lancement à distance de la fonction Antivol.....	94
DISSIMULATION DES INFORMATIONS PERSONNELLES.....	96
Présentation du composant Contacts personnels	96
Présentation des modes de Contacts personnels	97
Activation/désactivation de Contacts personnels.....	97
Activation automatique de Contacts personnels.....	98
Activation de la dissimulation des informations confidentielles à distance	99
Composition de la liste des numéros confidentiels	101
Ajout d'un numéro à la liste des numéros confidentiels	102
Modification d'un numéro de la liste des numéros confidentiels	103
Suppression d'un numéro de la liste des numéros confidentiels.....	103
Sélection des informations à dissimuler : Contacts personnels	104
FILTRAGE DE L'ACTIVITE RESEAU. PARE-FEU	106
À propos du Pare-feu	106
Activation/désactivation du Pare-feu	106
Sélection du mode Pare-feu	107
Notifications sur les blocages	108
CHIFFREMENT DES DONNEES PERSONNELLES.....	109
À propos du chiffrement.....	109
Chiffrement des données.....	110
Déchiffrement des données.....	111
Interdiction d'accès aux données chiffrées	113
MISE A JOUR DES BASES DU PROGRAMME	115
À propos de la mise à jour des bases.....	115
Affichage des informations sur les bases	116
Mise à jour manuelle	116
Planification des mises à jour	117
Mise à jour en itinérance.....	118
JOURNAUX DU LOGICIEL	120
À propos des journaux.....	120
Affichage des événements du journal.....	120
Suppression des enregistrements du journal.....	121
CONFIGURATION DES PARAMETRES COMPLEMENTAIRES	122
Modification du code secret.....	122
Affichage des astuces	122
Administration des notifications sonores.....	123
CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE	124
GLOSSAIRE	125
KASPERSKY LAB.....	128
INFORMATIONS SUR LE CODE TIERS	129
Code de programmation diffusé	129

ADB129

ADBWINAPI.DLL129

ADBWINUSBAPI.DLL.....129

Autres informations.....131

INDEX132

A PROPOS DE CE MANUEL

Le présent document est un Guide d'installation, de configuration et d'utilisation de l'application Kaspersky Mobile Security 9. Ce document est destiné au grand public.

Buts du document :

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

DANS CETTE SECTION

Dans ce document	13
Conventions	16

DANS CE DOCUMENT

Ce document reprend les sections suivantes :

Sources d'informations complémentaires

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

Kaspersky Mobile Security 9

Cette section contient une description des fonctionnalités de l'application et offre des informations succinctes sur ses composants et leurs fonctions principales. Cette section contient les informations concernant le pack livré. La section décrit également la configuration matérielle et logicielle requises pour l'installation de Kaspersky Mobile Security 9.

Installation de Kaspersky Mobile Security 9

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

Suppression de l'application

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

Mise à jour de l'application

Cette section contient les instructions qui vous aideront à mettre à jour la version de l'application.

Premiers pas

Cette section contient les informations sur le début de l'utilisation de Kaspersky Mobile Security 9 : activation de l'application, saisie du code secret, activation de la fonction de restauration du code secret, lancement du programme, mise à jour des bases antivirus et lancement de l'analyse antivirus de l'appareil.

Gestion de la licence

Cette section contient les informations sur les concepts de base utilisés pour l'octroi de licence de l'application. La section présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Mobile Security 9 et son renouvellement.

Interface de l'application

Cette section présente les informations sur les principaux composants de l'interface de Kaspersky Mobile Security 9.

Protection du système de fichiers

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

Analyse de l'appareil

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

Quarantaine des objets malveillants

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

Filtrage des appels et des SMS entrants

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

Restrictions sur les appels et les SMS sortants. Contrôle Parental

Cette section présente le composant Contrôle parental qui permet de restreindre les appels et les SMS sortants à certains numéros. Elle explique également comment établir des listes de numéros interdits ou autorisés et configurer les paramètres du Contrôle parental.

Protection des données en cas de perte ou de vol de l'appareil

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

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

Dissimulation des informations personnelles

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

Filtrage de l'activité réseau. Pare-feu

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

Chiffrement des données personnelles

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. La section décrit également comment chiffrer et déchiffrer les dossiers sélectionnés.

Mise à jour des bases du programme

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

Journaux du logiciel

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

Configuration des paramètres complémentaires

La section présente les informations sur les fonctionnalités complémentaires de Kaspersky Mobile Security 9 : comment modifier le code secret, comment administrer les notifications sonores de l'application et le rétro-éclairage, et comment activer / désactiver l'affichage des astuces, de l'icône de protection ou de la fenêtre d'état de la protection.

Contacter le Service d'assistance technique

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

Glossaire

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

Kaspersky Lab

La section reprend les informations relatives à Kaspersky Lab.

Informations sur le code tiers

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

Index

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

CONVENTIONS

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

Tableau 1. Conventions

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

SOURCES D'INFORMATIONS COMPLEMENTAIRES

Pour toute question sur l'installation ou l'utilisation de Kaspersky Mobile Security 9, vous pouvez rapidement trouver des réponses en utilisant plusieurs sources d'information. Vous pouvez sélectionner celle qui vous convient le mieux en fonction de l'importance et de l'urgence du problème.

DANS CETTE SECTION

Sources de données pour des consultations indépendantes	17
Contacter le Département commercial	18
Publier des messages sur le forum concernant les applications de Kaspersky Lab	18
Contacter l'Equipe de rédaction de la documentation	18

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

- page de l'application sur le site de Kaspersky Lab ;
- page du logiciel, sur le site du serveur du Service d'assistance technique (Knowledge Base) ;
- aide électronique et astuces ;
- documentation.

Page sur le site Web de Kaspersky Lab

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

Sur cette page vous allez retrouver les informations générales sur Kaspersky Mobile Security 9, ses possibilités et ses particularités. Vous pouvez également acheter Kaspersky Mobile Security 9 dans notre boutique en ligne.

Page de l'application sur le serveur du Service d'assistance technique (Knowledge Base)

<http://support.kaspersky.fr>

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

Ces articles contiennent des informations utiles, des recommandations et les réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Mobile Security 9. Ils sont regroupés par thèmes, par exemple, "Mise à jour des bases" ou "Elimination des échecs". Les articles répondent non seulement à des questions sur Kaspersky Mobile Security 9, 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

Si vous avez des questions sur une fenêtre ou sur un onglet spécifiques de Kaspersky Mobile Security 9, vous disposez de l'aide contextuelle.

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

Documentation

Le Manuel de l'utilisateur contient des informations détaillées sur les fonctions de l'application, sur l'utilisation de Kaspersky Mobile Security 9, ainsi que des conseils et des recommandations pour la configuration.

La documentation au format PDF est fournie dans le pack du produit Kaspersky Mobile Security 9.

Vous pouvez également télécharger les fichiers sur le site de Kaspersky Lab.

CONTACTER LE DEPARTEMENT COMMERCIAL

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

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

Le service est offert en russe et en anglais.

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

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

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

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer de nouvelles discussions ou lancer des recherches.

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 l'objet, mettez "Kaspersky Help Feedback : Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 protège les appareils mobiles (ci-après les "appareils") tournant sous Symbian OS. L'application protège les données de l'appareil contre une infection par des menaces connues, refuse les SMS et les appels non sollicités, contrôle les connexions de réseau de l'appareil, chiffre les données, masque les informations pour les contacts confidentiels et protège les données confidentielles en cas de perte ou de vol de l'appareil. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application.

Kaspersky Mobile Security 9 reprend les composants suivants pour la protection :

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

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

- **État de protection.** Les états des composants de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection des données stockées sur l'appareil.
- **La mise à jour des bases antivirus de l'application.** La fonction permet de tenir à jour les bases antivirus de Kaspersky Mobile Security 9.
- **Journal des événements.** Les informations sur le fonctionnement de chacun des composants (par exemple, opération effectuée, détails sur un objet bloqué, rapport d'analyse ou mise à jour) sont consignées dans un journal d'événements spécifique.
- **Licence.** Au moment d'acheter Kaspersky Mobile Security 9, un contrat de licence est signé entre Kaspersky Lab et vous-mêmes vous donnant le droit d'utiliser l'application, de recevoir les mises à jour des bases antivirus de l'application et de contacter le Service d'assistance technique durant une période déterminée. La durée de validité de la licence ainsi que toute autre information requise pour le fonctionnement complet de l'application figurent dans la licence.

Grâce à la fonction **Licence**, vous pouvez obtenir des informations détaillées sur la licence que vous utilisez ainsi que renouveler la licence en cours.

Kaspersky Mobile Security 9 ne réalise pas de copies de sauvegarde des données en vue d'une restauration ultérieure.

DANS CETTE SECTION

Nouveautés de Kaspersky Mobile Security 9	20
Kit de distribution.....	20
Spécifications matérielles et logicielles	20

NOUVEAUTES DE KASPERSKY MOBILE SECURITY 9

Voici une présentation détaillée des nouveautés de Kaspersky Mobile Security 9.

Les nouvelles possibilités suivantes sont réalisées dans Kaspersky Mobile Security 9 :

- L'accès au programme est régi par un mot de passe.
- Pour les contacts confidentiels de la liste des contacts, le composant Contacts personnels permet de masquer les informations suivantes : entrées dans les Contacts, SMS, journal des appels, SMS reçus et appels entrants. Les informations confidentielles sont accessibles si la fonction de dissimulation est désactivée.
- Le composant Chiffrement permet de chiffrer les dossiers enregistrés dans la mémoire de l'appareil ou sur une carte mémoire. Le composant stocke les informations confidentielles en mode crypté et ne permet d'accéder aux informations chiffrées qu'après avoir saisi le code secret de l'application.
- L'application propose également une nouvelle fonction de service Affichage des astuces : Kaspersky Mobile Security 9 affiche une brève description du composant avant la configuration de ses paramètres.
- Vous pouvez directement acheter le code d'activation et renouveler la durée de validité de la licence depuis l'appareil mobile à l'aide de la fonction d'abonnement ou en ligne.

KIT DE DISTRIBUTION

Vous pouvez acquérir Kaspersky Mobile Security 9 via Internet (le kit de distribution et la documentation du programme sont disponibles au format numérique). Vous pouvez également acquérir Kaspersky Mobile Security 9 chez les revendeurs de téléphonie mobile. Pour des détails sur la méthode d'achat et le kit de distribution, contactez notre Département commercial au info@kaspersky.fr.

SPECIFICATIONS MATERIELLES ET LOGICIELLES

Kaspersky Mobile Security 9 peut être installé sur des appareils mobiles avec l'un des systèmes d'exploitation suivants :

- Microsoft Windows Mobile 5.0 ;
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

INSTALLATION DE KASPERSKY MOBILE SECURITY 9

L'installation de l'application sur l'appareil mobile s'effectue en plusieurs étapes.

Avant de lancer l'installation, il est conseillé de quitter toutes les autres applications sur l'appareil mobile.

➡ Pour installer Kaspersky Mobile Security 9, procédez comme suit :

1. Connectez l'appareil mobile à l'ordinateur à l'aide de l'application Microsoft ActiveSync.
2. Exécutez l'une des opérations suivantes :
 - Si vous avez acheté l'application sur CD, lancez l'installation automatique de Kaspersky Mobile Security 9 depuis le CD.
 - Si vous avez obtenu la distribution via Internet, copiez-la sur l'appareil mobile. Pour ce faire, appliquez l'une des méthodes suivantes :
 - depuis le site Internet de Kaspersky Lab ;
 - à l'aide de l'application Microsoft ActiveSync ;
 - à l'aide de la carte mémoire.
3. Lisez le contrat de licence conclut entre Kaspersky Lab et vous-même. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. Kaspersky Mobile Security 9 sera installé sur l'appareil. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**.
4. Choisissez la langue de l'interface de Kaspersky Mobile Security 9, puis cliquez sur **OK**.
5. Pour terminer l'installation, redémarrez l'appareil. Pour ce faire, cliquez sur **Redémarrer**.

L'application sera installée avec les paramètres recommandés par les experts de Kaspersky Lab.

SUPPRESSION DE L'APPLICATION

➡ Pour supprimer Kaspersky Mobile Security 9, procédez comme suit :

1. Déchiffrez les données sur votre appareil si elles avaient été cryptées à l'aide de Kaspersky Mobile Security 9 (cf. section "Déchiffrement des données" à la page [111](#)).
2. Désactivez Contacts personnels (cf. section Activation/désactivation du composant Contacts personnels à la page [97](#)).
3. Fermez Kaspersky Mobile Security 9. Pour ce faire, choisissez **Menu** → **Quitter**.
4. Supprimez Kaspersky Mobile Security 9. Pour ce faire, exécutez les actions suivantes :
 - a. Cliquez sur **Démarrer** → **Paramètres**.
 - b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système** (cf. ill. ci-après).



Figure 1 : onglet **Système**

- c. Sélectionnez **Kaspersky Mobile Security** dans la liste des applications installées puis cliquez sur **Supprimer** (cf. ill. ci-après).

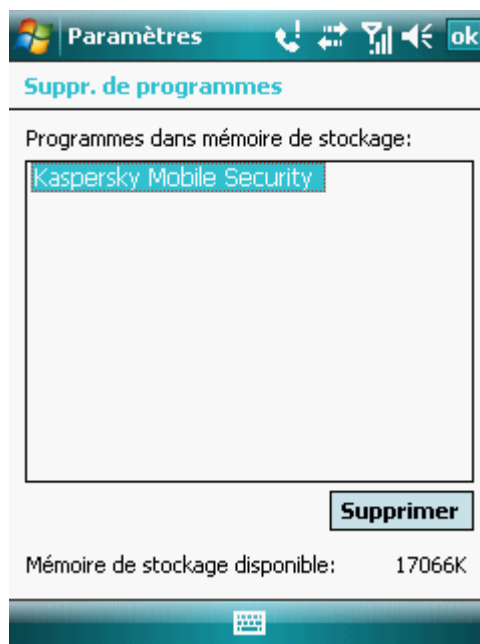


Figure 2 : sélection de l'application à supprimer

- d. Confirmez la suppression de l'application en cliquant sur **Oui** dans la fenêtre qui s'ouvre.
- e. Saisissez le code secret puis cliquez sur **OK**.

- f. Indiquez si vous voulez sauvegarder ou non les paramètres de l'application ainsi que les objets en quarantaine (cf. ill. ci-après) :
- Pour sauvegarder les paramètres de l'application ou les objets en quarantaine, cliquez sur **Conserver**.
 - Pour supprimer complètement une application, cliquez sur **Supprimer**.

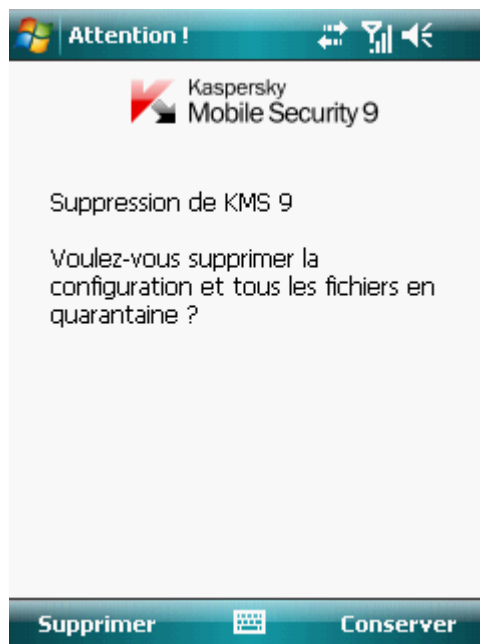


Figure 3 : suppression des paramètres de l'application

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

MISE A JOUR DE L'APPLICATION

Vous pouvez mettre à jour Kaspersky Mobile Security 9 en installant la version la plus récente de cette génération (par exemple, mettre à jour la version 9.0 à la version 9.2).

Si vous utilisez Kaspersky Mobile Security 8.0, vous pouvez passer à la version Kaspersky Mobile Security 9.

➤ *Pour mettre l'application à jour, procédez comme suit :*

1. Désactivez le chiffrement déchiffrez toutes les données (cf. section Déchiffrement des données à la page [111](#)).
2. Désactivez Contacts personnels (cf. section Activation/désactivation du composant Contacts personnels à la page [97](#)).
3. Quittez la version actuelle de Kaspersky Mobile Security. Pour ce faire, choisissez **Menu → Quitter**.
4. Copiez le fichier d'installation de l'application sur l'appareil. Pour ce faire, appliquez l'une des méthodes suivantes :
 - depuis le site Internet de Kaspersky Lab ;
 - à l'aide de l'application Microsoft ActiveSync ;
 - à l'aide de la carte d'extension mémoire.
5. Exécutez le fichier d'installation de Kaspersky Mobile Security 9 sur l'appareil.
6. Lisez attentivement le contrat de licence. Si vous êtes d'accord avec tous les termes, cliquez sur **J'accepte**. Vous serez d'abord invité à supprimer la version de l'application installée.
7. Pour confirmer la suppression de la version antérieure, cliquez sur **OK**.
8. Saisissez le code secret.
9. Indiquez si vous voulez sauvegarder ou non les paramètres de l'application et des objets en quarantaine :
 - Pour sauvegarder les paramètres de l'application ou les objets en quarantaine, cliquez sur **Conserver**.
 - Pour supprimer complètement une application, cliquez sur **Supprimer**.
10. Pour terminer la suppression, redémarrez l'appareil. Pour ce faire, cliquez sur **Redémarrer**.
11. Après le redémarrage de l'appareil, lancez l'installation de Kaspersky Mobile Security 9 (cf. section Installation de Kaspersky Mobile Security 9 à la page [21](#)).

Si la licence actuelle est toujours valide, alors l'application sera activée automatiquement. Si la licence n'est plus valide, activez l'application (cf. section Activation de l'application à la page [27](#)).

➤ *Pour passer de Kaspersky Mobile Security 8.0 à la version 9, procédez comme suit :*

1. Déchiffrez toutes les données si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security 8.0.
2. Fermez Kaspersky Mobile Security 9. Pour ce faire, choisissez **Menu → Quitter**.
3. Supprimez Kaspersky Mobile Security 9. Pour ce faire, exécutez les actions suivantes :
 - a. Cliquez sur **Démarrer → Paramètres**.
 - b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système**.

- c. Sélectionnez **Kaspersky Mobile Security** dans la liste des applications installées puis cliquez sur **Supprimer**.
 - d. Confirmez la suppression de l'application en cliquant sur **Oui** dans la fenêtre qui s'ouvre.
 - e. Saisissez le code secret défini dans la version antérieure de l'application, puis cliquez sur **OK**.
 - f. Supprimez tous les paramètres de Kaspersky Mobile Security 8.0 car ils sont incompatibles avec ceux de la version 9. Pour ce faire, cliquez sur **Supprimer**.
4. Redémarrez l'appareil pour terminer la suppression de Kaspersky Mobile Security 8.0.
 5. Passez à l'installation de Kaspersky Mobile Security 9 (cf. rubrique Installation de Kaspersky Mobile Security 9 à la page [21](#)).
 6. Passez à l'activation de l'application (cf. section Activation de l'application à la page [27](#)).

Si la licence pour Kaspersky Mobile Security 8.0 est toujours valide, activez la version 9.0 à l'aide du code d'activation de la version 8.0.

PREMIERS PAS

Cette section contient les informations sur le début de l'utilisation de Kaspersky Mobile Security 9 : activation de l'application, saisie du code secret, activation de la fonction de restauration du code secret, lancement du programme, mise à jour des bases antivirus et lancement de l'analyse antivirus de l'appareil.

DANS CETTE SECTION

Activation du logiciel.....	27
Saisie du code secret.....	31
Activation de la fonction de restauration du code secret.....	32
Restauration du code secret.....	33
Lancement du logiciel.....	34
Mise à jour des bases du programme.....	34
Recherche de virus sur l'appareil.....	34
Informations sur le programme.....	35

ACTIVATION DU LOGICIEL

Avant de commencer le travail avec l'application Kaspersky Mobile Security 9, il faut l'activer.

Pour activer Kaspersky Mobile Security 9, l'appareil doit être connecté à Internet.

Avant d'activer l'application, assurez-vous que la date et l'heure du système sont correctes.

Vous pouvez activer l'application selon l'une des manières suivantes :

- **Activer la version d'évaluation.** Lors de l'activation de la version d'évaluation de l'application, l'utilisateur reçoit une licence d'évaluation gratuite. La durée de validité de la licence d'évaluation est affichée à l'écran après activation. A expiration de la licence d'évaluation, les possibilités de l'application sont restreintes. Seules les fonctions suivantes sont accessibles :
 - activation du logiciel ;
 - administration de la licence de l'application ;
 - aide de Kaspersky Mobile Security 9 ;
 - désactivation de Chiffrement ;
 - désactivation de Contacts personnels.

Il est impossible d'activer une deuxième fois la version d'évaluation.

- **Activer la version commerciale.** L'activation de la version commerciale s'opère à l'aide du code d'activation obtenu lors de l'achat de l'application. Dans le cadre de l'activation de la version commerciale, l'application

obtient une licence commerciale qui permet d'utiliser toutes les fonctions de l'application. La durée de validité de la licence apparaît à l'écran de l'appareil. Une fois la licence parvenue à échéance, les fonctionnalités de l'application sont restreintes et la mise à jour de l'application n'a plus lieu.

Vous pouvez obtenir le code d'activation d'une des manières suivantes :

- en ligne, en passant de l'application Kaspersky Mobile Security 9 au site Web de Kaspersky Lab dédiés aux appareils mobiles ;
- dans la boutique en ligne de Kaspersky Lab (<http://kaspersky.telechargement.fr>);
- chez un revendeur de Kaspersky Lab.
- **Activer l'abonnement.** Lors de l'activation de l'abonnement, l'application reçoit une licence commerciale avec abonnement. La durée de validité de la licence avec abonnement est limitée à 30 jours. Dans le cadre de l'abonnement, l'application renouvelle la licence tous les 30 jours. Lors du renouvellement de la licence, le montant défini lors de l'activation de l'abonnement est débité de votre compte personnel pour l'utilisation de l'application. Le paiement s'opère via l'envoi d'un SMS payant. Une fois que la somme a été débitée, l'application reçoit une nouvelle licence à abonnement du serveur d'activation. Toutes les fonctions sont à nouveau accessibles. Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9. Dans ce cas, à l'échéance de la validité de la licence, les fonctionnalités de l'application sont restreintes. Les bases antivirus de l'application ne sont pas actualisées.

DANS CETTE SECTION

Activation de la version commerciale	28
Activation de l'abonnement à Kaspersky Mobile Security 9	29
Achat du code d'activation en ligne	30
Activation de la version d'évaluation	31

ACTIVATION DE LA VERSION COMMERCIALE

➡ Pour activer la version commerciale de l'application à l'aide du code d'activation, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

L'écran **Activation** s'ouvre.

3. Choisissez l'option **Saisie du code**.

L'écran d'activation de Kaspersky Mobile Security 9 s'ouvre (cf. ill. ci-dessous).

4. Saisissez le code d'activation obtenu dans les quatre champs, puis cliquez sur **Suivant**.

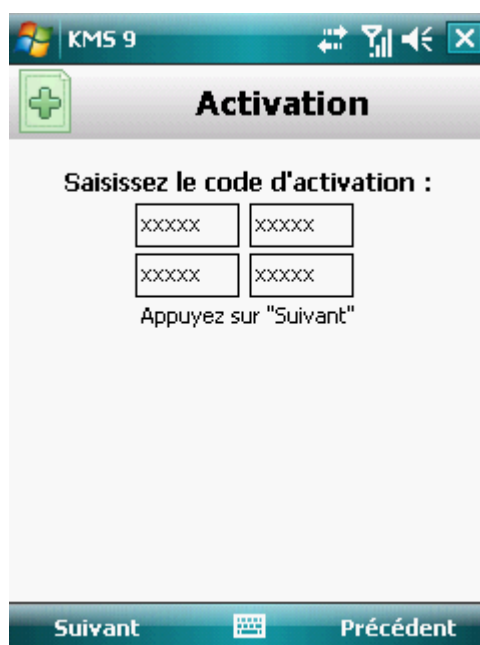


Figure 4 : activation de la version commerciale de l'application

5. Confirmez la connexion à Internet en cliquant sur **Oui**.

L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées à l'écran.

Si le code que vous avez saisi est incorrect pour une raison quelconque, un message de circonstance apparaîtra à l'écran de l'appareil mobile. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société à qui vous avez acheté le code d'activation de Kaspersky Mobile Security 9.

Si des erreurs se sont produites lors de la connexion au serveur et qu'il a été impossible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs persistent, contactez le Service d'assistance technique.

6. Passez à la saisie du code secret de l'application (cf. section "Saisie du code secret" à la page [31](#)).

ACTIVATION DE L'ABONNEMENT A KASPERSKY MOBILE SECURITY 9

L'activation de l'abonnement requiert une connexion à Internet sur l'appareil.

➡ Pour activer l'abonnement à Kaspersky Mobile Security 9, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

L'écran **Activation** s'ouvre.

3. Sélectionnez **Achat rapide**.
4. Confirmez la connexion à Internet en cliquant sur **Oui**.

L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement est disponible, alors l'écran **Activation** s'affiche et présente les conditions générales de l'abonnement.

Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran précédent où vous pourrez choisir un autre mode d'activation de l'application.

5. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9 en cliquant sur **Suivant**.

L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9 vous prévient lorsque l'abonnement est activé.

Si le solde de votre compte n'est pas suffisant pour envoyer le message SMS payant, l'activation de l'abonnement est annulée.

Si des erreurs se sont produites lors de la connexion au serveur et qu'il a été impossible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs persistent, contactez le Service d'assistance technique.

Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Annuler**. L'application annule, dans ce cas, l'activation et revient à l'écran où vous pouvez choisir le mode d'activation de l'application.

6. Passez à la saisie du code secret (cf. section "Saisie du code secret" à la page [31](#)).

ACHAT DU CODE D'ACTIVATION EN LIGNE

➡ Pour acheter le code d'activation de l'application en ligne, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.

2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

L'écran **Activation** s'ouvre.

3. Sélectionnez **Acheter en ligne**.

L'écran **Acheter en ligne** s'ouvre.

4. Cliquez sur **Ouvrir**.

Le site Web de Kaspersky Lab pour les appareils mobiles s'ouvre. Vous pourrez y commander le renouvellement de la licence.

5. Suivez les instructions.

6. Dès que vous avez terminé l'achat du code d'activation, passez à l'activation commerciale de l'application (cf. section "Activation de la version commerciale" à la page [28](#)).

ACTIVATION DE LA VERSION D'EVALUATION

➡ Pour activer la version d'évaluation de Kaspersky Mobile Security 9, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.

2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

L'écran **Activation** s'ouvre.

3. Sélectionnez **Version d'évaluation**.

4. Confirmez la connexion à Internet en cliquant sur **Oui**.

L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence.

Si des erreurs se sont produites lors de la connexion au serveur et qu'il a été impossible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs persistent, contactez le Service d'assistance technique.

5. Passez à la saisie du code secret de l'application (cf. section "Saisie du code secret" à la page [31](#)).

SAISIE DU CODE SECRET

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

Vous pourrez modifier ultérieurement le code secret de l'application définit.

Kaspersky Mobile Security 9 demande le code secret dans les cas suivants :

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

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

Si vous avez oublié le code secret, vous pouvez le restaurer (cf. section "Restauration du code secret" à la page [33](#)). Pour ce faire, il faut d'abord activer la fonction de restauration du code secret (cf. section "Activation de la fonction de restauration du code secret" à la page [32](#)).

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

1. Après l'activation de l'application dans la zone **Saisissez le code** : entrez les chiffres du code.
2. Tapez de nouveau ce code dans la zone **Confirmation du code**.

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

ACTIVATION DE LA FONCTION DE RESTAURATION DU CODE SECRET

Après la première activation, vous pouvez activer l'option de restauration du code secret de l'application. Vous pourrez alors restaurer ultérieurement le code secret oublié de l'application.

Si vous avez refusé l'activation de cette fonction après la première activation de l'application, vous pourrez l'activer après la réinstallation de Kaspersky Mobile Security 9 sur l'appareil.

Vous pouvez restaurer le code secret de l'application (cf. section "Restauration du code secret" à la page 33), uniquement si la fonction de restauration du code secret est activée. Si vous avez oublié le mot de passe et la fonction de restauration du code secret a été désactivée, il est impossible d'administrer les fonctions de Kaspersky Mobile Security 9, d'obtenir l'accès aux fichiers cryptés et de supprimer l'application.

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

1. Après la saisie du code secret de l'application, confirmez l'activation de la fonction de restauration du code secret, en cliquant sur **Oui**.
2. Saisissez l'adresse du courrier électronique dans le champ **Votre ad. courr. élec.** et cliquez sur **Suivant**.

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

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

RESTAURATION DU CODE SECRET

Vous pouvez restaurer le code secret uniquement si la fonction de restauration du code secret (cf. section "Activation de la fonction de restauration du code secret" à la page 32) avait été activée.

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

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

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

3. Cliquez sur **Annuler**.
4. Passez à la restauration du code secret, en cliquant sur **Oui**.

L'écran **Restaur. du code secret** affichera les informations suivantes :

- site Internet de Kaspersky Lab pour restaurer le code secret ;
 - code d'identification de l'appareil.
5. Allez à la page web <http://mobile.kaspersky.com/recover-code> pour restaurer le code secret.
 6. Saisissez les informations suivantes dans les champs correspondants :
 - adresse électronique que vous avez indiquée auparavant pour restaurer le code secret ;

- code d'identification de l'appareil.

Finalement, le code de restauration sera envoyé à l'adresse électronique indiquée.

7. L'écran **Restaur. du code secret** vous permet de cliquer sur **Continuer** et de saisir le code de restauration obtenu.
8. Saisissez un nouveau code secret de l'application. Pour ce faire, saisissez successivement le nouveau code secret dans les champs **Saisissez le code** et **Confirmation du code**.
9. Cliquez sur **OK**.

DEMARRAGE DU LOGICIEL

➡ *Pour lancer Kaspersky Mobile Security 9, procédez comme suit :*

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9** et lancez l'application à l'aide du stylet ou du bouton central du joystick.
3. Saisissez le code secret de l'application et cliquez sur **OK**.

La fenêtre d'état de la protection de Kaspersky Mobile Security 9 (cf. section "Fenêtre d'état de la protection" à la page [44](#)) s'ouvre. Pour passer aux fonctions de l'application, cliquez sur **Menu**.

MISE A JOUR DES BASES DU PROGRAMME

Kaspersky Mobile Security 9 recherche les menaces à l'aide des bases antivirus de l'application qui contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les moyens de les neutraliser. On y retrouve également les descriptions d'autres objets indésirables. Il se peut que les bases antivirus livrées avec Kaspersky Mobile Security 9 soient dépassées au moment de l'installation.

Il est conseillé d'actualiser les bases antivirus après installation de l'application.

Pour pouvoir actualiser les bases antivirus de l'application, l'appareil mobile doit être connecté à Internet.

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

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Mise à jour**.

L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Lanc. de la mise à jour**.

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

RECHERCHE DE VIRUS SUR L'APPAREIL

Une fois l'application installée, il est conseillé de lancer une analyse complète de l'appareil mobile à la recherche d'éventuels objets malveillants.

La première analyse s'opère selon les paramètres définis préalablement par les experts de Kaspersky Lab.

➡ *Pour lancer l'analyse complète de l'appareil, procédez comme suit :*

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Choisissez l'option **Analyser**.

L'écran **Analyser** s'ouvre.

3. Sélectionnez **Analyse complète**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez consulter les informations générales sur l'application Kaspersky Mobile Security 9 et sur ses versions.

➡ *Pour consulter les informations sur l'application, procédez comme suit :*

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez **Infos logiciel**.

GESTION DE LA LICENCE

Dans le cadre de l'octroi de licences pour l'utilisation des applications de Kaspersky Lab, il est important de comprendre les notions suivantes :

- Le contrat de licence ;
- La licence.

Ces notions sont liées les unes aux autres et forment un seul ensemble. Examinons chacune d'entre elles en détail.

La section présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Mobile Security 9 et son renouvellement.

DANS CETTE SECTION

Présentation du contrat de licence	36
A propos des licences de Kaspersky Mobile Security 9	36
Affichage des informations de licence	38
Renouvellement de la licence	38

PRESENTATION DU CONTRAT DE LICENCE

Le *contrat de licence* est un contrat conclut entre une personne physique ou morale détenant une copie légale de Kaspersky Mobile Security 9 d'une part et Kaspersky Lab d'autre part. Ce contrat est proposé avec chaque application de Kaspersky Lab. Il présente en détail les droits et les restrictions d'utilisation de Kaspersky Mobile Security.

Conformément aux termes du contrat de licence, vous avez le droit de détenir une copie de l'application après avoir acheté et installé celle-ci.

Kaspersky Lab vous propose également les services complémentaires suivants :

- Assistance technique ;
- Mise à jour des bases antivirus de Kaspersky Mobile Security 9 ;
- Mise à jour des modules logiciels de Kaspersky Mobile Security 9.

Pour pouvoir l'obtenir, vous devez acheter et activer une licence (cf. section Présentation des licences de Kaspersky Mobile Security 9 à la page [36](#)).

A PROPOS DES LICENCES DE KASPERSKY MOBILE SECURITY 9

La *licence* est un droit octroyé pour l'utilisation de Kaspersky Mobile Security 9 et des services complémentaires (cf. section Présentation du contrat de licence à la page [36](#)) offerts par Kaspersky Lab ou ses partenaires.

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

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

- Assistance technique ;
- Mise à jour des bases antivirus de Kaspersky Mobile Security 9 ;
- Mise à jour des modules logiciels de Kaspersky Mobile Security 9.

Le volume des services proposés dépend du type de licence.

Les types de licence sont les suivants :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Mobile Security 9.

La licence d'évaluation peut être utilisée une seule fois.

La licence d'évaluation vous permet de contacter le Service d'assistance technique uniquement pour des questions relatives à l'activation de l'application ou à l'achat de la licence commerciale. Dès la licence d'évaluation expirée, Kaspersky Mobile Security 9 arrête de fonctionner. Pour pouvoir continuer à utiliser l'application, il faut l'activer (cf. section "Activation de la version commerciale" à la page [28](#)).

- *Commerciale* : licence payante dont la durée de validité est définie (par exemple, un an) et octroyée lors de l'achat de Kaspersky Mobile Security 9.

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

Dès que la licence commerciale a expiré, certaines fonctionnalités de Kaspersky Mobile Security 9 deviennent inaccessibles et les bases antivirus de l'application ne seront plus actualisées. Sept jours avant expiration de la licence, l'application affichera une notification. Vous aurez ainsi le temps de renouveler la licence.

- *Commerciale avec abonnement* : licence payante offrant une possibilité de renouvellement automatique ou manuel. La licence avec abonnement est proposée aux prestataires de services.

L'abonnement a une validité limitée (30 jours). Une fois que l'abonnement expire, il peut être renouvelé manuellement ou automatiquement. Le mode de renouvellement de l'abonnement dépend de la législation en vigueur et de l'opérateur de téléphonie mobile. L'abonnement est renouvelé automatiquement si le prépaiement du prestataire de service a été effectué.

Lors du renouvellement de l'abonnement, le montant défini par les conditions générales de l'abonnement est débité de votre compte personnel. La somme est débitée de votre compte personnel via un SMS payant envoyé au numéro du prestataire de service.

Si l'abonnement n'est pas renouvelé, Kaspersky Mobile Security 9 n'effectue plus de mise à jour des bases antivirus de l'application et les fonctionnalités de l'application seront limitées.

Si vous choisissez l'abonnement, vous pouvez activer la licence commerciale via le code d'activation. Dans ce cas, l'abonnement sera automatiquement annulé.

Vous pouvez activer un abonnement si vous utilisez une licence commerciale. Si, au moment d'activer l'abonnement, vous aviez déjà activé la licence à durée déterminée, cette licence sera remplacée par une licence avec abonnement.

AFFICHAGE DES INFORMATIONS DE LICENCE

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

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

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Sélectionnez **Infos licence**.

RENOUVELLEMENT DE LA LICENCE

Kaspersky Mobile Security 9 permet de renouveler la durée de validité de la licence de l'application.

Vous pouvez renouveler la licence d'une des méthodes suivantes :

- saisir le code d'activation : activation de la licence à l'aide d'un code d'activation. Le code d'activation est disponible lors de l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html ou chez les distributeurs de Kaspersky Lab.
- Acheter le code d'activation en ligne : accédez au site Web ouvert sur votre appareil mobile et achetez le code d'activation en ligne.
- S'abonner à Kaspersky Mobile Security 9 : activez l'abonnement afin de renouveler la durée de validité de la licence tous les 30 jours.

Pour activer le logiciel sur l'appareil mobile, celui doit avoir la connexion à Internet.

DANS CETTE SECTION

Renouvellement de la licence à l'aide du code d'activation.....	39
Renouvellement de la licence en ligne.....	40
Renouvellement de la licence à l'aide de l'activation de l'abonnement	40
Refus de l'abonnement	42
Renouvellement de l'abonnement.....	43

RENOUVELLEMENT DE LA LICENCE A L'AIDE DU CODE D'ACTIVATION

➡ Pour renouveler la licence à l'aide du code d'activation, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Choisissez l'option **Renouveler**.

L'écran **Renouveler** s'ouvre.

4. Saisissez le code d'activation obtenu dans les quatre champs, puis cliquez sur **Suivant** (cf. ill. ci-après).

Figure 5 : renouvellement de la licence à l'aide d'un code d'activation

5. Confirmez la connexion à Internet en cliquant sur **Oui**.

L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées à l'écran.

Si le code que vous avez saisi est incorrect pour une raison quelconque, un message de circonstance apparaîtra à l'écran de l'appareil mobile. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société à qui vous avez acheté le code d'activation de Kaspersky Mobile Security 9.

Si des erreurs se sont produites lors de la connexion au serveur et qu'il a été impossible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs persistent, contactez le Service d'assistance technique.

6. Enfin, cliquez sur **OK**.

RENOUVELLEMENT DE LA LICENCE EN LIGNE

► Pour renouveler l'application en ligne, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Sélectionnez l'option **Acheter en ligne**.

L'écran **Acheter en ligne** s'ouvre.

4. Cliquez sur **Ouvrir** (cf. ill. ci-dessous).

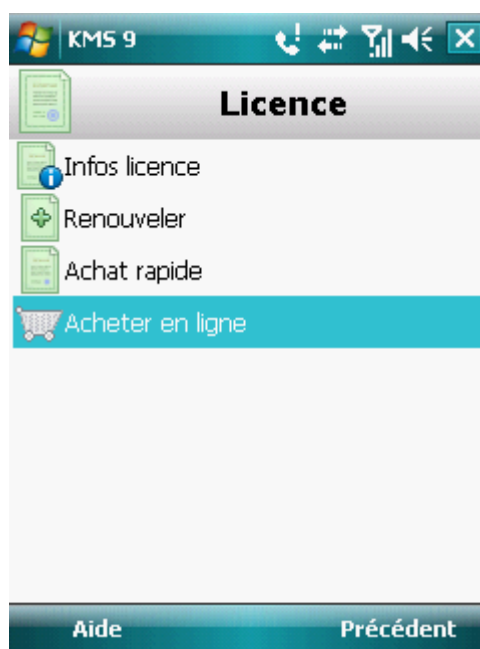


Figure 6 : renouvellement de la licence en ligne

Cette action entraîne l'ouverture d'une page Web sur laquelle vous serez invité à commander le renouvellement de la licence.

Si la durée de validité de la licence a expiré, alors la page Web de Kaspersky Lab pour appareils mobiles s'ouvrira. Vous pourrez y acheter le code d'activation en ligne.

5. Suivez les instructions.
6. Dès que la commande de renouvellement de la licence a été effectuée, saisissez le code d'activation reçu (cf. section "Renouvellement de la licence à l'aide d'un code d'activation" à la page [39](#)).

RENOUVELLEMENT DE LA LICENCE A L'AIDE DE L'ACTIVATION DE L'ABONNEMENT

Vous pouvez prolonger la période de validité de la licence, en activant l'abonnement (cf. section "A propos des licences de Kaspersky Mobile Security 9" à la page [36](#)) de Kaspersky Mobile Security 9. Dans le cadre de l'abonnement, Kaspersky Mobile Security 9 renouvelle la validité de la licence tous les 30 jours. Lors de chaque renouvellement de licence, le montant défini par les conditions générales de l'abonnement est débité de votre compte personnel.

L'activation de l'abonnement à Kaspersky Mobile Security 9 requiert une connexion à Internet.

► Pour activer l'abonnement à Kaspersky Mobile Security 9, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

Choisissez l'option **Achat rapide** (cf. ill. ci-après).

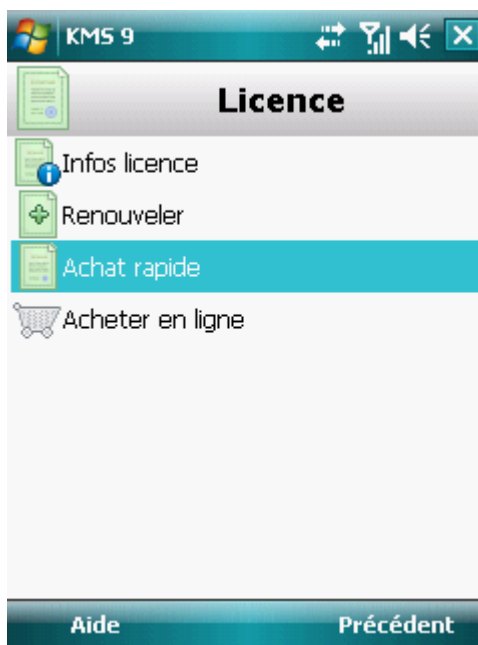


Figure 7 : activation de l'abonnement

3. Confirmez la connexion à Internet en cliquant sur **Oui**.

L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement.

Si le service d'abonnement est disponible, alors l'écran **Activation** s'affiche et présente les conditions générales de l'abonnement.

Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode de renouvellement de la licence. L'activation de l'abonnement sera annulée.

4. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9 en cliquant sur **Suivant**.

L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9 vous prévient lorsque l'abonnement est activé.

Si le solde de votre compte n'est pas suffisant pour envoyer le message SMS payant, l'activation de l'abonnement est annulée.

Si des erreurs se sont produites lors de la connexion au serveur et qu'il a été impossible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs persistent, contactez le Service d'assistance technique.

Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Annuler**. L'application annule, dans ce cas, l'activation et revient à l'écran précédent où vous pouvez choisir un autre mode de renouvellement de la licence.

5. Enfin, cliquez sur **OK**.

REFUS DE L'ABONNEMENT

Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9. Dans ce cas, Kaspersky Mobile Security 9 ne renouvelle pas la validité de la licence tous les 30 jours. À expiration de la licence en cours de validité, les fonctionnalités de l'application seront réduites et les bases antivirus de l'application ne seront pas mises à jour.

Si vous avez refusé l'abonnement, sachez que vous pourrez le reprendre (cf. section "Renouvellement de l'abonnement" à la page [43](#)).

➡ Pour refuser l'abonnement à Kaspersky Mobile Security 9, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Choisissez l'option **Annulation de l'abonnement** (cf. ill. ci-après).

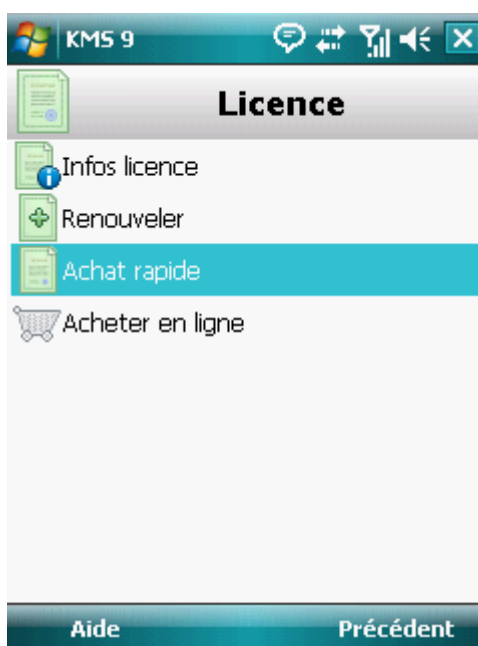


Figure 8 : refus de l'abonnement

4. Confirmez le refus de l'abonnement en cliquant sur **Oui**.

Kaspersky Mobile Security 9 vous signale que l'abonnement a été annulé.

RENOUVELLEMENT DE L'ABONNEMENT

Si vous aviez refusé l'abonnement (cf. section Refus de l'abonnement à la page [42](#)), vous pourrez le renouveler. Dans ce cas, Kaspersky Mobile Security 9 renouvellera la durée de validité de la licence tous les 30 jours.

En cas de renouvellement de l'abonnement, le montant requis sera débité de votre compte personnel uniquement si la licence actuelle expire dans moins de trois jours.

➡ Pour renouveler l'abonnement, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Choisissez l'option **Achat rapide**.

Si la licence actuelle arrive à échéance, alors, Kaspersky Mobile Security 9 propose d'activer à nouveau l'abonnement (cf. section "Renouvellement de la licence" à la page [38](#)).

Si la licence actuelle est toujours valide, alors Kaspersky Mobile Security 9 prolonge l'abonnement et à échéance, il la renouvellera tous les 30 jours.

INTERFACE DE L'APPLICATION

Cette section présente les informations sur les principaux composants de l'interface de Kaspersky Mobile Security 9.

DANS CETTE SECTION

Fenêtre d'état de la protection.....	44
Menu de l'application.....	46

FENETRE D'ETAT DE LA PROTECTION

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

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

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

- **Protection** : état de la protection en temps réel (cf. section "Protection en temps réel" à la page [48](#)).

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

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

L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil. Par exemple, la protection est désactivée. Il est possible que les bases antivirus n'aient pas été actualisées depuis plus de 15 jours.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. section "Filtrage de l'activité de réseau. Pare-feu" à la page [106](#)).

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

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

- **Antivol** : état de la protection des données en cas de vol ou de perte de l'appareil (cf. section "Protection des données en cas de perte ou de vol de l'appareil" à la page [83](#)).

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

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

- **Contacts personnels** : état de la protection des données confidentielles (cf. section "Dissimulation des données personnelles" à la page [96](#)).

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

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

- **Licence** : durée de validité de la licence (cf. la section "Administration des licences" à la page [36](#)).

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

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

L'icône rouge indique que la validité de la licence a expiré.



Figure 9 : la fenêtre d'état des composants du programme

Vous pouvez aussi passer à la fenêtre de l'état de la protection en choisissant l'option **Menu** → **Etat de protection**.

MENU DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et sont accessibles dans le menu de l'application. Chaque option du menu permet d'accéder aux paramètres du composant sélectionné ainsi qu'aux tâches de la protection (cf. ill. ci-après).



Figure 10 : menu de l'application

Le menu de Kaspersky Mobile Security 9 propose les options suivantes :

- **Anti-Virus** : protection du système de fichiers contre les virus, analyse à la demande et actualisation des bases antivirus de l'application.
- **Antivol** : blocage de l'appareil et suppression des informations en cas de vol ou de perte.
- **Contacts personnels** : dissimulation des données confidentielles sur l'appareil.
- **Chiffrement** : protection des données sur l'appareil grâce au chiffrement.
- **Filtre des appels et SMS** : filtrage des SMS et des appels entrants non sollicités.
- **Contrôle parental** : contrôle des SMS et des messages sortants.
- **Pare-feu** : protection de réseau de l'application.
- **Avancé** : paramètres généraux de l'application, informations sur l'application, sur les bases antivirus utilisées et sur la licence.
- **Etat de protection** : informations sur l'état de la protection de l'appareil.
- **Quitter** : fin de l'utilisation de l'application.

- *Pour ouvrir le menu de l'application,*
sélectionnez **Menu**.

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

- *Pour revenir à la fenêtre d'état des composants logiciels,*
sélectionnez **Menu → Etat de protection**.

- *Pour quitter l'application,*
sélectionnez **Menu → Quitter**.

PROTECTION DU SYSTEME DE FICHIERS

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

DANS CETTE SECTION

Présentation de la protection.....	48
Activation et désactivation de la protection	48
Sélection des actions à appliquer sur les objets identifiés.....	50

PRESENTATION DE LA PROTECTION

La protection est lancée en même temps que le système d'exploitation et se trouve en permanence dans la mémoire vive de l'appareil. La protection analyse tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. La protection analyse chaque fichier au moment où vous essayez d'y accéder.
2. La protection analyse le fichier pour détecter des objets malveillants éventuels. Les objets malveillants sont détectés en les comparant aux bases antivirus utilisées par le logiciel. Les bases antivirus de l'application contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.
3. Après l'analyse, la Protection agit en fonction de ses résultats :
 - lorsqu'un code malveillant est découvert dans le fichier, la protection le bloque et agit conformément aux paramètres définis ;

Si aucun code malveillant n'est découvert dans le fichier, ce dernier sera accessible pour travailler aussitôt. Les informations concernant les résultats de l'analyse sont enregistrés dans le Journal du logiciel (cf. section "Journaux du logiciel" à la page [120](#)).

ACTIVATION ET DESACTIVATION DE LA PROTECTION

Lorsque la Protection est activée, toutes les actions exécutées dans le système sont contrôlées de manière permanente.

La protection contre les virus et les autres menaces est effectuée en utilisant les ressources de l'appareil. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

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

La désactivation de la protection n'affecte pas les tâches d'analyse antivirus et de mise à jour des bases antivirus de l'application.

L'état actuel de la protection est repris sur l'écran **Antivirus** à côté de l'option de menu **Protection**.

Vous pouvez activer/désactiver la protection selon l'une des méthodes suivantes :

- depuis le menu de configuration du composant ;
- depuis le menu **Antivirus**.

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

➡ *Pour désactiver la Protection, procédez comme suit :*

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Protection**.

L'écran **Protection** s'ouvre.

3. Cochez la case **Activer la Protection** (cf. ill. ci-après).

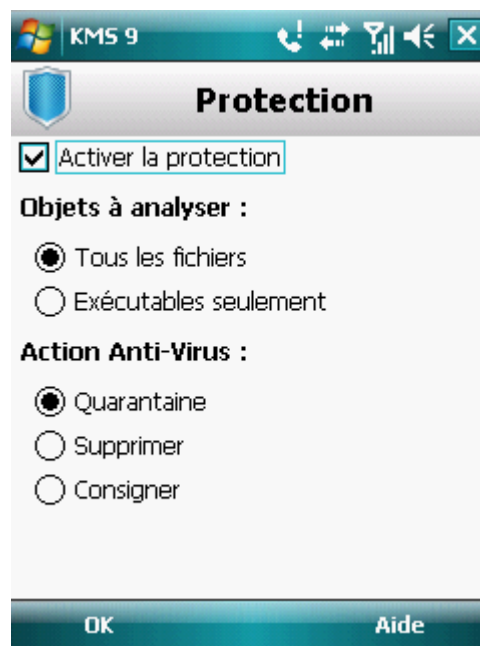


Figure 11 : activation de la protection

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

➡ *Pour désactiver la protection, procédez comme suit :*

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Protection**.

L'écran **Protection** s'ouvre.

3. Décochez la case **Activer la Protection**.

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

➡ Pour activer/désactiver la Protection, procédez comme suit :

1. Sélectionnez **Menu** → Anti-Virus.
2. L'écran **Anti-Virus** s'ouvre.
3. Appuyez sur **Activer** / **Désactiver**. Le texte du bouton prendra la valeur opposée en fonction de l'état actuel de la protection.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9 met les objets malveillants découverts en quarantaine. Vous pouvez sélectionner l'action que Kaspersky Mobile Security 9 exécutera sur l'objet malveillant découvert.

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

Pour modifier la valeur des paramètres de la protection, assurez-vous qu'elle est activée.

➡ Pour configurer la réponse du programme en présence d'un objet malveillant, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.
L'écran **Anti-Virus** s'ouvre.
2. Sélectionnez l'option **Protection**.
L'écran **Protection** s'ouvre.
3. Définissez l'action que l'application exécutera en cas de découverte d'un objet malveillant. Pour ce faire, attribuez une valeur au paramètre **Action Anti-Virus** (cf. ill. ci-après) :
 - **Quarantaine** : place en quarantaine les objets malveillants.
 - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

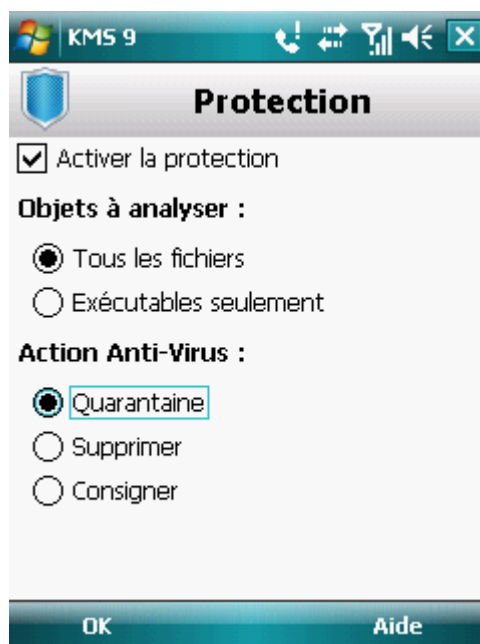


Figure 12 : sélection de l'action appliquée à un objet

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

ANALYSE DE L'APPAREIL

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

DANS CETTE SECTION

À propos de l'analyse à la demande	52
Exécution manuelle d'une analyse	52
Exécution programmée de l'analyse	54
Sélection du type d'objet à analyser	55
Configuration de l'analyse des archives	56
Sélection des actions à appliquer sur les objets identifiés.....	57

À PROPOS DE L'ANALYSE A LA DEMANDE

L'analyse de l'appareil permet d'identifier et de neutraliser les objets malveillants. Kaspersky Mobile Security 9 peut effectuer une analyse complète ou partielle de l'appareil. Autrement dit, il peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier en particulier (y compris les dossiers sur les cartes mémoire).

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

1. Kaspersky Mobile Security 9 analyse les fichiers d'un type défini (cf. section "Sélection des types de fichiers à analyser" à la page [55](#)).
2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés en les comparant aux bases antivirus utilisées par le logiciel. Les bases antivirus contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

Selon les résultats de l'analyse, Kaspersky Mobile Security 9 peut adopter les comportements suivants :

- Lorsqu'un code malveillant est découvert dans un fichier, Kaspersky Mobile Security 9 bloque le fichier et exécute l'action sélectionnée conformément aux (cf. la section "Sélection des actions à appliquer sur des objets" à la page [57](#)) ;
- Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

La tâche d'analyse est lancée manuellement ou automatiquement selon un horaire défini (cf. section "Exécution de l'analyse à la demande" à la page [54](#)).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. section Journaux de l'application à la page [120](#)).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer une analyse manuellement, par exemple lorsque le processeur de l'application n'est pas occupé par l'exécution d'autres tâches.

➡ Pour lancer une analyse antivirus, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Choisissez l'option **Analyser**.

L'écran **Analyser** s'ouvre.

3. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

- **Analyse complète** : analyse tout le système de fichiers de l'application. Les objets suivants sont analysés par défaut : mémoire de l'appareil et carte d'extension de mémoire.
- **Analyse de la mémoire** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.
- **Analyser dossier** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte d'extension de mémoire. La sélection de l'option **Analyser dossier** ouvre un écran qui présente le système de fichier de l'appareil. Utilisez le stylet ou le joystick pour naviguer dans le système de fichiers. Pour lancer l'analyse du dossier, sélectionnez le dossier requis, puis appuyez sur **Analyser**.

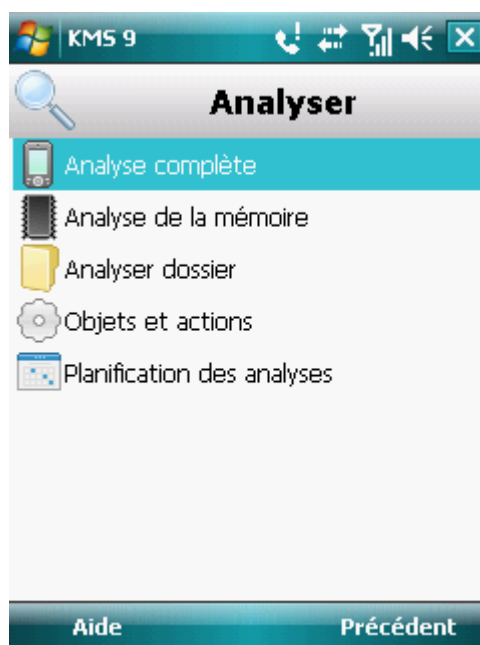


Figure 13 : sélection de la zone d'analyse

Après le démarrage de l'analyse, une fenêtre affiche l'état actuel de la tâche : nombre d'objets analysés, chemin d'accès de l'objet en cours d'analyse.

Si Kaspersky Mobile Security 9 découvre un objet infecté, il exécute l'action conformément aux paramètres d'analyse définis (cf. section "Sélection des actions à appliquer sur les objets identifiés" à la page [57](#)).

Par défaut, Kaspersky Mobile Security 9 place en quarantaine toutes les menaces identifiées.

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

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

4. Enfin, cliquez sur **OK**.

EXECUTION DE L'ANALYSE PROGRAMMEE

Kaspersky Mobile Security 9 permet de planifier des analyses de l'appareil qui s'exécuteront automatiquement à des heures programmées à l'avance. L'analyse est exécutée en arrière plan. Lorsqu'un objet infecté est détecté, l'application exécute l'action sélectionnée dans la configuration de l'analyse (cf. section "Sélection des actions à appliquer sur les objets identifiés" à la page [57](#)).

Par défaut, la planification est désactivée.

➡ *Pour configurer l'analyse programmée, procédez comme suit :*

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Choisissez l'option **Analyser**.

L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Planification des analyses**.

L'écran **Planification** s'ouvre.

4. Cochez la case **Analyse programmée** (cf. ill. ci-après).

5. Sélectionnez l'une des valeurs proposées pour le paramètre **Fréquence** :

- **Chaque jour** : l'analyse s'exécutera tous les jours. Spécifiez l'**Heure** dans le champ de saisie.
- **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Définissez les paramètres **Heure** et **Jour de la semaine**.

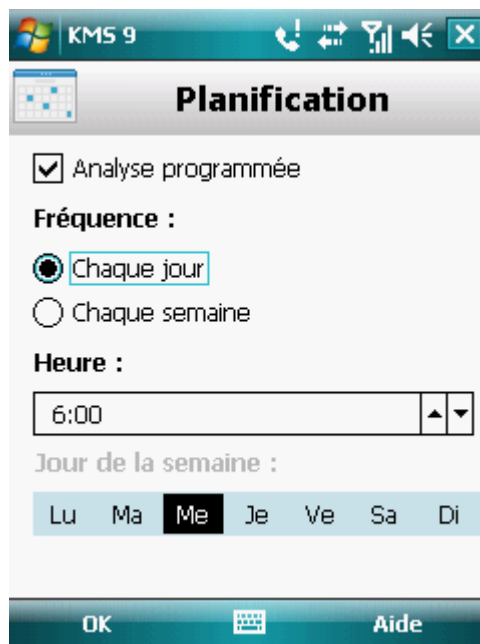


Figure 14 : planification des analyses automatiques

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

SELECTION DU TYPE D'OBJET A ANALYSER

Vous pouvez sélectionner les types d'objet qui seront soumis à la recherche de code malveillant.

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

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Choisissez l'option **Analyser**.

L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

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

4. Sélectionnez les objets à analyser dans le groupe **Objets à analyser** (cf. ill. ci-après) :

- **Tous les fichiers** : analyse les fichiers de tout type.
- **Exécutables seulement** : analyse uniquement les fichiers exécutables des applications au format EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

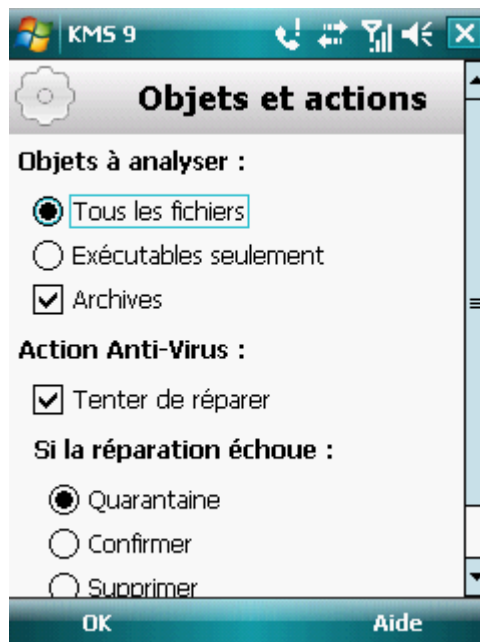


Figure 15 : sélection des objets à analyser

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

CONFIGURATION DE L'ANALYSE DES ARCHIVES

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

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

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

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

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Choisissez l'option **Analyser**.

L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

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

4. Dans le groupe **Objets à analyser**, cochez la case **Archives**.
5. Cliquez sur **OK** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9 met les objets infectés découverts en quarantaine. Vous pouvez modifier l'action de l'application en cas de découverte d'un objet malveillant.

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

➡ Pour configurer la réponse du programme en présence d'un objet malveillant, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.
L'écran **Anti-Virus** s'ouvre.
2. Choisissez l'option **Analyser**.
L'écran **Analyser** s'ouvre.
3. Sélectionnez l'option **Objets et actions**.
L'écran **Objets et actions** s'ouvre.
4. Pour que le programme tente de réparer les objets infectés, cochez la case **Tenter de réparer** pour le paramètre **Action Anti-Virus** (cf. ill. ci-après).
5. Définissez l'action à exécuter sur les objets malveillants découverts. Pour ce faire, attribuez une valeur au paramètre **Exécuter l'action** :

Si la case **Tenter de réparer** a été cochée, le paramètre s'appelle **Si la réparation échoue**. Ce paramètre détermine l'action de l'application en cas d'échec de la réparation.

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

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application et bloque les tentatives d'accès à l'objet (par exemple, copie ou ouverture).

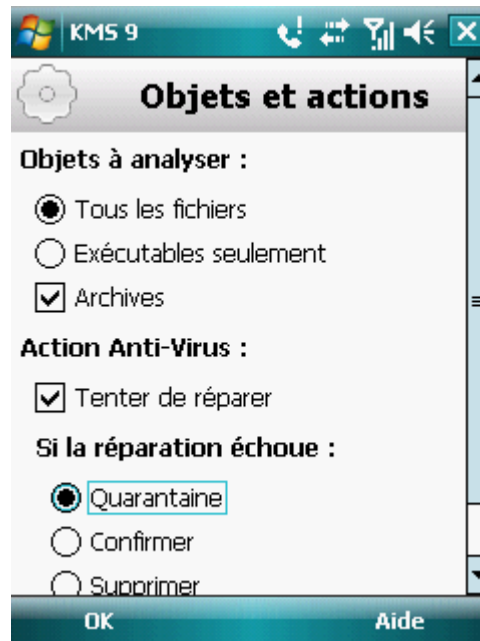


Figure 16 : sélection de l'action appliquée à un objet malveillant

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

QUARANTAINE DES OBJETS MALVEILLANTS

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

DANS CETTE SECTION

À propos de la quarantaine	59
Affichage des objets en quarantaine	59
Restauration d'objets de la quarantaine	60
Suppression d'objets de la quarantaine	61

À PROPOS DE LA QUARANTAINE

L'application place les objets malveillants détectés en *quarantaine* dans un dossier spécifique isolé pendant l'analyse de l'appareil ou pendant le fonctionnement de la protection. Les objets malveillants placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil.

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

AFFICHAGE DES OBJETS EN QUARANTAINE

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

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

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Quarantaine**.

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



Figure 17 : liste des objets placés en quarantaine

- Pour consulter les informations relatives à l'objet infecté,

cliquez sur **Détails**.

L'écran **Détails** s'ouvre.

L'écran **Détails** présente les informations suivantes sur l'objet : chemin d'accès au fichier sur l'appareil avant sa détection et nom du virus.

RESTAURATION D'OBJETS DE LA QUARANTAINE

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

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Quarantaine**.

L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à restaurer, puis choisissez l'option **Menu** → **Restaurer**.

L'objet sélectionné dans la quarantaine est restauré dans son dossier d'origine.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

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

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Quarantaine**.

L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à supprimer, puis choisissez l'option **Menu** → **Supprimer**.

L'objet sélectionné est supprimé de la quarantaine.

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Quarantaine**.

L'écran **Quarantaine** s'ouvre.

3. Cliquez sur **Menu** → **Supprimer tout**.

Tous les objets en quarantaine seront supprimés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

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

DANS CETTE SECTION

A propos du Filtre des appels et SMS	62
A propos des Modes du Filtre des appels et SMS	63
Modification du mode Filtre des appels et SMS	63
Composition de la liste noire	64
Composition de la liste blanche.....	67
Réaction aux SMS et appels de contacts ne figurant pas dans le répertoire téléphonique	71
Réaction aux SMS en provenance de numéros sans chiffres	72
Sélection de l'action à appliquer sur les SMS entrants.....	73
Sélection de l'action à appliquer sur des appels entrants.....	73

A PROPOS DU FILTRE DES APPELS ET SMS

Le Filtre des appels et SMS empêche la réception d'appels et de SMS non sollicités sur la base des Listes noire et blanche que vous avez créées.

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

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

Filtre des appels et SMS filtre les appels et les SMS entrants selon le mode sélectionné (cf. section A propos des Modes du Filtre des appels et SMS à la page [63](#)). Filtre des appels et SMS analyse, sur la base du régime, chaque SMS ou appel entrant et détermine si ce SMS ou cet appel est sollicité ou non (spam). L'analyse se termine dès que Filtre des appels et SMS a attribué l'état, sollicité ou non, au SMS ou à l'appel.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. section Journaux du logiciel à la page [120](#)).

A PROPOS DES MODES DU FILTRE DES APPELS ET SMS

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

Les modes de fonctionnement Filtre des appels et SMS disponibles :

- **Désactivé** : accepte tous les appels et les SMS entrants.
- **Autoriser "Liste blanche"** : accepte uniquement les appels et les SMS en provenance des numéros de la liste blanche.
- **Bloquer "Liste noire"** : accepte tous les appels et les SMS, sauf ceux qui proviennent des numéros de la liste noire.
- **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 d'un numéro qui ne figure sur aucune des listes, Filtre des appels et SMS vous invitera à ajouter ce numéro sur l'une des listes.

Vous pouvez modifier le mode Filtre des appels et SMS (cf. section Modification du mode Filtre des appels et SMS à la page [63](#)). Le mode actuel du Filtre des appels et SMS s'affiche sur l'écran **Filtre app./SMS** à côté du point du menu **Mode**.

MODIFICATION DU MODE FILTRE DES APPELS ET SMS

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app. /SMS** s'ouvre.

2. Sélectionnez l'option **Mode**.

L'écran **Filtre app. /SMS** s'ouvre.

3. Sélectionnez une valeur pour le paramètre **Mode Filtre app./SMS** (cf. ill. ci-après).

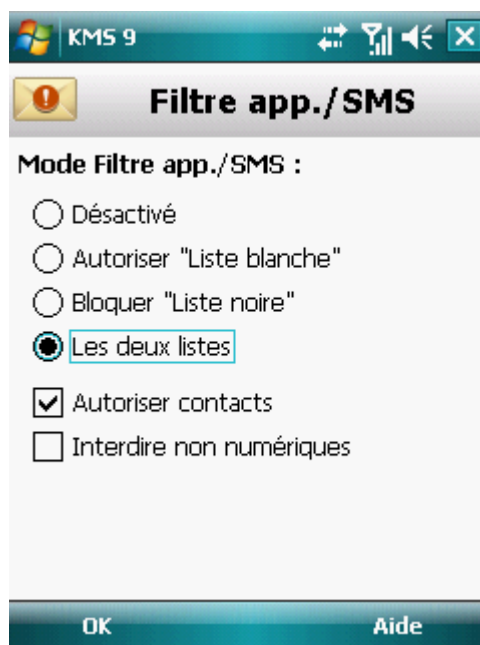


Figure 18 : modification du mode Filtre des appels et SMS

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

COMPOSITION DE LA LISTE NOIRE

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

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

Filtre des appels et SMS bloque uniquement les appels et les SMS qui répondent à tous les critères d'une entrée de la liste noire. Filtre des appels et SMS accepte les appels et les SMS qui ne répondent pas à un ou plusieurs critères de l'entrée 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. section "Journaux du logiciel" à la page [120](#)).

DANS CETTE SECTION

Ajout d'une entrée à la liste noire	65
Modification d'une entrée de la liste noire	66
Suppression d'une entrée de la liste noire	67

AJOUT D'UNE ENTREE A LA LISTE NOIRE

N'oubliez pas qu'un même numéro ayant des critères de filtrage identiques ne peut se trouver en même temps dans la liste noire et dans la liste blanche des numéros du Filtre des appels et SMS. Lorsqu'un numéro ayant ces critères de filtrage est déjà enregistré dans l'une des deux listes, Kaspersky Mobile Security 9 vous prévient : un message de circonstance s'affiche.

► Pour ajouter une entrée à la liste noire Filtre des appels et SMS, procédez comme suit :

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app./SMS** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

3. Sélectionnez **Menu** → **Ajouter**.

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

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

- **Bloquer tout** : type d'événements en provenance d'un numéro de téléphone que Filtre des appels et SMS refusera pour les numéros de la liste noire :
 - **Appels et SMS** : bloque les appels et les SMS entrants.
 - **Appels seuls** : bloque uniquement les appels entrants.
 - **SMS seuls** : bloque uniquement les SMS entrants.
- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par Filtre des appels et SMS. Le numéro peut commencer par un chiffre, 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). Par exemple, le numéro *1234 ? de la liste noire. Filtre des appels et SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
- **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Filtre des appels et SMS refuse uniquement les SMS contenant 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 cette entrée, vide.

Figure 19 : paramètres de l'enregistrement

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

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

➡ Pour modifier une entrée de la liste noire du **Filtre des appels et SMS**, procédez comme suit :

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app. /SMS** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

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

L'écran **Modifier** s'ouvre.

4. Modifiez les paramètres requis :

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

- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont refusées par Filtre des appels et SMS. Le numéro peut commencer par un chiffre, 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). Par exemple, le numéro *1234 ? de la liste noire. Filtre des appels et SMS refusera tout appel ou SMS en provenance du numéro qui contient les chiffres 1234, suivis de tout autre caractère.
- **Contenant le texte** : expression clé qui indique que le SMS reçu est non sollicité (spam). Filtre des appels et SMS refuse uniquement les SMS contenant l'expression clé et accepte tous les autres SMS.

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

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

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

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

➡ Pour supprimer une entrée de la liste noire du Filtre des appels et SMS, procédez comme suit :

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.
L'écran **Filtre app. /SMS** s'ouvre.
2. Sélectionnez l'option **Liste noire**.
L'écran **Liste noire** s'ouvre.
3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
4. Confirmez la suppression de l'entrée. Pour ce faire, cliquez sur **Oui**.

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.
L'écran **Filtre app. /SMS** s'ouvre.
2. Sélectionnez l'option **Liste noire**.
L'écran **Liste noire** s'ouvre.
3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

La liste blanche contient les entrées des numéros de téléphone autorisés dont les appels et les SMS sont acceptés par Filtre des appels et SMS. Chacune de ces entrées contient les informations suivantes :

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

Filtre des appels et SMS accepte uniquement les appels et les SMS qui répondent à tous les critères d'une entrée de la liste blanche. Filtre des appels et SMS refuse les appels et les SMS qui ne répondent pas à un ou plusieurs critères de l'entrée de la liste blanche.

DANS CETTE SECTION

Ajout d'une entrée à la liste blanche.....	68
Modification d'une entrée de la liste blanche.....	69
Suppression d'une entrée de la liste blanche.....	70

AJOUT D'UNE ENTREE A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro ayant des critères de filtrage identiques ne peut se trouver en même temps dans la liste noire et dans la liste blanche des numéros du Filtre des appels et SMS. Lorsqu'un numéro ayant ces critères de filtrage est déjà enregistré dans l'une des deux listes, Kaspersky Mobile Security 9 vous prévient : un message de circonstance s'affiche.

► Pour ajouter une entrée dans la liste blanche Filtre des appels et SMS, procédez comme suit :

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app. /SMS** s'ouvre.

2. Choisissez l'option **Liste blanche**.

L'écran **Liste blanche** s'ouvre.

3. Sélectionnez **Menu** → **Ajouter**.

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

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

- **Autoriser tout** : type d'événements en provenance d'un numéro de téléphone que Filtre des appels et SMS autorisera pour les numéros de la liste blanche :
 - **Appels et SMS** : autorise les appels et les SMS entrants.
 - **Appels seuls** : autorise uniquement les appels entrants.

- **SMS seuls** : autorise les messages SMS entrants uniquement.
- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont acceptées par Filtre des appels et SMS. Le numéro peut commencer par un chiffre, 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). Par exemple, le numéro *1234 ? de la liste blanche. Filtre des appels et SMS acceptera 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. Pour les numéros de la liste blanche, Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

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

Figure 20 : paramètres de l'enregistrement

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

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

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.
L'écran **Filtre app. /SMS** s'ouvre.
2. Choisissez l'option **Liste blanche**.
L'écran **Liste blanche** s'ouvre.
3. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez **Menu** → **Modifier**.
L'écran **Modifier** s'ouvre.

4. Modifiez les paramètres requis :

- **Autoriser tout** : type d'événements en provenance d'un numéro de téléphone que Filtre des appels et SMS autorisera pour les numéros de la liste blanche :
 - **Appels et SMS** : autorise les appels et les SMS entrants.
 - **Appels seuls** : autorise uniquement les appels entrants.
 - **SMS seuls** : autorise les messages SMS entrants uniquement.
- **Numéro de téléphone** : numéro de téléphone dont les informations entrantes sont acceptées par Filtre des appels et SMS. Le numéro peut commencer par un chiffre, 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). Par exemple, le numéro *1234 ? de la liste blanche. Filtre des appels et SMS acceptera 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. Pour les numéros de la liste blanche, Filtre des appels et SMS accepte uniquement les SMS avec l'expression clé et refuse tous les autres SMS en provenance de ce numéro.

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

5. Cliquez sur **OK** 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 une entrée de la liste blanche du Filtre des appels et SMS, procédez comme suit :*

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.
L'écran **Filtre app. /SMS** s'ouvre.
2. Choisissez l'option **Liste blanche**.
L'écran **Liste blanche** s'ouvre.
3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
4. Confirmez la suppression de l'entrée. Pour ce faire, cliquez sur **Oui**.

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.
L'écran **Filtre app. /SMS** s'ouvre.
2. Choisissez l'option **Liste blanche**.
L'écran **Liste blanche** s'ouvre.
3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

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

Si le mode **Les deux listes** ou **Liste blanche** (cf. section "A propos des Modes du Filtre des appels et SMS" à la page 63) du Filtre des appels et SMS a été sélectionné, vous pouvez définir la réaction du Filtre des appels et SMS face aux SMS ou aux appels de personnes dont le numéro ne figure pas dans le répertoire téléphonique. Filtre des appels et SMS permet d'élargir la liste blanche en y introduisant les numéros des contacts.

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

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app. /SMS** s'ouvre.

2. Sélectionnez l'option **Mode**.

L'écran **Filtre app. /SMS** s'ouvre.

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

- Pour que Filtre des appels et SMS considère un numéro du répertoire téléphonique 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 le répertoire, cochez la case **Autoriser contacts** ;
- Pour que Filtre des appels et SMS filtre les SMS et les appels uniquement sur la base du régime défini de Filtre des appels et SMS, décochez la case **Autoriser contacts**.



Figure 21 : réaction de Filtre des appels et SMS face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

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

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode **Les deux listes** ou **Liste noire** (cf. section "Modification du mode Filtre des appels et SMS" à la page 63) de Filtre des appels et SMS a été sélectionné, vous pouvez enrichir la liste noire en incluant tous les numéros sans chiffre (composés de lettres). Alors Filtre des appels et SMS pourra bloquer les SMS en provenance de numéros sans chiffres.

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

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

1. Sélectionnez **Menu** → **Filtre des appels et SMS**.

L'écran **Filtre app. /SMS** s'ouvre.

2. Sélectionnez l'option **Mode**.

L'écran **Filtre app. /SMS** s'ouvre.

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

- afin que Filtre des appels et SMS supprime automatiquement les messages en provenance de numéros sans chiffres, cochez la case **Interdire non numériques** ;
- afin que Filtre des appels et SMS filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour Filtre des appels et SMS, décochez la case **Interdire non numériques**.



Figure 22 : configuration des actions exécutées par Filtre des appels et SMS en cas de réception de SMS depuis un numéro sans chiffres.

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

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

En mode **Les deux listes** (cf. section "A propos des modes de Filtre des appels et SMS" à la page [63](#)), Filtre des appels et SMS analyse les SMS reçus correspondant aux listes noire et blanche.

Si le numéro de l'expéditeur ne figure ni dans la liste noire, ni dans la liste blanche, Filtre des appels et SMS vous prévient. Vous serez invité à choisir une des actions du Filtre des appels et SMS pour traiter le SMS entrant (cf. ill. ci-après).



Figure 23 : notification de Filtre des appels et SMS sur le SMS reçu

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

Les informations sur les SMS bloqués sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page [120](#)).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

En mode **Les deux listes** (cf. section **A propos des modes de Filtre des appels et SMS** à la page [63](#)) Filtre des appels et SMS analyse les SMS reçus correspondant aux listes noire et blanche.

Si le numéro de l'appelant ne figure ni dans la liste blanche, ni dans la liste noire, Filtre des appels et SMS vous le signalera après l'appel et proposera une action à exécuter sur les appels entrants (cf. ill. ci-après).



Figure 24 : notification de Filtre des appels et SMS sur l'appel reçu

Vous pouvez choisir l'une des actions suivantes pour le numéro de l'appelant :

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

Les informations relatives aux appels bloqués sont consignées dans le journal de l'application.

RESTRICTIONS SUR LES APPELS ET LES SMS SORTANTS. CONTROLE PARENTAL

Cette section présente le composant Contrôle parental qui permet de restreindre les appels et les SMS sortants à numéros. Elle explique également comment composer des listes de numéros interdits ou autorisés et configurer les paramètres du contrôle parental.

DANS CETTE SECTION

À propos du Contrôle parental	75
Modes du Contrôle parental	75
Activation/désactivation du Contrôle parental	76
Composition de la liste noire	76
Composition de la liste blanche.....	79

À PROPOS DU CONTROLE PARENTAL

Contrôle parental permet de contrôler les appels et les messages SMS sortants sur la base de listes noire et blanche de numéros de téléphone. Le fonctionnement du composant dépend du mode.

En mode **Liste noire**, le Contrôle parental interdit l'envoi de SMS et la réalisation d'appels vers les numéros de la liste noire. L'envoi de SMS et la réalisation d'appels vers les autres numéros est autorisée. En mode **Liste blanche**, le Contrôle parental autorise l'envoi de SMS et la réalisation d'appels uniquement vers les numéros de la liste blanche. L'envoi de SMS et la réalisation d'appels vers les autres numéros sont interdits par le Contrôle parental. En mode **Désactivé**, le Contrôle parental ne contrôle pas les SMS et les appels sortants.

Le Contrôle parental interdit les SMS envoyés uniquement à l'aide des outils standards de l'appareil. Le Contrôle parental autorise l'envoi de SMS via des logiciels tiers.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page [120](#)).

MODES DU CONTROLE PARENTAL

Le mode du Contrôle parental définit la règle selon laquelle le contrôle des SMS et des appels sortants est effectué.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Désactivé** : désactive Contrôle parental. Ne pas contrôler les SMS et les appels sortants.

Ce mode est sélectionné par défaut.

- **Liste blanche** : autorise l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste blanche (cf. section "Composition de la liste blanche" à la page [79](#)). Tous les autres SMS ou numéros sont bloqués.
- **Liste noire** : interdit l'envoi de SMS et/ou la réalisation d'appels uniquement vers des numéros de la liste noire (cf. section "Composition de la liste noire" à la page [76](#)). Tous les autres SMS ou numéros sont autorisés.

Vous pouvez changer le mode du Contrôle parental (cf. section "Activation/désactivation du contrôle parental" à la page 76). Le mode sélectionné de Contrôle parental apparaît à l'écran **Contrôle Parental** à côté de l'option de menu **Mode**.

ACTIVATION/DESACTIVATION DU CONTROLE PARENTAL

➔ Pour modifier le mode de Contrôle parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Sélectionnez l'option **Mode**.

L'écran **Contrôle Parental** s'ouvre.

3. Sélectionnez un des modes proposés pour Contrôle parental (cf. ill. ci-après).



Figure 25 : modification du mode du Contrôle parental

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

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à Contrôle parental pour bloquer les SMS et les appels sortants. La liste reprend les numéros de téléphone vers lesquels l'envoi de SMS et la réalisation d'appels seront interdits.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page [120](#)).

DANS CETTE SECTION

Ajout d'une entrée à la liste noire	77
Modification d'une entrée de la liste noire	78
Suppression d'une entrée de la liste noire	79

AJOUT D'UNE ENTREE A LA LISTE "NOIRE"

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la fois dans la liste noire et dans la liste blanche des numéros du Contrôle parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

➡ Pour ajouter une entrée à la liste noire de Contrôle parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

3. Sélectionnez **Menu** → **Ajouter**.

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

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

- **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
 - **Appels et SMS** : bloque les appels et les SMS sortants.
 - **Appels seuls** : bloque uniquement les appels sortants.
 - **SMS seuls** : interdit les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et 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).



Figure 26 : paramètres de l'enregistrement

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

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

► Pour modifier un enregistrement de la liste noire de *Contrôle parental*, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

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

L'écran **Modifier** s'ouvre.

4. Modifiez les paramètres requis :

- **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
 - **Appels et SMS** : bloque les appels et les SMS sortants.
 - **Appels seuls** : bloque uniquement les appels sortants.
 - **SMS seuls** : interdit les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe "+" et 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).

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

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste. De plus, vous pouvez purger la liste noire du Contrôle parental en supprimant tous les enregistrements qu'elle contient.

➡ *Pour supprimer une entrée de la liste noire de Contrôle parental, procédez comme suit :*

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.

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

➡ *Pour purger la liste noire Filtre des appels et SMS, procédez comme suit :*

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

L'écran **Liste noire** s'ouvre.

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

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer la liste blanche qui servira à Filtre des appels et SMS pour autoriser les SMS et les appels entrants.

DANS CETTE SECTION

Ajout d'une entrée à la liste blanche.....	80
Modification d'une entrée de la liste blanche.....	81
Suppression d'une entrée de la liste blanche.....	82

AJOUT D'UNE ENTREE A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la fois dans la liste noire et dans la liste blanche des numéros du Contrôle parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9 vous prévient : le message de circonstance s'affiche.

➡ Pour ajouter une entrée dans la liste blanche de Contrôle parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Choisissez l'option **Liste blanche**.

3. L'écran **Liste blanche** s'ouvre.

4. Sélectionnez **Menu** → **Ajouter**.

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

5. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

- **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :
 - **Appels et SMS** : autorise les appels et les SMS sortants.
 - **Appels seuls** : autorise uniquement les appels sortants.
 - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle parental pour l'envoi de SMS et/ou la réalisation d'appels. 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).



Figure 27 : paramètres de l'enregistrement

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

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

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

➡ Pour modifier un enregistrement de la liste blanche de Contrôle parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

L'écran **Contrôle Parental** s'ouvre.

2. Choisissez l'option **Liste blanche**.

3. L'écran **Liste blanche** s'ouvre.

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

L'écran **Modifier** s'ouvre.

5. Modifiez les paramètres requis :

- **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :
 - **Appels et SMS** : autorise les appels et les SMS sortants.
 - **Appels seuls** : autorise uniquement les appels sortants.

- **SMS seuls** : autorise les messages SMS sortants uniquement.
- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle parental pour l'envoi de SMS et/ou la réalisation d'appels. 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).

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

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

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

➡ *Pour supprimer une entrée de la liste blanche de Contrôle parental, procédez comme suit :*

1. Sélectionnez **Menu** → **Contrôle Parental**.
L'écran **Contrôle Parental** s'ouvre.
2. Choisissez l'option **Liste blanche**.
3. L'écran **Liste blanche** s'ouvre.
4. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
5. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

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

1. Sélectionnez **Menu** → **Contrôle Parental**.
L'écran **Contrôle Parental** s'ouvre.
2. Choisissez l'option **Liste blanche**.
3. L'écran **Liste blanche** s'ouvre.
4. Sélectionnez **Menu** → **Supprimer tout**.

La liste est désormais vide.

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, tout en facilitant sa recherche.

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

DANS CETTE SECTION

A propos du composant Antivol.....	83
Verrouillage de l'appareil.....	84
Suppression des données personnelles	86
Composition de la liste des dossiers à supprimer	88
Contrôle du remplacement de la carte SIM sur l'appareil.....	89
Détermination des coordonnées géographiques de l'appareil.....	91
Lancement à distance de la fonction Antivol	93

A PROPOS DU COMPOSANT ANTIVOL

L'Antivol protège les données de votre appareil mobile contre tout 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 de photos, 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 sont envoyées au numéro de téléphone et/ou à l'adresse de la messagerie électronique que vous avez spécifiée.
- **Localisation** : permet de déterminer les coordonnées de l'appareil. Le message indiquant les coordonnées géographiques de l'appareil est envoyé au numéro de téléphone qui a émis le SMS spécial, ainsi qu'à l'adresse de la messagerie électronique.

Toutes les fonctions d'Antivol sont désactivées après l'installation de Kaspersky Mobile Security 9.

Kaspersky Mobile Security 9 permet de lancer à distance la fonction Antivol via l'envoi d'une instruction SMS (cf. section "Lancement à distance de la fonction Antivol" à la page [93](#)) depuis un autre appareil mobile.

Pour exécuter les fonctions Antivol à distance, vous devrez utiliser le code secret de l'application qui a été défini lors de la première exécution de Kaspersky Mobile Security 9.

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. section "Journaux de l'application" à la page [120](#)).

VERROUILLAGE DE L'APPAREIL

Après réception d'une instruction spécifique de la commande SMS, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données comprises. 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. Choisissez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Verrouillage**.

L'écran **Verrouillage** s'ouvre.

3. Cochez la case **Activer le verrouillage**.

4. Dans le champ **Texte en cas de verrouillage**, modifiez le message qui apparaîtra à l'écran de l'appareil en position verrouillage (cf. ill. ci-après). Un texte standard est utilisé par défaut. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

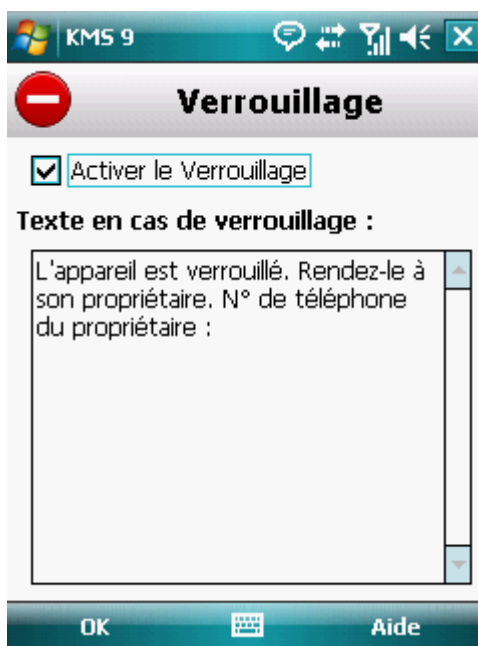


Figure 28 : paramètres de la fonction Verrouillage

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

Pour verrouiller un autre appareil, si la fonction Verrouillage est activée, procédez comme suit :

- Sur un autre appareil mobile doté de l'application de Kaspersky Lab pour appareils mobiles (par exemple, Kaspersky Mobile Security 9), rédigez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction spécifique SMS, 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. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

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

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 verrouiller l'appareil à distance, il est conseillé d'utiliser la méthode sûre à l'aide de la fonction Envoi d'une instruction. Dans ce cas, l'instruction et le code secret sont envoyés 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. Choisissez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Envoi d'une instruction**.

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

3. Attribuez au paramètre **La commande SMS** la valeur **Verrouillage** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code de l'appareil distant**, saisissez le code secret de l'appareil qui recevra l'instruction SMS.

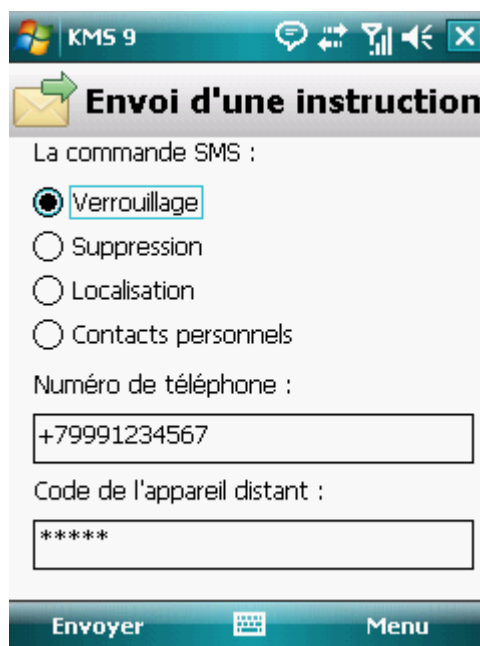


Figure 29 : lancement à distance du verrouillage de l'appareil

6. Cliquez sur **Envoyer**.

➡ *Pour composer un SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,*

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

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction spécifique SMS, la fonction Suppression des données permet de supprimer les informations suivantes de l'appareil :

- données personnelles de l'utilisateur (entrées des Contacts et sur la carte SIM, SMS, galerie, calendrier, paramètres de connexion à Internet) ;
- données sur la carte mémoire ;
- Les fichiers du dossier **Mes documents** et d'autres dossiers de la liste **Dossiers à supprimer**.

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

➡ *Pour activer la fonction Suppression des données, procédez comme suit :*

1. Choisissez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Mode**.

L'écran **Suppression** s'ouvre.

4. Cochez la case **Activer la suppression de données**.

5. Sélectionnez les informations à supprimer. Pour ce faire, dans le group **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 du dossier **Mes documents** et de la liste **Dossiers à supprimer**, cochez la case **Dossiers à supprimer**.

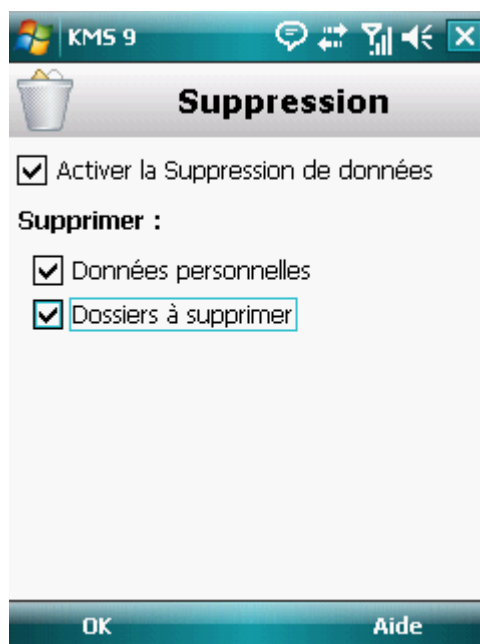


Figure 30 : sélection du type de données à supprimer

6. Cliquez sur **OK** pour enregistrer les modifications.
7. Passez à la constitution de la liste **Dossiers à supprimer** (cf. section "**Composition de la liste des objets à supprimer**" à la page [88](#)).

La suppression des données personnelles de l'appareil peut être effectuée comme suit :

- Sur un autre appareil mobile doté de l'application de Kaspersky Lab pour appareils mobiles (par exemple, Kaspersky Mobile Security 9), rédigez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction spécifique SMS, utilisez la fonction Envoi d'une instruction. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.
- Sur un autre appareil mobile, rédigez le message SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le.

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

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

1. Sélectionnez **Menu** → **Avancé**.
L'écran **Avancé** s'ouvre.
2. Choisissez l'option **Envoi d'une instruction**.
L'écran **Envoi d'une instruction** s'ouvre.
3. Attribuez au paramètre **La commande SMS** la valeur **Suppression** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code de l'appareil distant**, saisissez le code secret de l'appareil qui recevra l'instruction SMS.

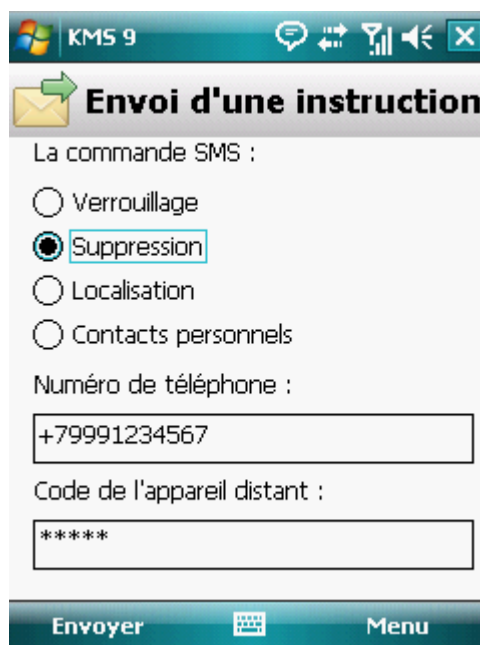


Figure 31 : lancement à distance de la fonction Supprimer

6. Cliquez sur **Envoyer**.

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

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

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception du SMS spécial.

Pour qu'Antivol supprime les dossiers de la liste après la réception de l'instruction spéciale par SMS, assurez-vous que la case **Dossiers à supprimer** est cochée dans le menu **Mode**.

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

1. Sélectionnez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

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

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

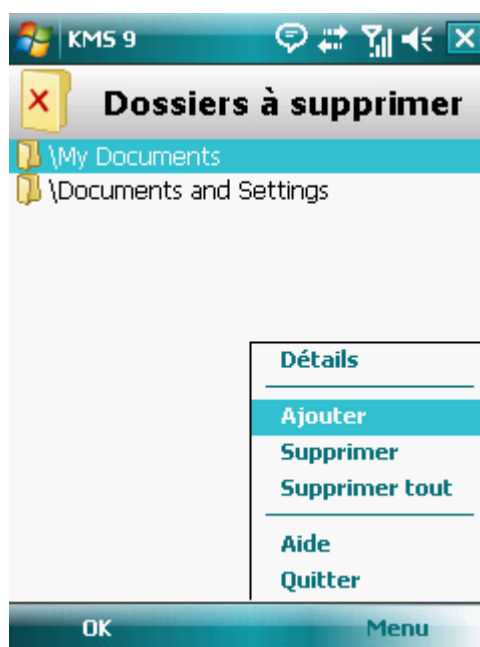


Figure 32 : sélection du dossier à supprimer

5. Sélectionnez le dossier requis dans l'arborescence, puis cliquez sur **Sélect.**

Le dossier sera ajouté à la liste.

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

1. Sélectionnez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

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

4. Sélectionnez un dossier dans la liste, puis appuyez sur **Menu** → **Supprimer**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

En cas de remplacement de la carte SIM, SIM-Surveillance permet 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 **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Choisissez l'option **SIM-Surveillance**.

L'écran **SIM-Surveillance** s'ouvre.

3. Cochez la case **Activer SIM-Surveillance**.

4. Pour contrôler le remplacement de la carte SIM sur l'appareil, configurez les paramètres suivants (cf. ill. ci-dessous) :

- Pour envoyer automatiquement le SMS concernant le nouveau numéro de votre téléphone, dans le champ **SMS au numéro de tél** du groupe **Envoyer le numéro de tél.**, saisissez le numéro de téléphone vers lequel le message sera envoyé.

Ces numéros peuvent commencer par un chiffre ou par le signe "+" et ne peuvent contenir que des chiffres.

- Pour recevoir un courrier électronique sur le nouveau numéro de téléphone, dans le group **Envoyer le numéro de tél.** dans le champ **Mess. sur l'ad. du cour. élec.**, saisissez l'adresse du courrier électronique.
- Pour verrouiller l'appareil en cas de remplacement de la carte SIM ou de mise en marche de l'appareil sans celle-ci, pour le paramètre **Avancé**, cochez la case **Verrouiller l'appareil**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

- 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 33 : paramètres de la fonction SIM-Surveillance

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

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Localisation 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. Choisissez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Localisation**.

L'écran **Localisation** s'ouvre.

3. Cochez la case **Activer la localisation**.

Kaspersky Mobile Security 9 renvoie par défaut les coordonnées de l'appareil dans un SMS.

4. Pour recevoir les coordonnées de l'appareil dans le courrier électronique, pour le paramètre **Mess. sur l'ad. du cour. élec.**, saisissez l'adresse du courrier électronique (cf. ill. ci-après).



Figure 34 : paramètres de la fonction Localisation

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

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, procédez comme suit :

- Sur un autre appareil mobile doté de l'application de Kaspersky Lab pour appareils mobiles (par exemple, Kaspersky Mobile Security 9), rédigez une instruction SMS et envoyez-la à 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 spécifique SMS, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'autre appareil recevant le SMS et envoyez-le. Votre appareil recevra à l'insu de l'utilisateur un SMS, et 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 mobile.

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 déterminer à distance les coordonnées, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, l'instruction et le code secret sont envoyés en mode crypté.

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

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Envoi d'une instruction**.

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

3. Attribuez au paramètre **La commande SMS** la valeur **Localisation** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
5. Dans le champ **Code de l'appareil distant**, saisissez le code secret de l'appareil qui recevra l'instruction SMS.

Figure 35 : Détermination des coordonnées de l'appareil

6. Cliquez sur **Envoyer**.

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

envoyez à l'autre appareil un message SMS contenant le texte `find :<code>` (où `<code>` est le code secret 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 spécifique par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Mobile Security. L'instruction SMS est envoyée sous forme d'un SMS crypté qui contient le code secret de l'application, installé 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 vers un autre appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Envoi d'une instruction**.

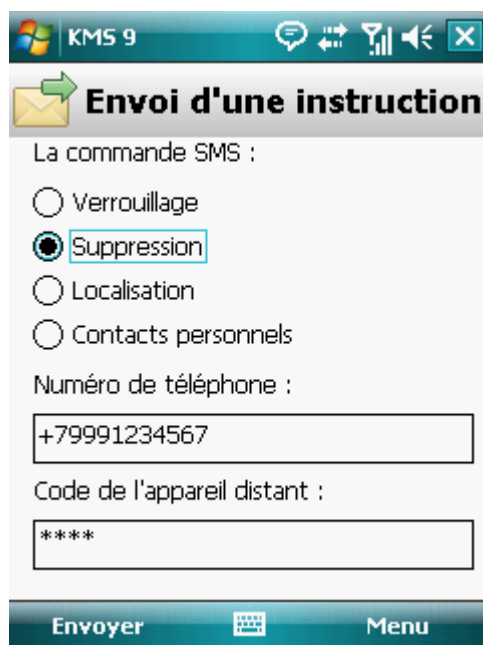
L'écran **Envoi d'une instruction** s'ouvre.

3. Sélectionnez une des valeurs proposées pour le paramètre **La commande SMS** (cf. ill. ci-après) :

- **Verrouillage.**
- **Suppression.**
- **Localisation.**
- **Contacts personnels** (cf. section "**Dissimulation des informations confidentielles**" à la page [96](#)).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code de l'appareil distant**, saisissez le code secret de l'appareil qui recevra l'instruction SMS.



KMS 9

Envoi d'une instruction

La commande SMS :

☐ Verrouillage

☒ Suppression

☐ Localisation

☐ Contacts personnels

Numéro de téléphone :

+79991234567

Code de l'appareil distant :

Envoyer Menu

Figure 36 : lancement à distance de la fonction Antivol

6. Cliquez sur **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

Présentation du composant Contacts personnels	96
Présentation des modes de Contacts personnels	96
Activation/désactivation de Contacts personnels	97
Activation automatique de Contacts personnels	98
Activation de la dissimulation des informations confidentielles à distance	99
Composition de la liste des numéros confidentiels.....	101
Sélection des informations à dissimuler : Contacts personnels.....	104

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 Mobile Security 9 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. section "Journaux de l'application" à la page [120](#)).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

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

La dissimulation est désactivée par défaut.

Les modes suivants sont prévus pour Contacts personnels :

- **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 de la dissimulation des données personnelles (cf. section "Activation automatique de Contacts personnels" à la page [98](#)) ou son activation à distance depuis un autre appareil (cf. section "Activation de la dissimulation des informations confidentielles à distance" à la page [99](#)).

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

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

ACTIVATION/DESACTIVATION DE CONTACTS PERSONNELS

Vous pouvez modifier le mode de Contacts personnels d'une des méthodes suivantes :

- depuis le menu de configuration du composant ;
- depuis le menu **Contacts personnels**.

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

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Mode**.

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

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

4. Cliquez sur **OK**.

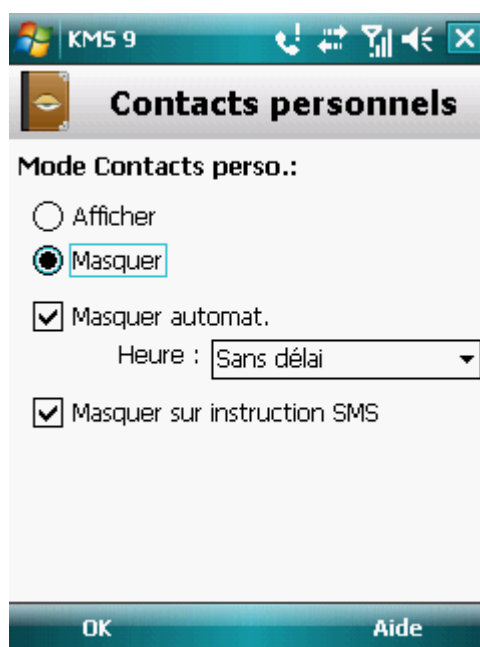


Figure 37 : modification du mode de Contacts personnels

5. Confirmez la modification du mode de travail de Contacts personnels. Pour ce faire, cliquez sur **Oui**.

➤ Pour changer rapidement le mode Contacts personnels, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Appuyez sur **Masquer** / **Afficher**. Le texte du bouton changera en fonction de l'état actuel de Contacts personnels.
3. Confirmez la modification du mode Contacts personnels. Pour ce faire, cliquez sur **Oui**.

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 **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Mode**.

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

3. Cochez la case **Masquer automat.** (cf. ill. ci-après).

4. 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.
- Dans 1 minute.
- Dans 5 minutes.
- Dans 15 minutes.
- Dans 1 heure.

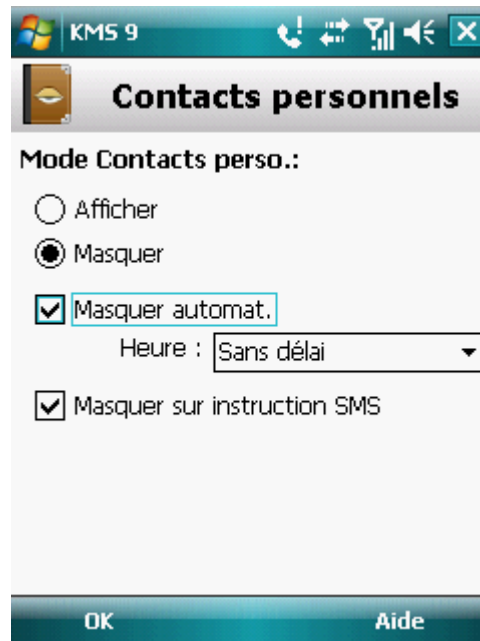


Figure 38 : paramètres de lancement automatique de Contacts personnels

5. Cliquez sur **OK**.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Mobile Security 9 permet d'activer à distance la dissimulation des informations confidentielles depuis un autre appareil mobile. Pour ce faire, il faut d'abord activer sur votre appareil la fonction Masquer par instruction SMS.

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

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Mode**.

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

3. Cochez la case **Masquer sur instruction SMS** (cf. ill. ci-après).

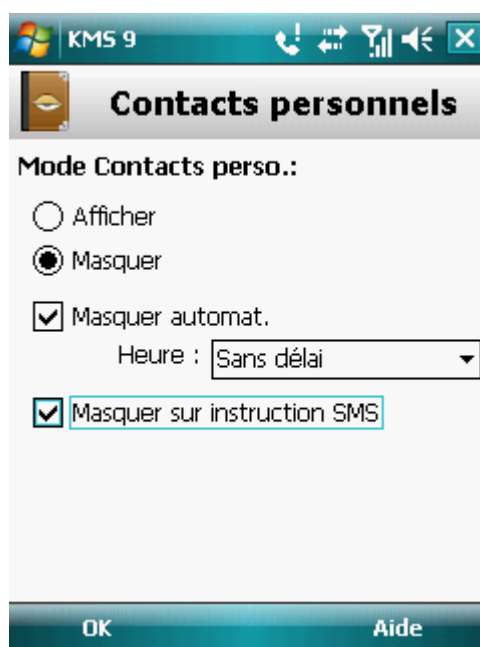


Figure 39 : paramètres d'activation à distance du composant *Contacts personnels*

4. Cliquez sur **OK**.

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

- Sur un autre appareil mobile doté de l'application de Kaspersky Lab pour appareils mobiles (par exemple, Kaspersky Mobile Security 9), rédigez une instruction SMS et envoyez-la à votre appareil. Votre appareil recevra à l'insu de l'utilisateur un SMS qui déclenchera la dissimulation des informations confidentielles. Pour rédiger l'instruction spécifique SMS, utilisez la fonction Envoi d'une instruction.
- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra un SMS qui déclenchera la dissimulation des informations confidentielles.

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

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

1. Sélectionnez **Menu** → **Avancé**.
L'écran **Avancé** s'ouvre.
2. Choisissez l'option **Envoi d'une instruction**.
L'écran **Envoi d'une instruction** s'ouvre.
3. Attribuez au paramètre **La commande SMS** la valeur **Contacts personnels** (cf. ill. ci-après).
4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code de l'appareil distant**, saisissez le code secret de l'appareil qui recevra l'instruction SMS.

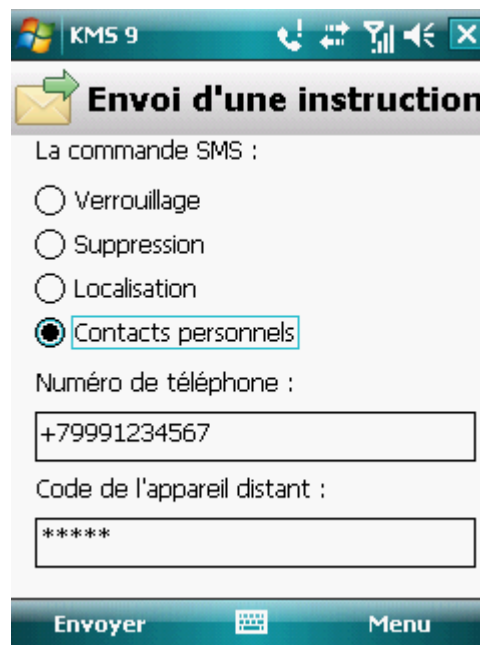


Figure 40 : lancement à distance de Contacts personnels

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

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 numéro à la liste des numéros confidentiels.....	102
Modification d'un numéro de la liste des numéros confidentiels.....	103
Suppression d'un numéro de la liste des numéros confidentiels.....	103

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

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

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

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

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Liste des contacts**.

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

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

- Pour ajouter un numéro depuis les Contacts, sélectionnez **Menu** → **Ajouter** → **Contact Outlook**. Dans l'écran **Contact Outlook** qui s'ouvre, choisissez l'entrée requise, puis appuyez sur **Sélect**.
- Pour ajouter un numéro enregistré sur la carte SIM, sélectionnez **Menu** → **Ajouter** → **Contact de la carte SIM**. Dans l'écran **Contact de la carte SIM** qui apparaît, choisissez l'enregistrement requis, puis cliquez sur **OK**.
- Pour ajouter un numéro manuellement, choisissez l'option **Menu** → **Ajouter** → **Numéro**. Dans l'écran **Ajouter** qui apparaît, remplissez le champ **Numéro de téléphone** puis cliquez sur **OK**.



Figure 41 : ajout d'un enregistrement à la liste des contacts protégés

Le numéro est alors ajouté à la liste des contacts.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

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

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

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

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Liste des contacts**.

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

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

L'écran **Modifier** s'ouvre.

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

5. Cliquez sur **OK** une fois les modifications effectuées.

Le numéro sera modifié.

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro de la liste des numéros confidentiels ou purger la Liste de contacts.

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

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

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Liste des contacts**.

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

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

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

➤ Pour purger la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

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

2. Sélectionnez l'option **Liste des contacts**.

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

3. Sélectionnez l'option **Menu** → **Supprimer tout**.
4. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

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

Désactivez la dissimulation des informations 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. Choisissez **Menu** → **Contacts personnels**.

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

2. Choisissez l'option **Objets à masquer**.

L'écran **Objets à masquer** (cf. ill. ci-après) apparaît.

3. Dans le groupe **Masquer les infos**, choisissez les informations qui seront masquées pour les numéros confidentiels. Les paramètres suivants sont prévus :

- **Contacts** : masque toutes les informations relatives aux numéros confidentiels.
- **SMS** : masque les SMS dans les dossiers **Entrant**, **Sortant**, **Transmis** pour les numéros confidentiels.
- **Enreg. des appels** : accepte les appels en provenance des numéros confidentiels sans identifier le numéro de l'appelant et sans afficher les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).

4. Dans le groupe **Masquer les événements**, sélectionnez les événements qui seront masqués pour les numéros confidentiels. Les paramètres suivants sont prévus :

- **SMS entrant** : masquer la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.

- **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité "occupé"). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.



Figure 42 : sélection des objets cachés

5. Cliquez sur **OK**.

FILTRAGE DE L'ACTIVITE RESEAU.

PARE-FEU

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

DANS CETTE SECTION

À propos du Pare-feu	106
Activation/désactivation du Pare-feu	106
Sélection du mode Pare-feu	107
Notifications sur les blocages	107

À PROPOS DU PARE-FEU

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

Le Pare-feu est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.

Le Pare-feu permet de configurer les notifications des connexions bloquées (cf. section "Activation/désactivation du Pare-feu" à la page [106](#)).

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section "Journaux de l'application" à la page [120](#)).

ACTIVATION/DESACTIVATION DU PARE-FEU

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

- **Désact.** : autorisation de la moindre activité de réseau. Ce niveau de sécurité est choisi par défaut.
- **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Protection maximum** : bloque toutes les connexions entrantes. La réception du courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Bloquer tout** : bloque la moindre activité de réseau, à l'exception de la mise à jour des bases antivirus et du renouvellement de la licence.

Vous pouvez modifier le niveau de sécurité offert par Pare-feu (cf. section "Sélection du niveau de sécurité du Pare-feu" à la page [107](#)). Le mode actuel apparaît sur l'écran **Pare-feu** à côté de l'option du menu **Mode**.

SELECTION DU MODE PARE-FEU

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

➡ Pour sélectionner le niveau de protection du Pare-feu, procédez comme suit :

1. Sélectionnez **Menu** → **Pare-feu**.

L'écran **Pare-feu** s'ouvre.

2. Sélectionnez l'option **Mode**.

L'écran **Mode** s'ouvre.

3. Sélectionnez l'un des modes proposés pour le Contrôle parental (cf. ill. ci-après).

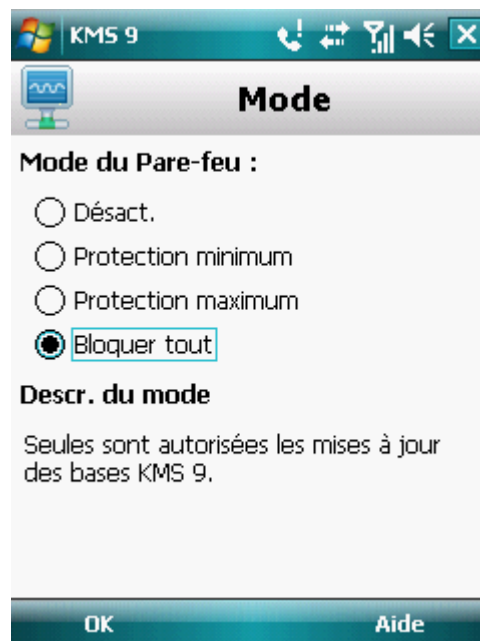


Figure 43 : sélection du niveau de sécurité du Pare-feu

4. Cliquez sur **OK**.

NOTIFICATIONS SUR LES BLOCAGES

Le Pare-feu permet d'obtenir des notifications sur le blocage des connexions. Vous pouvez administrer les notifications du Pare-feu.

Par défaut, la remise des notifications sur le blocage est désactivée.

➡ Pour administrer les notifications sur le blocage, procédez comme suit :

1. Sélectionnez **Menu** → **Pare-feu**.

L'écran **Pare-feu** s'ouvre.

2. Choisissez l'option **Notifications**.

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

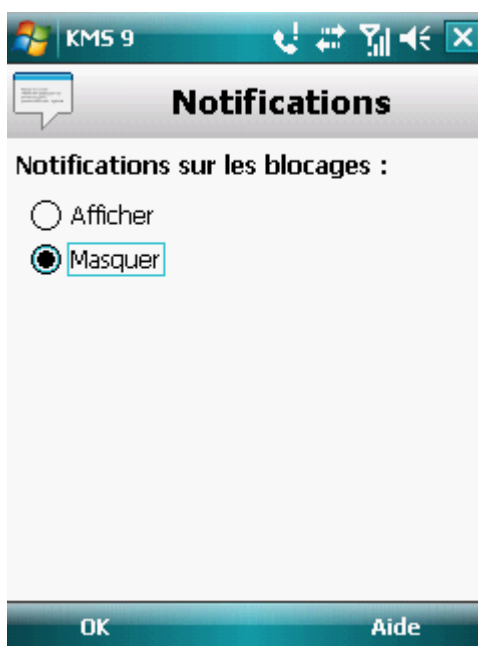


Figure 44 : configuration de la remise des notifications sur le blocage

3. Dans le groupe **Notifications sur les blocages**, sélectionnez une des options proposées :
 - **Afficher** : active la remise des notifications. Le Pare-feu signale le blocage de la connexion.
 - **Masquer** : désactiver la distribution des notifications. Le Pare-feu ne signale pas le blocage de la connexion.
4. Cliquez sur **OK**.

CHIFFREMENT DES DONNEES PERSONNELLES

La section présente le composant Chiffrement, qui permet de chiffrer les dossiers sur l'appareil. La section décrit également comment chiffrer et déchiffrer les dossiers sélectionnés.

DANS CETTE SECTION

À propos du chiffrement	109
Chiffrement des données	109
Déchiffrement des données	111
Interdiction d'accès aux données chiffrées.....	112

À PROPOS DU CHIFFREMENT

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

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

Pour utiliser les dossiers chiffrés, il faut saisir le code secret de l'application (cf. section "Saisie du code secret" à la page [31](#)). Une fois que la période définie après le passage de l'appareil en mode d'économie de l'énergie est écoulée (cf. section "Interdiction d'accès aux données chiffrées" à la page [112](#)), l'accès aux données sera bloqué automatiquement.

Les fichiers dans le dossier sont chiffrés lors de l'exécution de la commande **Chiffrer** après quoi les données sont chiffrées ou déchiffrées "au vol" au fur et à mesure que des fichiers sont ajoutés, extraits ou consultés dans le dossier.

Avant de lancer des fichiers exécutables depuis le dossier chiffré, il faut déchiffrer ce dossier.

Le Chiffrement est désactivé après l'installation de Kaspersky Mobile Security 9.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page [120](#)).

CHIFFREMENT DES DONNEES

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

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

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

➡ *Pour chiffrer les données, procédez comme suit :*

1. Sélectionnez **Menu** → **Chiffrement**.

L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

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

3. Appuyez sur **Menu** → **Ajouter**.

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

4. Sélectionnez le dossier qu'il faut absolument chiffrer, puis appuyez sur **Chiffrer** (cf. ill. ci-après).

Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick de l'appareil.

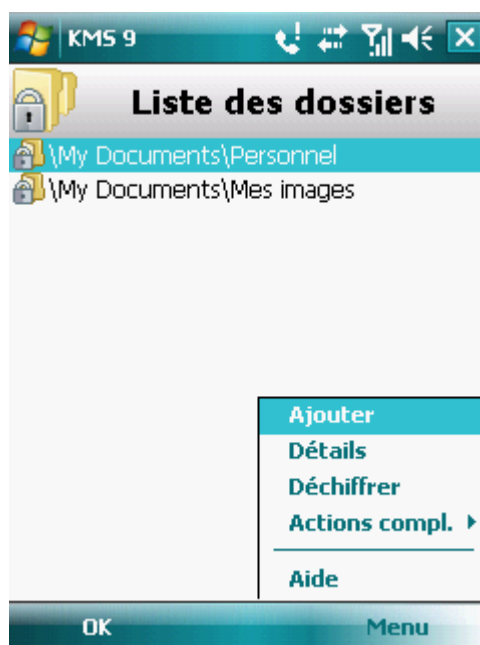


Figure 45 : chiffrement des données

Kaspersky Mobile Security 9 vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

5. Cliquez sur **OK**.

Pour le dossier sélectionné, l'option **Chiffrer** du **Menu** devient **Déchiffrer**.

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

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

1. Sélectionnez **Menu** → **Chiffrement**.

L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

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

3. Sélectionnez **Menu** → **Actions compl.** → **Tout chiffrer**.

Kaspersky Mobile Security 9 vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Cliquez sur **OK**.

DECHIFFREMENT DES DONNEES

Il est possible de déchiffrer complètement les données préalablement chiffrées (cf. section "Chiffrement de données" à la page [109](#)). Vous pouvez déchiffrer un seul dossier ou tous les dossiers chiffrés sur l'appareil.

➡ *Pour déchiffrer un dossier chiffré, procédez comme suit :*

1. Sélectionnez **Menu** → **Chiffrement**.

L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

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

- Sélectionnez le dossier chiffré dans la liste, puis appuyez sur **Menu** → **Déchiffrer** (cf. ill. ci-après).

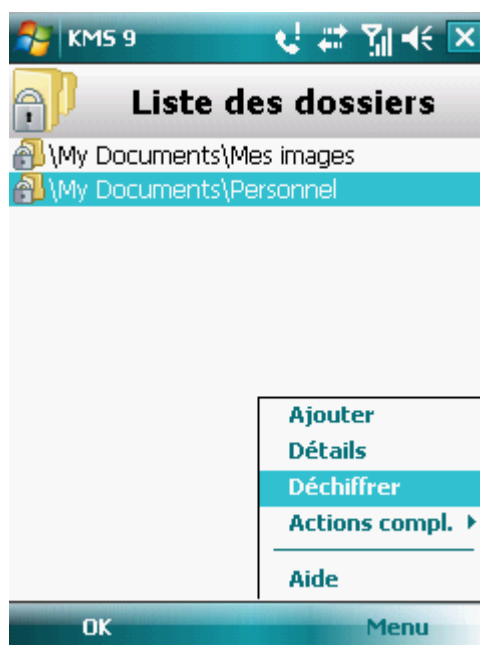


Figure 46 : activation de la fonction

Kaspersky Mobile Security 9 vous préviendra lorsque la procédure de déchiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

- Cliquez sur **OK**.

Pour le dossier déchiffré, l'option **Déchiffrer** du **Menu** devient **Chiffrer**. Vous pouvez à nouveau utiliser le chiffrement de données (cf. section "Chiffrement de données" à la page [109](#)).

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

- Sélectionnez **Menu** → **Chiffrement**.

L'écran **Chiffrement** s'ouvre.

- Choisissez l'option **Liste des dossiers**.

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

- Sélectionnez **Menu** → **Actions compl.** → **Tout déchiffrer**.

Kaspersky Mobile Security 9 vous préviendra lorsque la procédure de déchiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

- Cliquez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le Chiffrement permet de définir la période à l'issue de laquelle l'interdiction de l'accès aux dossiers chiffrés sera activée. La fonction est activée au moment de passage de l'appareil en mode d'économie de l'énergie. Pour utiliser les informations chiffrées, il faudra saisir le code secret de l'application. Ensuite, pour pouvoir utiliser les données chiffrées, il faudra saisir le code secret (cf. section "Saisie du code secret" à la page [31](#)).

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

► Pour bloquer l'accès au dossier après l'écoulement d'une durée définie, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Interdiction de l'accès**.

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

3. Définissez la durée après le passage de l'appareil en mode de veille pendant laquelle les données seront accessibles. Pour ce faire, attribuez au paramètre **Bloquer l'accès** une des valeurs proposées (cf. ill. ci-après) :

- **Sans délai.**
- **Dans 1 min.**
- **Dans 5 min.**
- **Dans 15 min.**
- **Dans 1 heure.**



Figure 47 : blocage de l'accès aux données chiffrées

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

➡ *Pour interdire momentanément l'accès aux dossiers,*

cliquez sur l'icône de Kaspersky Mobile Security 9 dans la barre d'état système de l'appareil et choisissez l'option **Verrouiller les données** (cf. ill. ci-après).



Figure 48 : menu contextuel de l'application dans la barre d'état système de l'appareil

MISE A JOUR DES BASES DU PROGRAMME

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

DANS CETTE SECTION

À propos de la mise à jour des bases	115
Affichage des informations sur les bases	116
Mise à jour manuelle	116
Planification des mises à jour	117
Mise à jour en itinérance	118

À PROPOS DE LA MISE A JOUR DES BASES

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

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

Kaspersky Mobile Security 9 télécharge la mise à jour des bases antivirus de l'application depuis les serveurs de mises à jour de Kaspersky Lab. Il s'agit de sites Internet spéciaux où sont hébergées les mises à jour des bases pour toutes les applications de Kaspersky Lab.

Pour pouvoir actualiser les bases antivirus de l'application, l'appareil mobile doit être connecté à Internet.

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

1. Les bases antivirus de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial de Kaspersky Lab.
2. Kaspersky Mobile Security 9 exécute une des actions suivantes :
 - Si les bases antivirus de l'application que vous utilisez sont à jour, un message d'informations apparaît à l'écran.
 - Si les bases antivirus installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

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

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

Vous pouvez obtenir des informations détaillées sur les bases antivirus utilisées sur l'écran **Avancé** depuis l'option du menu **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. section "Journaux de l'application" à la page [120](#)).

AFFICHAGE DES INFORMATIONS SUR LES BASES

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

➡ *Pour consulter les informations sur les bases installées, procédez comme suit :*

1. Choisissez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Infos des bases**.

L'écran **Infos des bases** s'ouvre. Il présente des informations sur les bases antivirus de l'application installées (cf. ill. ci-après).

MISE A JOUR MANUELLE

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

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

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Mise à jour**.

L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Lanc. de la mise à jour** (cf. ill. ci-après).

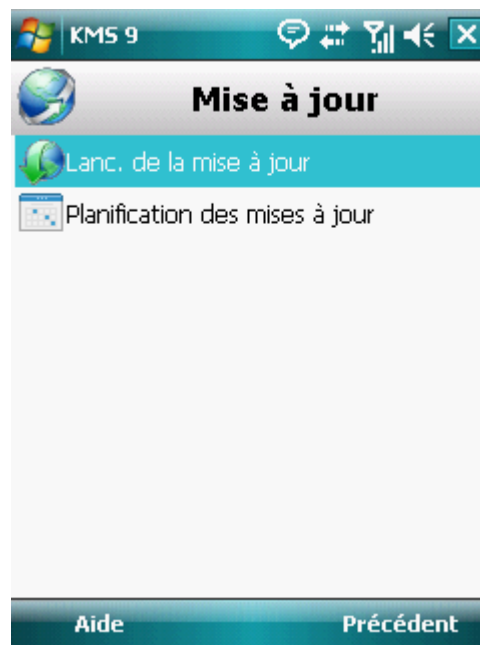


Figure 49 : lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

PLANIFICATION DES MISES A JOUR

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

➡ Pour configurer la mise à jour automatique des bases antivirus du logiciel, procédez de la manière suivante :

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Mise à jour**.

L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des mises à jour**.

L'écran **Planification** s'ouvre.

4. Cochez la case **Mise à jour programmée** (cf. ill. ci-après).

5. Programmez l'exécution de la mise à jour. Pour ce faire, attribuez une valeur au paramètre **Fréquence** :

- **Chaque jour** : actualise les bases antivirus chaque jour. Saisissez ensuite la valeur pour le paramètre **Heure**.

- **Chaque semaine** : actualise les bases antivirus de l'application une fois par semaine. Ensuite, sélectionnez une valeur pour les paramètres **Heure** et **Jour de la semaine**.

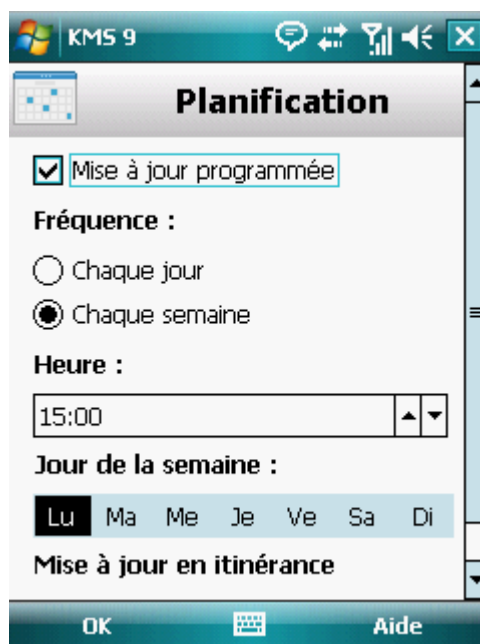


Figure 50 : paramètres de la mise à jour automatique

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

MISE A JOUR EN ITINERANCE

Si vous êtes en itinérance, vous pouvez activer/désactiver la mise à jour programmée des bases antivirus de l'application. Si la mise à jour programmée en itinérance est interdite, la mise à jour manuelle sera accessible en mode normal.

- *Pour autoriser la mise à jour programmée des bases antivirus de l'application en cas d'itinérance, procédez comme suit :*

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** s'ouvre.

2. Sélectionnez l'option **Mise à jour**.

L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des mises à jour**.

L'écran **Planification** s'ouvre.

4. Dans le groupe **Mise à jour en itinérance**, cochez la case **Mettre à jour en itinérance**.

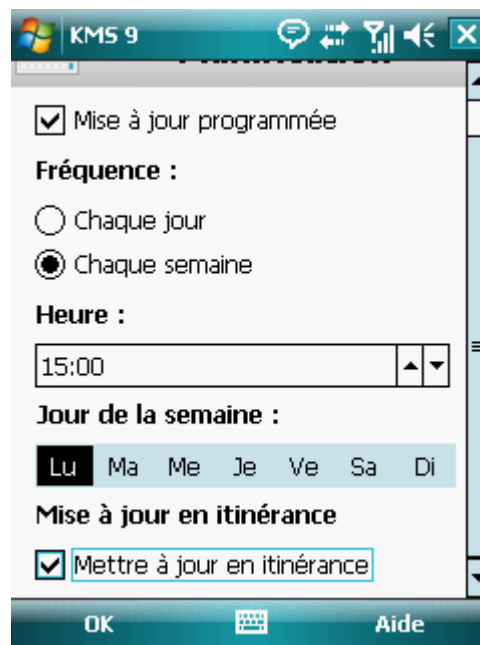


Figure 51 : configuration des mises en jour en itinérance

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

JOURNAUX DU LOGICIEL

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

DANS CETTE SECTION

À propos des journaux	120
Affichage des événements du journal	120
Suppression des enregistrements du journal	121

À PROPOS DES JOURNAUX

Les journaux reprennent les enregistrements des événements survenus pendant le fonctionnement de chaque composant de Kaspersky Mobile Security 9. Les enregistrements sont triés selon l'heure de l'événement et classés par ordre chronologique.

Il existe un journal des événements pour chaque composant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

➡ *Pour afficher tous les enregistrements repris dans le journal, procédez comme suit :*

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Journaux**.

L'écran **Journaux** s'ouvre.

3. Choisissez le composant pour lequel vous souhaitez consulter le journal.

Le journal des événements du composant sélectionné s'ouvre.

➡ *Pour afficher des informations détaillées sur les enregistrements du journal,*

sélectionnez l'enregistrement requis puis cliquez sur **Détails**.

L'écran **Détails** reprend des informations sur l'action exécutée par l'application et ses détails. Par exemple, pour l'action "Objet en quarantaine", le chemin d'accès au fichier infecté sur l'appareil est également affiché.

➡ *Pour revenir à la liste des journaux,*

appuyez sur **Menu** → **Précédent**.

SUPPRESSION DES ENREGISTREMENTS DU JOURNAL

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Mobile Security 9 seront supprimées.

➡ Pour purger tous les journaux, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Journaux**.

L'écran **Journal** s'ouvre.

3. Ouvrez le journal de n'importe quel composant.

4. Choisissez **Menu** → **Supprimer tout** (cf. ill. ci-dessous).



Figure 52 : suppression des enregistrements

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

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section offre des informations sur les possibilités complémentaires de Kaspersky Mobile Security 9 : comment modifier le code secret, administrer les notifications sonores de l'application et comment activer/désactiver l'affichage des astuces.

DANS CETTE SECTION

Modification du code secret.....	122
Affichage des astuces	122
Administration des notifications sonores	123

MODIFICATION DU CODE SECRET

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

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

1. Choisissez **Menu** → **Avancé**.
L'écran **Avancé** s'ouvre.
2. Sélectionnez l'option **Paramètres**.
L'écran **Paramètres** s'ouvre.
3. Choisissez l'option **Modification du code**.
4. Tapez le code actuel dans la zone **Saisissez le code secret**.
5. Saisissez le nouveau code dans le champ **Saisissez le code** et **Confirmation du code**, puis cliquez sur **OK** pour enregistrer les modifications.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Mobile Security 9 affiche, par défaut, des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Mobile Security 9.

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

1. Sélectionnez **Menu** → **Avancé**.
L'écran **Avancé** s'ouvre.
2. Sélectionnez l'option **Paramètres**.
L'écran **Paramètres** s'ouvre.

- Sélectionnez l'option **Astuces**.

L'écran **Astuces** s'ouvre.

- Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :

- **Afficher** : affiche l'astuce avant de configurer les paramètres de la fonction sélectionnée.
- **Masquer** : aucune astuce n'est affichée.

- Cliquez sur **OK**.

ADMINISTRATION DES NOTIFICATIONS SONORES

Divers événements définis peuvent survenir durant l'utilisation de l'application : découverte d'un objet infecté ou d'un virus, expiration de la licence, etc. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Par défaut, Kaspersky Mobile Security 9 active la notification sonore uniquement selon le mode défini de l'appareil.

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

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

- Choisissez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre.

- Sélectionnez l'option **Paramètres**.

L'écran **Paramètres** s'ouvre.

- Choisissez l'option **Son**.

L'écran **Son** s'ouvre.

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

- **Activer** : utilise les notifications sonores quel que soit le profil sélectionné pour l'appareil.
- **Désactiver** : n'utilise pas les notifications sonores.

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

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

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

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

Avant de contacter le Service d'assistance technique, prenez connaissance des Règles de support (<http://support.kaspersky.fr/support/rules>).

Poser votre question au Service d'assistance technique

Vous pouvez transmettre votre demande aux spécialistes du Service d'assistance technique en remplissant le formulaire de Helpdesk à l'adresse : <http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>.

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

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

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

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

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

- **Le type de demande.** Sélectionnez le sujet qui correspond le mieux au problème rencontré, par exemple, "Problème d'installation/de suppression du logiciel" ou "Problème de recherche/de neutralisation de virus". Si vous ne trouvez pas un sujet correspondant à votre situation, choisissez "Question générale".
- **Nom et version de l'application.**
- **Zone de texte.** Décrivez le problème rencontré avec le plus de détails possible.
- **Numéro client et mot de passe.** Saisissez l'Identifiant client et le mot de passe reçus lors de votre inscription sur le site du Service d'assistance technique.
- **Adresse électronique.** Les experts du Service d'assistance technique enverront leur réponse à cette adresse.

Assistance technique téléphonique

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

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

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

ANALYSE A LA DEMANDE

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

ARCHIVE

Fichier "conteneur" d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

BASES ANTIVIRUS

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît.

BLOPAGE D'UN OBJET

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

C

CODE SECRET DE L'APPLICATION

Le code secret de l'application permet d'éviter l'accès non autorisé aux paramètres de l'application et aux données protégées de l'appareil. Il est saisi par l'utilisateur lors du premier lancement de l'application et comprend au moins quatre chiffres. Il faut saisir le code secret de l'application dans les cas suivants :

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

D

DUREE DE LICENCE

Période de temps pendant laquelle il est possible d'exploiter toutes les caractéristiques d'une application Kaspersky Lab. A l'expiration de la licence, les fonctionnalités de l'application seront limitées. Dans ce mode sont accessibles les fonctions suivantes :

- désactiver tous les composants ;
- déchiffrer un ou plusieurs dossiers ;

- désactiver de la dissimulation des informations confidentielles ;
- désactiver la dissimulation automatique des informations confidentielles ;
- consulter le système d'aide.

DESINFECTION OU REPARATION D'OBJETS

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

L

LISTE BLANCHE

Les entrées de cette liste contiennent les informations suivantes :

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

M

MASQUE DE FICHIERS

Représentation du nom et de l'extension d'un fichier moyennant des caractères génériques. Les deux caractères génériques de base utilisés dans les masques de fichier sont * et ? (où * représente une suite de caractères quelconques et ? un seul caractère). Grâce à ces caractères génériques, il est possible de désigner n'importe quel fichier. Notez que le nom et l'extension du fichier sont toujours séparés par un point.

MISE A JOUR DES BASES

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

N

NON-NUMERIQUES

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

O**OBJET INFECTÉ**

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l'appareil.

P**PLACER DES OBJETS EN QUARANTAINE**

Méthode permettant de traiter des objets probablement infectés, en interdisant leur accès et en les déplaçant de leur position d'origine vers le dossier de quarantaine, où l'objet est enregistré sous une forme chiffrée qui annule toute menace d'infection.

Q**QUARANTAINE**

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

R**RESTAURATION D'UN OBJET**

Déplacement d'un objet original depuis le dossier de quarantaine vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un autre dossier spécifié par l'utilisateur.

S**SUPPRESSION SMS**

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

SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme. Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

KASPERSKY LAB

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/fr>

Laboratoire antivirus : newvirus@kaspersky.com
(envoi uniquement d'objets suspects sous forme d'archive)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>
(pour les questions aux experts antivirus)

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

INFORMATIONS SUR LE CODE TIERS

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

DANS CETTE SECTION

Code de programmation diffusé	129
Autres informations	131

CODE DE PROGRAMMATION DIFFUSE

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

DANS CETTE SECTION

ADB.....	129
ADBWINAPI.DLL	129
ADBWINUSBAPI.DLL	129

ADB

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

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

ADBWINAPI.DLL

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

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

ADBWINUSBAPI.DLL

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

Apache License

Version 2.0, January 2004

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

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

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

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

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

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

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

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

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

END OF TERMS AND CONDITIONS

AUTRES INFORMATIONS

Informations complémentaires sur le code tiers.

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

Actions	
analyse à la demande	57
Actions sur les objets	50, 57
Activation	
Contacts personnels	97
Activation de l'application	
licence	37
Activation du logiciel	27
Activer	
chiffrement	110
Contrôle parental	75, 76
Filtre des appels et SMS	63
firewall	107
Afficher	
Etat de la protection	44
Ajout	
liste blanche du Contrôle parental	80
liste blanche du Filtre des appels et SMS	68
liste des numéros confidentiels des Contacts personnels	102
liste noire du Contrôle parental	77
Ajouter	
liste noire du Filtre des appels et SMS	65
Analyse à la demande	
actions à appliquer sur les objets	57
archives	56
exécution manuelle	53
exécution planifiée	54
objets à analyser	55
Antivol	83
Antivol	
verrouillage	84
Antivol	
suppression de données	86
Antivol	
SIM-Surveillance	90
Antivol	
Localisation	91
Archives	
analyse à la demande	55, 56
Autorisation	
appels entrants	68
SMS entrants	68
Autoriser	
appels sortants	79
connexions réseau	107
messages SMS sortants	79

C

Chiffrement	
blocage automatique d'accès	113
chiffrement des données	110
déchiffrement des données	111
Code	

code d'activation	27, 28, 31
code secret de l'application	32
Code secret de l'application	32, 33
Contacts personnels	
lancement automatique	98
liste des contacts confidentiels	101
modes	97
sélection des informations et des événements à dissimuler	104
CONTACTS PERSONNELS	96
Contrat de licence	36
Contrôle parental	
liste blanche	79
liste noire	77
modes	75
D	
Désactivation	
Contacts personnels	97
Désactiver	
chiffrement	111
Contrôle parental	75, 76
Filtre des appels et SMS	63
firewall	106, 107
Données	
accès avec un code secret	113
chiffrement	110
déchiffrement	111
DONNÉES	
INFORMATIONS CONFIDENTIELLES	96
E	
Enregistrer	
liste blanche du Contrôle parental	80
Entrée	
liste blanche du Filtre des appels et SMS	68
liste noire du Filtre des appels et SMS	65
Etat de la protection	44
Exécuter	
analyse à la demande	53
mise à jour	116
programme	34
F	
FILTRAGE	
APPELS ENTRANTS	62
SMS ENTRANTS	62
Filtre des appels et SMS	62
Filtre des appels et SMS	
modes	63
Filtre des appels et SMS	
liste noire	64
Filtre des appels et SMS	
liste blanche	68
Filtre des appels et SMS	
numéros qui ne figurent pas dans les Contacts	71
Filtre des appels et SMS	
numéros sans chiffre	72
Filtre des appels et SMS	
action sur le SMS	73

Filtre des appels et SMS	
action sur l'appel.....	74

I

INSTALLATION DE L'APPLICATION	21
Interdiction d'accès aux données chiffrées.....	113
Interdire	
appels entrants	64, 68, 77
appels sortants	77
connexions réseau	107
messages SMS entrants.....	77
messages SMS sortants.....	77
INTERFACE DE L'APPLICATION.....	44

J

Journal des événements	120
Journal des événements	
consultation des enregistrements	120
Journaux des événements	
suppression des enregistrements.....	121

L

L'envoi d'une instruction SMS	94
Licence.....	37
Licence	
activation du logiciel	27
contrat de licence	36
Licence	
informations	38
Licence	
renouvellement	38
Liste blanche	
Contrôle parental	79
Filtre des appels et SMS.....	68
Liste noire	
Contrôle parental	77
Filtre des appels et SMS.....	64

M

Menu de l'application.....	46
Mettre à jour	
exécution manuelle.....	116
exécution planifiée.....	117
MISE A JOUR	
VERSION DE L'APPLICATION	25
Modes	
Contacts personnels	97
Contrôle parental	75
Filtre des appels et SMS.....	63
Modification	
liste blanche du Contrôle parental	81
liste blanche du Filtre des appels et SMS	69
liste des contacts confidentiels du composant Contacts personnels	103
liste noire du Contrôle parental.....	78
liste noire du Filtre des appels et SMS	66

N

Niveau de sécurité	
Pare-feu.....	107

P

Planifier	
analyse à la demande	54
mise à jour	117

Q

Quarantaine	
affichage des objets.....	59
restauration d'un objet	60
suppression d'un objet.....	61
QUARANTAINE	59

R

Renouvellement de la licence	38
Restauration d'un objet	60

S

Suppression	
liste blanche du Contrôle parental	82
liste blanche du Filtre des appels et SMS	70
liste des contacts confidentiels du composant Contacts personnels	103
liste noire du Filtre des appels et SMS	67
objet de la quarantaine	61
SUPPRESSION	
APPLICATION	22
Supprimer	
événements du journal	121
liste noire du Contrôle parental.....	79

V

Verrouillage	
chiffrement des données	113
SMS entrants	64